DOI: http://dx.doi.org/10.26642/pbo-2022-2(52)-40-46
UDC 657

S.F. Lehenchuk, Ph.D.
I.M. Vygivska, Ph.D., Prof.
Zhytomyr Polytechnic State University
O.O. Hryhorevska, Ph.D., Prof.
Kyiv National University of Technologies and Design

Protection of accounting information in the conditions of cyber security

In the given study, it is substantiated that the unauthorized use of information generated in the accounting system can lead to harmful consequences, risking loss of information, incorrect data entry and misuse of confidential information. Therefore, the issue of protecting information generated in the accounting system is extremely urgent, and ensuring its security is a priority in many companies. The purpose of the study was to generalize existing approaches and outline promising directions for the organization of accounting information protection in the context of cyber security. It has been proven that effective communication and joint strategies between management, accountants and auditors are important to reduce or protect against emerging threats to the accounting information system. To properly assess potential risks, accountants and auditors must be familiar with current and emerging technologies. Groups of risks are given, based on the selection of risks for all components of the accounting process, which are inherent in electronic accounting information systems (risks associated with the collection and input of data into an automated system, risks associated with information processing and its storage on electronic media, risks associated with stage of generalization and transfer of information) and analyzed their features in order to find ways of minimization. Controlling unauthorized access to accounting records is an important component of internal control. Access and password policies, encryption, digital signatures, disk locks, firewalls, and digital certificates are examples of controls that should be identified, documented, communicated, and tested when evaluating control effectiveness. Examples of the impact of cyberattacks on the accounting system and related costs are given. It is well-founded that the protection of accounting information and the avoidance of cyber-attacks is possible only if comprehensive measures and joint actions of management, accounting, auditors and educational institutions are followed in the training of future specialists.

Keywords: *accounting information; cybersecurity; cyberattack; information security; risk.*

Introduction. «COVID-19 risks outlook: A preliminary mapping and its implications» report, published by the World Economic Forum, reveals already known risks that can be maximized by the pandemic and new ones that it will only produce. The report uses the results of a survey of almost 350 top managers and risk assessors. They were required to outline the most important problems that could arise, both for the whole world and for their business. Thus, the five risks and threats-leaders, according to respondents, over the next 18 months will look like this: a prolonged downturn in the world economy (66,3 %); surge of bankruptcies and strengthening of consolidation of industries (52,7 %); cyberattacks and data fraud due to remote work (50,1 %); inability of some industries and sectors to fully recover (50,1 %); prolonged failures of global supply chains (48,4 %) [2].

Thus, it should be noted that technology has played a key role in how society, businesses and governments minimize the effects of the COVID-19 crisis. And a «contactless» economy can also create new employment opportunities in the post-pandemic world. However, heavy reliance on technology has increased cybersecurity risks. According to 38 % of experts surveyed, new work schemes (such as remote work) lead to cyberattacks and data fraud, and produce the most likely risk of technological consequences for the world. The rapid spread of new technological solutions has exacerbated other risks, such as digital fragmentation, breaches of confidentiality and inequality. Thus, COVID-19 may challenge the relationship between technology and governance, while mistrust or misuse of technology can have long-term consequences for society [12].

Information security is one of the most important aspects of general security at various levels, i.e., national, sectoral, corporate, personal. This is due to the fact that in the modern world the exponential increase in the amount of information has turned it from a secondary resource into a factor that decisively affects almost all spheres of public life, thus reflecting the growing information dependence of society [3].

In turn, the accounting information system is formed from confidential and private information, which can be violated if it is not protected. Unauthorized use of information generated in the accounting system can lead to detrimental consequences, risking loss of information, incorrect data entry and misuse of confidential information [9]. Inadequate information security increases the possibility of manipulation, falsification or alteration of accounting records [11]. Therefore, the protection of information generated in the accounting system is extremely important, and ensuring its security is a priority of many firms.

Related works. Works devoted to the research of the issues of determining the threats of cyber and information security imbalance were written by Hrabchuk I. [4], Popivniak Yu. [5], Fedorenko I. [6], Kharlamov P. [7], Chekh N. [8], Konoplina O. [8], Shakhverdian D. [8] and other scientists and practitioners. The research of mentioned authors is really interesting and highlights the personal approach to the preservation of accounting information, the development of measures to improve its security and prevent violations of information security and cyberattacks. However, approaches to the organization of information security in terms of cybersecurity need further generalization. It is important to outline the contribution of each involved in the businees activity of the enterprise in the formation of means and areas of information protection and review of modern approaches to management of the studied subject area.

Methodology. The study used general and special research methods, which are the basis for identifying the risks and threats of accounting information in cyberattacks. Methods of observation, comparison, analysis, synthesis, generalization became the methods of research and expected results in terms of developing approaches to the organization of accounting information protection in terms of cybersecurity.

Results and discussion. «Information about the facts of business activity of the entity is formed in the accounting system, and is characterized by a high degree of value. It is a guarantee of stability, development and efficiency of such an entity, but only if it is reliably protected» [5]. Unauthorized or inadequate access to the accounting information system or the inability to establish and maintain a division of responsibilities within the internal control system can make it difficult to ensure the registration, processing and submission of reliable and accurate transactions. The active use of the Internet and IT technologies by the accounting system (on the example of individual transcations), which may be affected by the risk of cyberattacks can be shown in Table 1.

Table 1

The use of the Internet and IT technologies in the reflection of certain facts of economic life in the accounting system

Business transaction	Characteristics
Cash flow management	The accounting information system provides a management process that includes data on cash, inventories and sales. A computerized system can provide information much faster than non-automated accounting, making it an important tool in cash and inventory management
Sales process	Recognition of the sales process is the first step towards revenue generation. The accounting system recognizes sales as an increase in revenue together with an increase in cash or receivables. Retailers also need to reduce inventories. This type of transaction is automatically processed using a computerized system. Many firms are implementing outlet software that allows them to scan goods and transfer data to a real-time accounting system, which is a major advantage in cash and inventory management
Payments	Payments that are attentively monitored by management increase cash flows. Depending on the type of business, payments can be made in the form of checks, credit cards, cash, bank transfer and money transfers. These transactions are recorded in the accounting system using entries manually made in journal or interfaces from other systems. Some companies have special receivables modules that recognize not only accounting data, but also sales details, conditions, contacts and other information. When the payment is received, the accountant enters his payment details in the module that goes to the general ledger
Delivery	Delivery is a vital part of the revenue cycle. In integrated delivery systems, activities are reflected in the general ledger, mainly in the inventory section. The system registers all relevant transactions, so employees working in the warehouse do not need to know accounting to properly perform this activity. The shipment function consists of two parts: product selection and shipment. Barcodes are often used to speed up this process, documentation and to reduce inventory accounts
Online commerce	The Internet has removed physical barriers to trade by opening access to previously unprofitable markets. The Internet's possibilities to make business easier can be seriously offset by users' security concerns. Website issues that are sometimes encountered by large e-commerce providers such as Yahoo, eBay, E-Trade, and Amazon.com indicate some of the risks of attacks
Reporting	The accounting information system can generate reports that are used by management to make financial decisions. Some general reports include inventory reports, trend analysis, and receivables maturity reports that tell the manager who the debtor is, how much they owe, and the timing of payments. Without a computer system, it would be very difficult to compile these detailed reports in a timely and efficient manner

Source: systematized and supplemented on the basis of [14, 11]

It is estimated that cybersecurity incidents threaten some people with tens of thousands of dollars. A cyberattack that results in significant data breaches can have detrimental consequences not only for the firm's operating side, but will also have legal consequences for business directors when senior management may face regulatory investigation or litigation.

Data breaches can also lead to a significant risk of trust and reputation, which can lead to loss of income / decrease in share price of publicly registered companies.

As Karen McDonald notes in her research, «Australians lost millions of dollars in 2019 because of phishing emails and text messages posing as banks or utilities suppliers looking for login details; fake online quizzes, surveys and job postings» [13]. And one of Australia's latest tax scams target victims of recent natural disasters, promising an 8 % bonus on 2020 tax returns if the recipient clicks a link that takes them to a fake myGov website designed to steal personal information, including names, addresses, e-mails, telephone numbers and bank details.

The study of cybercrime cases and related costs shows a significant increase. Table 2 provides some examples of cybercrime and related costs that are often significant. Thus, there are a number of threats to accounting information systems, especially for those systems that are used together with the Internet. These threats are problems for management, accountants, auditors and scientists. Sufficient attention is paid to the identification of risks to threats to the security of accounting data by researchers.

Popivniak M. emphasizes «the use of weak tools for authentication of accounting information users; the neglect of the rules of protection of work computers or other devices from which access and work with accounting data take place; the use of working devices for non-working purposes; accountant's lack of basic knowledge in the fundamentals of cybersecurity; incorrect prioritization and lack of proper support from the entity management system; the neglect of the rules of storage of accounting data and its periodic redundancy; ignoring the existing risks and negative experiences of other market participants; the absence of an appropriate specialist who deals with protection of accounting information, etc» [5].

Table 2

Examples of the impact of cyberattacks on the accounting system and related costs (on the example of outsourcing companies in Australia)

Type of cyberattack, damage	Description of the situation
Program-Fraudster Total cost: $ 83,660	A small accounting firm with 10 employees was attacked after one of the employees opened an e-mail, which, in his opinion, contained an attached invoice. The application contained the Cryptolocker virus. All the computers in the office stopped working, and a message appeared asking for $ 8,000 (paid in bitcoins) for starting the system. The amount will increase by another $ 1,200 per day until it is paid. Costs included not only ransom payments, but also IT forensics costs, system recovery after it was found to be malfunctioning after launch, downtime costs, public relations costs, and costs incurred on notifications to counterparties with whom communication was broken
Violation of confidentiality. Total cost: $ 246,000 plus ongoing court proceedings from persons whose personal data have been violated	An employee of a medium-sized accounting firm accidentally left a USB flash drive containing the personal data of several clients in a taxi. Upon discovering the damage, the employee informed his employers, who involved specialized agencies to identify customers whose personal data were disclosed. 175 clients were affected and should have been notified. In addition, data on all victims were kept for the next 12 months by the Credit Monitoring Service and a PR company hired to restore trust and mitigate the negative advertising caused by the event
Hacking. Total cost, including related business interruption: $ 330,000	A dissatisfied employee of a financial services firm changes all administrator passwords to the network, which actually disconnects the entire company from the system. Access to the system had to be restored. At this time, the company could not work
Malicious software. Total cost: $ 300,000	The accounting system of the cloud supplier of accounting firm has been shut down due to an aggressive computer virus. In addition, the business suffers a loss of profits during the system recovery and for 6 months after
Theft of personal data. Total cost is $ 140,000	The accounting firm was hacked, and information about customers and staff was stolen on several laptops. Unfortunately, this information has not been encrypted. Several customers became victims of identity theft, as a result they sued for damages. In addition, the firm incurred significant costs in notifying all affected customers / employees and providing credit monitoring services for two years
Social engineering. Total cost is $ 174,000	Late Friday evening before the weekend (public holiday), a senior employee of the accounting firm received an e-mail, allegedly from a client, notifying him of a change in the details of the client's bank account and requesting to forward the urgent payment to a new account. The letter looked real, and the employee transferred the money. Two weeks later, the client contacted for payment, and the staff informed them that the payment had been made. The investigation revealed that the network had been hacked 6 weeks earlier

Source: systematized on the basis of [13]

Hrabchuk I. notes that «one of the most common types of information threats using computer technology is virus attacks, which not only damage computers software, but also lead to their breakdowns and malfunctions» [4].

Fedorenko I. notes that «a specific threat to the information security of accounting information is the inaccuracy of information, which may arise due to the influence of a number of factors, in particular, due to errors in the software used» [6].

Sheila Shanker in her study lists the risks associated with accounting systems: from booking fake transactions to stealing a backup tape with all the financial information. Examples of risks: theft of social security numbers from employees and contractors; payments to counterfeit suppliers; data deletion / loss; damage of backup tapes; theft of servers or computers [14].

However, an interesting approach that should be agreed with is the approach to the highlighting the risk groups suggested by Ayedh Abdullah, who cited risks based on processes that accounting include: the process of collecting, accumulating, systematizing, summarizing accounting information (Table 3).

Thus, it is objectively that the presence of highlighted threats produces the development of methods to minimize them. For example, Deborah Beard and H. Joseph Wen, emphasizing the need to protect against risks, note that if they are ignored, they can undermine the relevance and reliability of financial information, which will lead to the wrong decisions by various stakeholders [11].

Table 3

Risks faced by electronic accounting information systems

Risk	Content	Characteristic
Risks associated with the collection and input of data into an automated system	1. Staff enters data incorrectly (intentionally/ unintentionally). 2. Unintentional destruction of data by employees. 3. Intentional destruction of data by employees	Masquerade (pretending to be an authorized user) and combination (connection to telecommunication lines) are examples of hacking actions that can seriously affect the collection of reliable data
Risks associated with the processing of information and its storage on electronic media	1. Illegal access (unauthorized) to data and the system by employees. 2. Illegal access to data and the system by people from outside. 3. Using the same password by many employees. 4. Introduction of a computer virus for the accounting system and impact on the operation of the data system. 5. Interception and access to data from servers to users' computers	Illegal access to files or their deletion, destruction or damage of program logic by viruses or change of program logic, forcing the application to process data incorrectly. Failure to maintain backup files or other extraction methods leads to devastating data loss
Risks associated with the stage of generalization and transfer of information	1. Destruction. 2. Formation of falsified reporting. 3. Theft of data / information. 4. Copying 5. Unauthorized disclosure of data by displaying on the screen or printing on paper. 6. Printing and dissemination of information by third parties 7. Transfer of confidential documents to people who do not meet security requirements, for their rupture or disposal	Theft, redirection, or misuse of computer data can damage an organization's competitiveness or reputation.

Source: generalized and supplemented on the basis of [10]

Hrabchuk I. suggests the following measures to minimize risks in terms of logical (risk identification, consideration of information security of the entity as part of corporate culture) and physical (data encryption, physical protection of technical support) security. Taking these measures into account will significantly minimize the consequences of cyberattacks [4].

Sheila Shanker also identifies two groups of management methods: preventive (to prevent risks) and detective (to identify problems ex post facto). Once the risks have been identified, you can configure controls to protect the system: frequent change of password; data encryption; monthly inspection of suppliers' reports; safe and secure server and computer environment; safe and secure archiving of backup tapes outside the office [14].

Viter S. and Svitlyshyn I. distinguishes three groups of measures: 1) organizational (restriction of unauthorized access to confidential accounting information); 2) technical (prevention of intentional damage to accounting information by means of specially provoked malfunctions of hardware or software); 3) personnel work (increasing the competence of employees and their responsibility in the application of the latest information technologies) [1].

We can agree with all the above suggestions. After all, every business entity tries to avoid the risks of cyberattacks and ensure information security of information in any way.

But, in our opinion, the protection of accounting information and avoidance of the «hook» of a cyberattack is possible only in the case of comprehensive measures and joint actions of management, accounting staff, auditors and, not surprisingly, educational institutions in training future professionals.

For example, the director of the entity must have the knowledge and competence to understand the procedure for documentation and be able to test the internal control system. This does not mean that the director must be an accountant by profession, or be a specialist in programming or information security. But the director must understand the nature of all transactions and be interested in such issues as the actual availability of assets and liabilities specified in the financial statements; the validity of the reflection of business transactions registered and reflected in the reporting and whether all transactions are reflected; whether the objects of accounting are correctly classified and disclosed in the financial statements; whether it is possible to trust the answers of responsible employees if there is a threat to the information security of the entity, and management has not taken measures to protect the organization from internal and external threats.

Accountants should be aware of security threats and appropriate controls to protect their own information systems and advise businesses on security risks. It is important to provide accountants with the latest antivirus software. The ability to recognize fraud by e-mail that is not addressed directly is relevant. For example, Karen McDonald suggests 6 ways to recognize fake letters: low grammar / spelling, poor quality illustrations; presence of instructions for following the link; strange origin; sense of urgency [13]. It is also important to back up data as often as possible as well as to use strong passwords. And, of course, avoid opening attachments from unknown people in the mail. An important subject of ensuring the avoidance of cyberattacks of the entity is the auditor (external, internal). Thus, procedures where an auditor may appoint an IT professional include: clarifying what data and transactions are initiated, recorded, processed, and recognized; what IT management tools are implemented; verification of system documentation; monitoring the work of IT-controls; planning and performing tests of IT management tools. The auditor should have sufficient IT knowledge to communicate the purpose of the audit to the IT professional, assess whether the procedures will meet the auditor's objectives, and evaluate the results of the procedures as they relate to the nature, timing and extent of other audit procedures [11].

Scientists and teachers. In today's world, an important aspect of training future professionals is their understanding of the need for IT security and the importance of working with others to develop policies, processes and technologies to eliminate threats. Today, future accounting and taxation professionals should be required to have the knowledge, skills, and ethics to understand the business environment, conduct risk assessments, assess internal controls, and implement effective and efficient security measures. It is important to strive for the integration of security topics and methods into accounting curricula.

As Deborah Beard and H. Joseph Wen point out, CPA certificates (confirms professional knowledge in audit, business law, financial accounting and reporting, taxation), CMA (Certified Management Accountant) and CIA (Certified Internal Auditor) increasingly recognize the importance of IT. In the CPA exam, from 12 % to 18 % in the section «Auditing and Attestation» and from 22 % to 28 % in the test section «Business Environment and Concepts» relate to the computerized environment and its impact on IT in the business environment. In the CMA exam, 15 % of Parts I and II is taken into account in determining expected risks, internal control, system control and security, systems development and design, e-commerce, enterprise resource planning (ERP) and other areas related to information systems and technologies. In the CIA exam, from 30 % to 40 % of Part III covers IT, including management structures, data and networking, electronic data interchange, encryption and information security [11]. New professional designations, such as Certified Information Technology Professional (CITP), Certified Information Systems Auditor (CISA), and Certified Information Systems Security Professional (CISSP), demonstrate the need for certification related to information technology, systematic audit, and systems security.

Another promising area of risk minimization is comprehensive cyber insurance. This phenomenon is new for both the global insurance market and the Ukrainian market, which covers only 5 % of cyberattacks. Note that in the market of insurers such services are provided by Insurance Company «Ridna», Insurance Company «Ingo», Insurance Company «Aska» and others. As P. Kharlamov notes, «according to Munich Re, a total of 60 insurance companies in different countries offer such protection. At the same time, insurance covers only 5 % of cyber risks. However, the shaft-like growth of threats from hackers stimulates the development of this area, and according to the same Munich Re, the volume of cyber insurance in 2020 will amount to $ 8–9 billion against $ 3,4–4 billion in 2017. And according to a study by the insurance group Allianz, the cyber insurance market is growing by 25–50 % annually» [7].

Thus, understanding the need for security is a common denominator. The security of electronic information has become a critical issue. Scientists, managers, accountants and auditors should be aware of emerging threats and security measures that are effective in ensuring the security of accounting information systems.

Conclusions and recommendations. Thus, effective communication and strategies between management, accountants, and auditors are important to reduce or protect against emerging threats to the accounting information system. To properly assess potential risks, accountants and auditors must be familiar with current and new technologies. Control of unauthorized access to accounting records is an important component of internal control. Access policies and passwords, encryption, digital signatures, disk locks, firewalls, and digital certificates are examples of controls that need to be identified, documented, reported, and verified when evaluating the effectiveness of controls.

References:

1. Viter, S.A. and Svitlyshyn, S.A. (2017), «Protection of accounting information and cyber security of the enterprise», *Economy and society: electronic specialist publication*, No. 11, pp. 497–502.
2. The impact of the pandemic: an overview of global risks, [Online], available at: https://cutt.ly/7CM9vSf.
3. Glukhov, N.I. (2013), *Assessment of information risks of the enterprise*, 148 p.
4. Hrabchuk, I.L. (2018), «Organization of protection of accounting information in conditions of hybrid warfare», *Problems of theory and methodology of accounting, control and analysis*, No. 3 (41), pp. 20–24.
5. Popivniak, Yu.M. (2019), «Cyber security and protection of accounting data in conditions of application of the latest information technologies», *BUSINESS INFORMATION*, No. 8, pp. 150–157.
6. Fedorenko, I.V. (2015), «Methodological issues of information security risk assessment in accounting», *Bulletin KrasGAU*, No. 3, pp. 161–168.
7. Kharlamov, P. (2019), «The Hacker Pill: How Businesses Protect Yourself from Cyber Attacks», *MIND.UA*, [Online], available at: https://mind.ua/publications/20192978-pigulka-vid-hakeriv-yak-biznes-zahishchae-sebe-vid-kiberatak
8. Cheh, N.O., Konoplina, O.O. and Shakhverdyan, D.S. (2019), «Ensuring the information security of the company's accounting», *Communal management of cities*, Ser. *Economic sciences*, Vol. 2, pp. 111–117.
9. Shanker, Sheila (2017), «Accounting Information Systems Security», *Bizfluent*, No. 26, [Online], available at: https://bizfluent.com/list-6396287-accounting-information-systems-security-issues.html
10. Ayedh, Abdullah (2018), «Risk of computerizing accounting information systems in the libyan bank», *South East Asia Journal of Contemporary Business, Economics and Law*, Vol. 10, Issue 1, pp. 74–79.
11. Deborah Beard, H. Joseph Wen (2017), «Reducing the Threat Levels for Accounting Information Systems», *Challenges for Management, Accountants, Auditors, and Academicians The CPA Journal*, [Online], available at: http://archives.cpajournal.com/2007/507/essentials/p34.htm
12. Emilio Granados Franco Richard Lukacs, Marie Sophie Müller Philip Shetler-Jones and Saadia Zahidi (2020), «COVID-19 Risks Outlook», *A Preliminary Mapping and Its Implications*, May, [Online], available at: https://go.pardot.com/l/395202/2020-05-19/bm4tdn/395202/206461/covid19_risks_outlook_en_uk.pdf
13. McDonald, Karen (2020), *Cyber crime – The threat is real and could dramatically affect you and your accounting firm. Accountancy Insurance*, [Online], available at: https://www.accountancyinsurance.com.au/cyber-crime-threat/
14. Shanker, Sheila (2017), «The Revenue Cycle in Accounting Information Systems», *Bizfluent*, [Online], available at: https://bizfluent.com/info-8001409-revenue-cycle-accounting-information-systems.html
15. Lehenchuk, S., Valinkevych, N., Vyhivska, I. and Khomenko, H. (2020), «The Significant Principles Of Development Of Accounting Support For Innovative Enterprise Financing», *International Journal of Advanced Science and Technology*, No. 29 (8s), pp. 2282–2289, [Online], available at: http://sersc.org/journals/index.php/IJAST/article/view/14701

Легенчук Сергій Федорович – доктор економічних наук, професор, завідувач кафедри інформаційних систем в управлінні та обліку Державного університету «Житомирська політехніка».

http://orcid.org/0000-0002-3975-1210.

Наукові інтереси:

– проблеми бухгалтерського обліку.

Вигівська Ірина Миколаївна – кандидат економічних наук, доцент, доцент кафедри інформаційних систем в управлінні та обліку Державного університету «Житомирська політехніка».

http://orcid.org/0000-0002-4974-5834.

Наукові інтереси:

– добровільне розкриття облікової інформації;
– облікове забезпечення управління ризиками господарської діяльності;
– проблеми бухгалтерського обліку витрат.

Григоревська Олена Олександрівна – кандидат економічних наук, доцент, доцент кафедри фінансів та бізнес-консалтингу Київського національного університету технологій та дизайну.

http://orcid.org/0000-0001-8279-3523.

Наукові інтереси:

– проблеми бухгалтерського обліку та аналізу господарської діяльності.

Легенчук С.Ф., Вигівська І.М., Григоревська О.О.

Захист облікової інформації в умовах забезпечення кібербезпеки

У статті обгрунтовано що несанкціоноване використання інформації, сформованої в системі бухгалтерського обліку, може призвести до згубних наслідків, ризикуючи втратою інформації, неправильним введенням даних та зловживанням конфіденційною інформацією. Тому питання захисту інформації, сформованої в системі бухгалтерського обліку, є надзвичайно актуальними, а забезпечення її безпеки є пріоритетом у багатьох фірмах. Метою дослідження стало узагальнення існуючих підходів та окреслення перспективних напрямів до організації захисту облікової інформації в умовах забезпечення кібербезпеки.

Доведено, що ефективна комунікація та спільні стратегії між керівництвом, бухгалтерами та аудиторами важливі для зменшення або захисту від виникаючих загроз інформаційній системі бухгалтерського обліку. Щоб правильно оцінити потенційні ризики, бухгалтери та аудитори повинні бути знайомі з поточними і новими технологіями. Наведено групи ризиків, на основі виділення ризиків для всіх компонентів облікового процесу, які притаманні електронним бухгалтерським інформаційним системам (ризики, пов'язані з збором та введенням даних в автоматизовану систему, ризики, пов'язані з обробкою інформації та її зберіганням на електронних носіях, ризики, пов'язані з етапом узагальнення та передачею інформації) та проаналізовано їх особливості з метою пошуку шляхів мінімізації.

Контроль несанкціонованого доступу до бухгалтерських записів є важливим компонентом внутрішнього контролю. Політика доступу і паролів, шифрування, цифрові підписи, блокування дисків, міжмережеві екрани і цифрові сертифікати є прикладами заходів контролю, які повинні бути ідентифіковані, задокументовані, повідомлені і піддані перевірці при оцінці ефективності контролю. Наведено приклади впливу кібератак на систему бухгалтерського обліку та пов'язані з цим витрати. Обгрунтовано, що захист облікової інформації та уникнення кібератаки можливе лише за умови дотримання комплексних заходів та спільних дій керівництва, бухгалтерії, аудиторів та навчальних закладів у підготовці майбутніх фахівців.

Ключові слова: облікова інформація; кібербезпека; кібератака; інформаційна безпека; ризик.

Стаття надійшла до редакції 12.05.2022.