DOI: 10.55643/fcaptp.6.53.2023.4254

ENSURING CYBERSECURITY IN ACCOUNTING IN THE DIGITAL ECONOMY ERA

Svitlana Laichuk
PhD in Economics, Associate Professor of the Department of Information System in Management and Accounting, Zhytomyr Polytechnic State University, Kyiv, Ukraine;
e-mail: laychuksm@gmail.com
ORCID: 0000-0001-7939-1195
(Corresponding author)

Yatsko Maksym
PhD in Economics, Associate Professor of the Department of Accounting and Auditing, Uzhhorod National University, Uzhhorod, Ukraine;
ORCID: 0000-0003-1145-5302

Liubov Koval
Candidate of Economy Sciences, Associate Professor of the Department of Accounting, Vinnytsia National Agrarian University, Vinnytsia, Ukraine;
ORCID: 0000-0003-3637-850X

Olena Dovzhyk
PhD in Economics, Associate Professor of the Department of Accounting and Taxation, Sumy National Agrarian University, Sumy, Ukraine;
ORCID: 0000-0001-6547-1418

Serhii Harkusha
PhD in Economics, Associate Professor of the Department of Accounting and Taxation, Sumy National Agrarian University, Sumy, Ukraine;
ORCID: 0000-0002-2043-1217

Received: 17/11/2023
Accepted: 19/12/2023
Published: 31/12/2023

ABSTRACT

The study emphasizes the importance of protecting accounting data in cyberspace, namely the introduction and improvement of computer systems that allow solving the problem of protecting accounting information and other resources of state importance. Information security is an urgent problem today, as the number of threats in the information and communication space is increasing every time. A leading role in ensuring information security in accounting systems is played by a variety of modern programs, the main task of which is to ensure the confidentiality, integrity and authenticity of transmitted data. Therefore, the purpose of the study is to highlight the importance and role of using a secure system to protect against cyber threats in accounting in modern conditions. The research results reflect the process of cyber protection with the help of accounting protection programs, their essence, signs, indicators, prospects of application now and in the future. Accounting information systems are formed from confidential and personal information that can be leaked if not protected. Unauthorized use of information generated by accounting systems can lead to such negative consequences as loss of information, incorrect data entry and misuse of confidential information. An inadequate level of information security increases the likelihood of manipulation, falsification or alteration of accounting records. The protection of data generated by accounting systems is critical, and ensuring its security is a priority for many companies. The conclusion confirms that the cryptographic system is innovative and reliable today for protection against cyber-attacks.

Keywords: information warfare, cyber threats, cyber-attack, information security, cyber security strategies, opportunities and risks

JEL Classification: M40, M15, C87

INTRODUCTION

Today, cybersecurity is one of the main factors in the existence of states and the functioning of enterprises in all areas of activity, including the digital economy, and in particular, accounting. Cyberspace and cybersecurity are key features of the modern world, which is characterised by increasing informatisation and digitalisation of all areas of government, society, business, science, education, and personal life. The development of accounting leads to the development of methods and technologies for cyber-attacks while providing more and more opportunities for more effective protection against them. This area of information activity is becoming increasingly important. Therefore, finding ways to ensure cybersecurity is now an important issue for the accounting sector.

Speaking about the current state of information and security in Ukraine, it can be argued that it has been under the threat of cyberattacks since independence, and now, with the beginning of the full-scale occupation, cyberattacks are becoming widespread. In this context, all companies should assess the vulnerability of their operations to cybersecurity incidents and technical failures. Such threats may arise as a result of attacks on systems and infrastructure or as a consequence of military operations. Companies operating in critical infrastructure sectors, such as energy, telecommunications, media, and financial companies, should be on high alert as they are the main targets for cyberattacks in times of war. Businesses should be prepared to respond to these challenges and assess their readiness to continue operations in the event of a cyber incident. Ensuring cybersecurity is a priority in Ukraine's national security system.

The study emphasises the importance of new information technologies, namely the introduction and improvement of computer systems that help to solve the problem of protecting accounting information and other resources of national importance. Information security is an urgent issue today, as the number of threats in the information and communication space is increasing. The leading role in ensuring information security in accounting systems is played by modern software, one of the main tasks of which is to ensure the confidentiality, integrity, and authenticity of transmitted data. A large number of domestic and foreign scholars are studying the importance of data protection in accounting.

LITERATURE REVIEW

To ensure the stable and efficient operation and development of enterprises, the main task is to ensure the security of economic information.

The most valuable economic information is the accounting information that characterises all aspects of an enterprise's activities (Novitsky, 2020). Today, most companies have switched to computerised accounting and use specialised software and hardware. Unauthorised use of information generated by accounting systems can have negative consequences, such as loss of information, incorrect data entry, and misuse of confidential information. Inadequate information security increases the likelihood that accounting records may be manipulated, falsified or altered.

Otonne et al. (2023) point out that cyber fraud and other disruptions in payment financial technology negatively impact the productivity, management, and development of enterprises. At the same time, large amounts of accounting information are stored and processed in computer systems, and any failure can lead to unnecessary costs, revenue loss, loss of assets, and sanctions. Therefore, the protection of accounting information at enterprises is a priority, as is the development of measures aimed at preserving the information contained in the company's computer databases (Bushman, 2021).

Abdullayeva and Ataeva (2022) point out that the use of secure cryptographic systems is extremely important for modern countries with developed economies, as it contributes to the security of the state and improves the standard of living in general. Spilnykand Palukh(2019) continued this idea and noted that changes in cyber defence are necessary for the global economy, politics, and scientific and technological development, and, in particular, new approaches in various fields, namely in the accounting system. According to a study by Vdovichena et al. (2022), accounting is impossible without interconnecting with the latest technologies and improving models and methods for cybersecurity.

In other words, there are many obstacles to creating effective mechanisms for future economic development. On the one hand, one of the most important is the high level of uncertainty in the current economic and political environment. On the other hand, there is a high risk of cyberattacks in the economic sphere. Effective mechanisms for future economic development must be in line with current global trends. They should be in line with current global trends (e.g., the concept of sustainable development, digital transformation of the economy, business support, etc.) It should be as adaptable and flexible as possible to unpredictable changes, according to Tarasenko et al. (2022).

Verbivska et al. (2022) find that electronic document management makes it possible to make document flow more transparent and significantly speed it up. Integration of the electronic document management system and accounting software will increase the efficiency of accounting and management accounting at an agricultural enterprise. Omelchyk et al. (2022) point out that the transformation of the economy in certain areas through the use of information and communication technologies not only increases the competitiveness of countries in international markets but also contributes to the optimisation and improvement of business processes in the international business environment, which is directly related to cyberattacks. Popivniak (2019) adds that in the process of European integration, Ukraine has developed its own strategies in accounting and protection, which are in line with the principles of European public policy.

Drawing on international experience, we can say that the process of ensuring cybersecurity involves primarily counteracting destructive influences in this area. This requires the creation and organisation of a powerful cyber defence subsystem. An equally important element of the cybersecurity system is the cyberintelligence and cyberinfluence subsystem Legenchuk et al. (2022).

The problem of cyber defence of economic systems is becoming more and more urgent every year. Cyberattacks affect both individuals and the international community as a whole. This affects the international community as a whole. Financial institutions and financial market infrastructures are the most vulnerable to cyberattacks, the specifics of which change almost daily.

Harkusha (2021) emphasises in his study that the protection of the global financial system is primarily about its proper organisation. Secondly, it consists of the process of strengthening the protection of electronic means and systems from

DOI: 10.55643/fcaptp.6.53.2023.4254

cyber threats is important. It is important because it is the only way to ensure that the system is protected from the growing number of cyber risks, but it is not sufficient to address the growing number of existing and emerging cyber risks. Cyber risks Unlike other industries, the financial services sector has neither the resources nor the capacity to implement technical solutions. The main challenge lies in collective action to protect against cyber-attacks. It is a question of how best to organise the protection of systems between governments, financial authorities, and industry, and how to use these resources effectively and efficiently.

Popivniak (2019) explores the transition of national economies to digital forms, the development of innovative digitalisation processes, observations in the context of the level of information awareness of society, and the organisation of cybersecurity, which are current challenges. System and database administrators are in a favourable position to commit or facilitate fraud, as they have full access to the accounting system, encryption keys, passwords, and the destruction of the consequences of illegal actions, Liubymovet al. (2022) noted in their study. Muravskyi and Shevchuk(2021) point out that the transition of the digital economy is the transition of business entities to electronic transactions. Accounting forms an information array for cash management, an element that ensures the financial security of an enterprise.

An important aspect is the arguments of Shyrokopoias (2020), who points out that in order to provide sufficient and effective accounting information on the sale of business security services to internal and external users, companies are offered the following measures: internal and external reporting and the sale of business security services.

The issue of cybersecurity of accounting data requires further research.

AIMS AND OBJECTIVES

The purpose of this study is to determine the importance and role of using a secure accounting system to protect against cyber threats in accounting in the context of the development of the digital economy.

The main objectives of the article are:

- to analyse the state of information threats in accounting, assess the current state, risks, and shortcomings;
- to compare the functioning of accounting security programs in Ukraine;
- to identify and analyse the prospects for implementing the latest cyber security programmes and their impact on the accounting system as a whole.

METHODS

This study uses two groups of methods: empirical (comparison, description, experiment) and theoretical (analysis, synthesis, induction, deduction). The description method is used to characterise the theoretical and methodological aspects of the use of accounting data protection software, its main advantages, and disadvantages. The features of modern cybersecurity systems in Ukraine are identified. Using the inductive and deductive methods, a comprehensive analysis of further prospects for the development of information security with the help of countermeasures that protect information and accounting data is carried out. The author uses the method of analysis and synthesis to clarify the need to use cybersecurity programs in the digital economy due to possible risks. Based on the information collected, it is established that the management and protection of financial data in accounting is important. The study is based on a research method that reflects the current state of cyberattacks and allows for identifying negative factors affecting economic activity in the current and long-term perspective. The generalisation method identifies and summarises the main aspects of financial data cybersecurity issues. The combination of these methods necessitates the use of innovative methods of protection against financial threats. The methodology makes it possible to determine the value of financial data security in accounting through the implementation and use of modern software. A search method is implemented to identify effective steps and evaluate cryptographic methods. The method of comparison used in the study and mastered in this problem can expand the boundaries of the problem under study and facilitate further analysis to compare this issue in Ukraine and the world.

RESULTS

Accounting provides information for many other types of accounting for analysis, management, and management decision-making, as it is continuously stored and reflects all business activities of the enterprise. Accounting is closely related to

other economic sciences, such as business analysis, statistics, sectoral economics, finance, taxation, management, and marketing (Tesak, 2022).

As a rule, the volume and composition of accounting data constitute a significant secret of the enterprise. Therefore, the order of their protection is determined by the management of the organization independently in accordance with the current legislation. This is due to the fact that "the most important issue in the process of using such information is the protection of trade secrets". Security is about protection against danger, damage and/or loss and a range of other criminal activities. Quite often, the concept of "cyber security" is found alongside "information security". (Viter&Svitlyshyn, 2017). It is important to distinguish between these concepts.

Cybersecurity goes beyond simple information security and ensures the protection of various corporate assets (not just information) that are at risk when companies use computer systems and communication networks (Spilnyk & Palukh, 2019). At the same time, information security is a process that makes it possible to maintain the confidentiality of information, its availability and integrity. It is important to note that this security also protects information resources and allows to process and store them without the use of computer technologies, but together with electronic information (Martsenyuk et al. 2021).

In this study, cybersecurity is considered only in the area of protecting credentials circulating in cyberspace (an environment consisting of information systems around the world, including the networks connecting these systems), and not just stored on individual user computers.

Cybersecurity systems for accounting information are a set of measures aimed at ensuring the security and protection of such information and automated accounting systems from cyber threats both at the national level and at the level of an individual enterprise (Harkusha, 2019).

An increasing number of different companies are automating and digitising accounting in line with global trends, using the latest technologies and tools such as blockchain, artificial intelligence, cloud, mobile computing, fog and machine learning (Muravskyi et al. 2022). Each of the above-mentioned technologies is characterised by specific risks to accounting information arising from the nature and functional features of the particular technology, in addition to the list of general threats mentioned above (Grigorevska, 2020). Therefore, it is necessary to understand what information is private for any business or organization and what information should be kept secret. In accordance with this, cyber security norms are highlighted in the accounting policy, which are important to observe in the era of the digital economy (Figure 1).

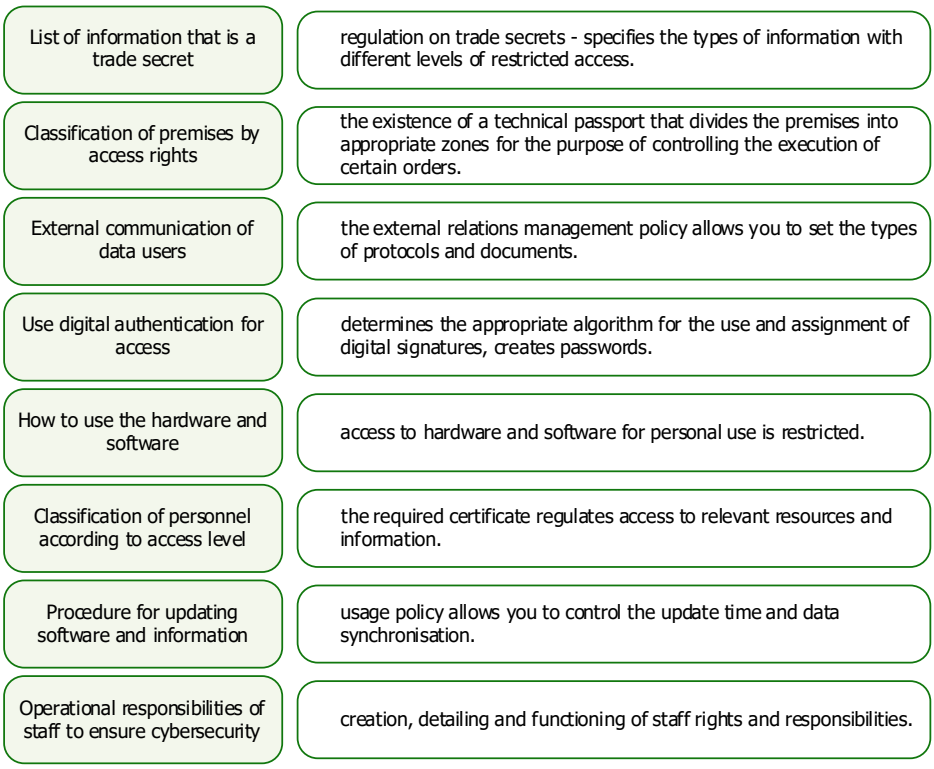

Figure 1. Security standards in enterprise-based accounting policies. *(Source: compiled by the author based on data from Lehenchuk et al., 2022)*

DOI: 10.55643/fcaptp.6.53.2023.4254

To avoid the risk of information being compromised, it is worth using cloud services. They allow you to work with software (Muravskyi & Patel, 2020). The software can be connected via an encrypted channel (Tomislav, 2018). This is the most effective way to protect accounting databases from external attacks and force majeure. The database containing the information is not stored on the accountant's computer, but on a remote server in a room without access for unauthorised persons, which ensures that no matter what happens to the equipment (e.g., breakdown, seizure, theft), valuable information will be protected and preserved.

Cloud-based accounting and reporting technologies have their own peculiarities and are not completely secure (Muravskyi & Chevchuk, 2021). Specific threats to accounting information include the inability to use old versions of software, high dependence on the quality of services provided by providers, uncertainty about confidentiality and ownership of data in the cloud (lack of proper legal protection of information rights in the cloud environment), and sources of threats can be difficult to identify (Martsenyuk et al. 2021).

Blockchain technology contributes to the development and improvement of the field of accounting and auditing and has significant prospects in the era of the digital economy. Therefore, it is important to highlight the advantages of using this technology, which are reflected in Figure 2.

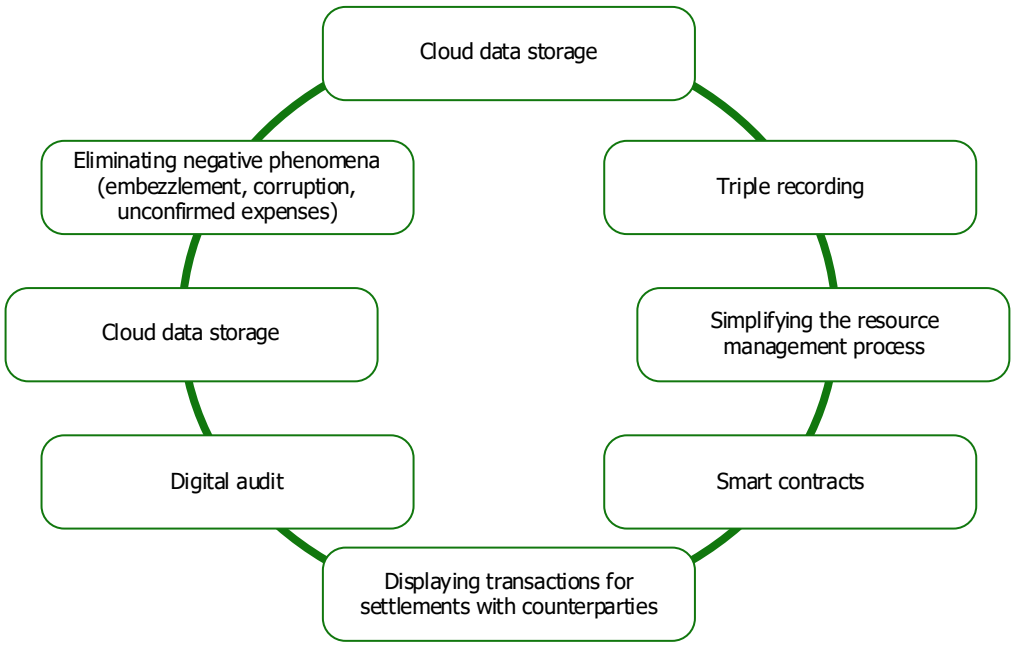

Figure 2. Advantages of using blockchain technology in accounting. *(Source: compiled by the author based on data from Savkiv and Kuzmin, 2023)*

Despite the significant advantages of blockchain technology in accounting, there are also specific threats to information. This technology has a low level of privacy and confidentiality of data about the company's activities, legally authorized persons responsible for maintaining a distributed database of transactions, as well as overloading data storage devices due to the inevitable increase in their volume.

Popivniak (2019) defines a comprehensive system of measures to ensure the cybersecurity of accounting information. The researcher believes that it is necessary to apply legal, technical, organisational, and personnel measures to protect against cyber threats at any enterprise or organisation. Legal measures include the following steps:

- signing documents with employees on proper non-disclosure and storage of information that is a trade secret;
- development of regulations, orders, internal standards, instructions on data non-disclosure, organisation of security, and protection of accounting information;
- Enshrining provisions on the protection of accounting information in the constituent documents of any company;
- creating rules for working with accounting information in automated management, determining the responsibility of employees for non-compliance;
- documentary approval of the list of data constituting a trade secret at the enterprise;
- use of forms, forms, and registers for recording information;

- purchase of a cyber insurance policy.

Technical measures include:

- prohibition of privileged activation of accounting software, adding its updates to the "white list" of security systems;
- regular updates of operating systems and anti-virus software;
- use of anti-virus software, modern technical information security tools, virtual private networks (VPNs), secure browser extensions, firewalls, and other means of protecting the server environment;
- disabling automatic software updates;
- mandatory anti-virus scanning of all incoming business emails;
- careful selection of accounting software to protect accounting information;
- regular testing of information systems to identify possible threats;
- availability of technical means of protecting premises from unauthorised entry, use of entrance cards and badges;
- accounting on remote servers;
- using only licensed software products and updating them from official sources;
- use of reliable data encryption technology when sending data;
- use of secure devices and access channels for remote accounting;
- ensuring periodic changes and improvements to cyber defence tools and systems, focusing on preventing rather than detecting cyber threats.

Personnel measures to protect accounting information:

- regular backup of accounting information to media not connected to the head office;
- avoiding unnecessary software on work computers;
- a clear system of authentication of persons who have access to accounting information, such as PIV/CAC cards;
- establishing a cybersecurity unit and regulating its activities;
- a clear list of persons who have access to information and accountability mechanisms;
- a clear list of authorised persons and accountability mechanisms;
- efficient organisation of accounting information storage systems;
- thoroughly checking the reliability and reputation of service providers when outsourcing accounting tasks;
- Establishing effective risk control and analysis systems.

Personnel measures include:

- training employees of any organisation in the basics of cybersecurity and the rules for the safe handling of information in the cyber environment;
- hire people with appropriate moral and positive characteristics from previous jobs;
- provide ongoing training for security personnel on new types of threats and best practices to address them;
- to increase the level of in-depth awareness and responsibility of accounting personnel regarding the existence of cyber threats and the problem of protecting information from them (Popivniak, 2019).

According to SonicWall's (2023) Cyber Threat Report, malware attacks are on the rise for the first time since 2018. The number of attacks increased to 5.5 billion, which is 2% more than the previous year. This significant growth is due to a significant increase in the intensity of cryptojacking and IoT malware.

The Global Cybersecurity Index (NCSI, 2023) reflects the security of information in the cyber environment of any country. It is calculated on the basis of capacity building and cooperation factors, technical, legal, and organisational indicators. According to the relevant data, Ukraine lags behind the leaders and ranks only 24th (75.32%) among 176 countries, being roughly on par with Latvia, Ireland, Switzerland, etc. Table 1 presents an analysis of the countries that show the best results.

DOI: 10.55643/fcaptp.6.53.2023.4254

Table 1. Top 10 countries in the world according to the National Cybersecurity Index (January 2023). *(Source: compiled by the author based on NCSI, 2023).*

Country name	Location.	National cybersecurity index, %.	Digital development level, %.	Development of cyber-security policy, %.	Cyber threat analysis and information, %.	Contribution to global cybersecurity, %.	Protection of digital services, %.	Protection of essential services, %.	Electronic identification and trust services, %.	Protection of personal data, %.	Response to cyber incidents, %.	Combating cybercrime, %.
Belgium	1	94.81	74.07	86	100	100	100	100	100	100	100	100
Lithuania	2	93.51	67.34	100	100	100	100	100	89	100	83	100
Estonia	3	93.51	75.59	86	100	100	100	83	89	100	100	100
Czech Republic	4	90.91	69.21	100	100	50	100	100	89	100	100	100
Germany	5	90.91	80.01	100	100	50	100	100	89	100	100	100
Romania	6	89.61	59.84	100	80	83	80	100	89	100	100	100
Greece	7	89.61	64.02	100	80	83	100	100	100	100	100	100
Portugal	8	89.61	68.46	100	100	100	100	33	78	100	100	100
United Kingdom	9	89.61	79.96	71	100	100	40	83	89	100	100	100
Spain	10	88.61	72.21	86	100	50	100	83	100	100	67	100

CyberEdge Group (2022) conducted a study that addresses the protection of critical information, including accounting data, from cyber threats. 1,200 IT security professionals participated in this study to collect and process data. This applies to 19 industries and representatives of 17 countries. Figure 3 presents data on the general state of successful cyberattacks on the information data of organizations, which includes the accounting system.

Figure 3. Percentage of countries whose information data of organizations suffered from cyber attacks, %. *(Source: CyberEdge Group, 2022)*

A CyberEdge Group (2022) study found that 85% of organisations suffered a successful cyberattack in 2021, with an unprecedented 41% experiencing six attacks. Last year, 63% of ransomware victims paid a ransom, which in turn made it harder for cybercriminals to launch attacks. Only 64% of different organisations have adopted API security. The study found that only 84% of organisations require a significant number of skilled IT security personnel, especially analysts, IT security administrators, and architects. In 2022, a significant number of enterprises increased their typical IT security budget by 4.6% compared to previous years. Security accounts for 12.7% of total IT budgets. 41% of security services and applications are delivered via the cloud. Three out of four organisations have implemented or will soon implement SD-WAN, secure access to edge access service (SASE), and zero-trust network access (ZTNA).

The four most commonly used technologies for secure operations were identified as endpoint security software, virtual private networks (VPNS), SD-WANS, and network access control (NAO). The biggest threats to successful cybersecurity were: a lack of qualified personnel, low security awareness among employees, poor integration between security solutions, and lack of management support or awareness.

We believe that the era of the digital economy, the war, the COVID-19 pandemic and other imbalances in Ukraine have led to the activation of cyber risks in the field of accounting. We are observing a significant increase in the number of cyber-attacks as part of hybrid wars related to the manipulation of credentials, their distortion and replacement to cause economic damage to large enterprises and sectors of the economy, which ultimately leads to harm to the economic security of the country. Pandemic changes in the work process distanced and isolated employees, which required the provision of active information exchange between the workplaces of specialists and the information base of employers' enterprises. The active use of communication services for the implementation of functional duties has attracted the attention of cyber-criminals, whose goal is to steal the company's commercial secrets and intellectual property. Economic imbalances and corruption threats to business have a similar impact on accounting processes, which leads to a significant reduction in the costs of cyber security of business entities. As a result, the number of vulnerabilities in the accounting and management cyber protection system has increased significantly.

Despite everything, the level of security of Ukraine's cyberspace remains unsatisfactory. According to experts, Ukrainian systems remain vulnerable to hacker attacks.

In 2022, about 300 companies were affected by attacks on 63 suppliers. Compared to the previous year, in 2022 there was an average of 4.7 affected companies per supplier, while in 2021 the average was 2.5 affected companies per supplier.

Total spending on public cloud services will reach USD 591.8 billion in 2023, which is 20.7% more than USD 490.3 billion in 2022 (Figure 4). This is higher than the projected growth of 18.8% in 2022.

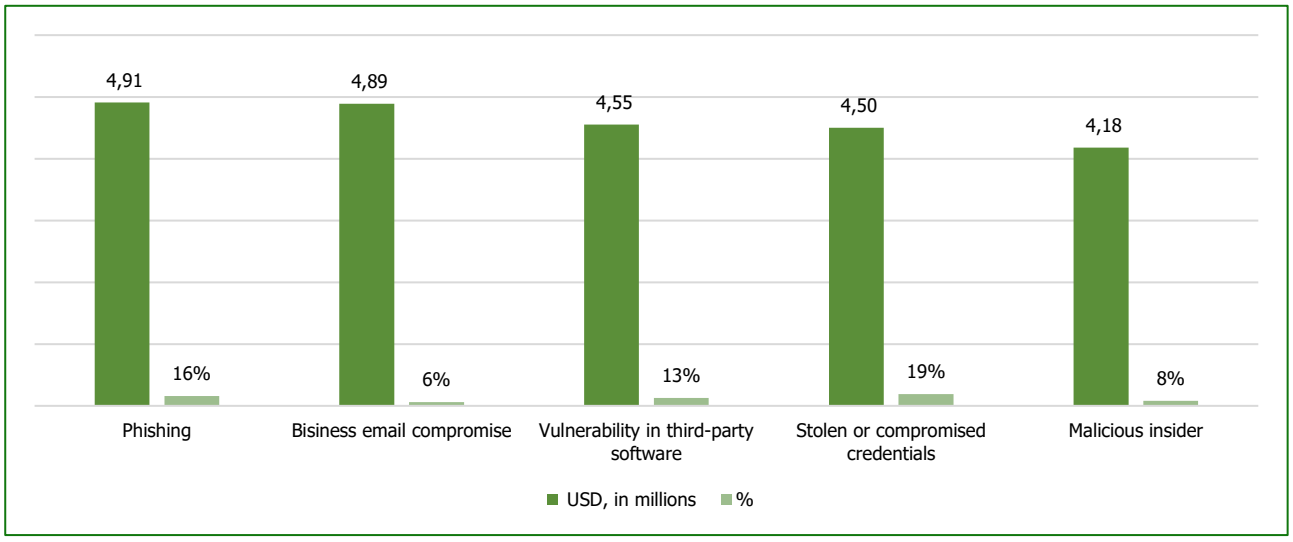

Figure 4. The average cost of data leakage from cyberattacks by industry in 2022. *(Source: compiled by the author based on CyberEdge Group, 2022).*

Therefore, the effectiveness of the cyber security system depends on effective risk management. In general, network security management is integrated into the general economic security management system of the enterprise, and the level of information protection, organizational and personnel issues are decided in accordance with the size and capabilities of the enterprise, as well as in accordance with the calculation of economic feasibility. They provide for the creation of a special service to ensure the cyber security of accounting information or the introduction of the position of a cyber security specialist in the company's structure, who will deal with the development of protection systems for various communication networks and electronic databases.

Specialists of information security and penetration testing organizations, inspectors of confidential information protection organizations, cyber security project analysts, system administrators, computer network administrators, cyber security system analysts, information security system managers can provide special cyber security services.

We found, comparing the functioning of the accounting security program in Ukraine, that the main shortcomings (cyber risks of accounting data processing) are phishing, financial fraud, database theft, industrial espionage, DDoS attacks,

DOI: 10.55643/fcaptp.6.53.2023.4254

extortion, information destruction, data entry errors; violation of the control limit; violation (loss) of records, etc. At the same time, there are a number of benefits of using security software, namely, it helps to identify cyber risks, prevent, avoid and minimize the consequences of cyber threats, etc.

We believe that there are significant prospects for the implementation of the latest cybersecurity programs, which are important in the digital economy. They have advantages in ensuring data security and have a significant impact on the accounting system as a whole.

DISCUSSION

The discussion of scientists is that information modernity is constantly transformed and modernized in every way. Today, the achievements of technical progress and digital innovation are accompanied by discussions, especially regarding the provision of cyber security in accounting, note the authors of Curti et al. (2023) and Boyko and Kryvko (2020).

We as the authors of this article support the opinion of Cheng et al. (2022) regarding the increased use of advanced information technology in recent years has brought many benefits but also created a number of challenges. In particular, the level of negative consequences of the processes of information storage and dissemination, as well as the number of new threats to information security, such as new forms of cyber attacks, has increased significantly.

Ensuring the stable and maximally effective functioning and development of any enterprise is the main task of protecting its economic information.

It is obvious that the most valuable economic information is accounting information, which characterizes all aspects of the enterprise's activities. Currently, most business entities have switched to computerized forms. It is worth paying attention to Balatska&Opirskyi's (2023) apt confirmation that computer systems also have certain risks, namely, they store and process large amounts of accounting information, and any failure can lead to excessive costs, inadequate revenues, loss of assets and sanctions. Therefore, the protection of accounting information at enterprises has great risks, but it is a primary task for the development of measures aimed at preserving information contained in the computer databases of the enterprise.

We, as authors, cannot disagree with Danyk et al (2019), who confirm this opinion and classify threats to computerized accounting information systems into two categories: active and passive threats. Active threats include computer fraud and computer sabotage. Passive threats include system errors (damage to individual hardware components) and catastrophic changes in the sphere of life support, social development, economy, education, business and management, the functioning of which has increased and is becoming more variable every year. The reasons for this growth are comprehensive convergence in the form of the process of spreading information and communication technologies and the Internet, globalization and the interpenetration of the digital ecosystem in all industries.

In this context, one cannot agree with the opinion of Grishko (2023) that the issue of cyber security affects the interests of state structures, since, in fact, it also concerns civil society and the private sector. And the lack of interaction between them makes it impossible to solve the issue of normative documents that solve the issue of cyber security.

Instead, we disagree with the opinion of Kurniawan and Mulyawan (2023) that the number of illegal financial transactions, theft, fraud, misuse of software and unauthorized access is increasing on the Internet, after which they were always and every time in their percentage.

In connection with the increase in the number of illegal financial transactions, fraud, abuse and falsification of software on the Internet, the priority in assessing the reliability of information protection systems should shift from traditional information security to cyber security.

Changes in cyber defence are necessary for the global economy, politics, and scientific and technological development, and, in particular, new approaches in various fields, namely in the accounting system.

In general, each of the researchers emphasizes the need to ensure the high efficiency of the cyber protection process in accounting.

CONCLUSIONS

In recent years, the rise in popularity of advanced information technology has brought many benefits to people, but it has also brought some problems. In particular, the negative impact of information on the process of its storage and distribution

has significantly increased, the number of new threats to information security, such as new forms of network attacks, is constantly increasing. Ensuring the stable and effective functioning and development of enterprises is the main task of protecting the economic information of the enterprise.

It is worth noting that the issue of the level of cyber security of accounting information in Ukraine is a problem at the company level. It should also be borne in mind that this is a national problem. The researched current state of cyber defence needs significant attention due to hostilities, pandemic and other imbalances in the country.

In the process of working on the article, we established that today in Ukraine, security software is used, in particular endpoint security software, virtual private networks (VPNS), SD-WANS and network access control (NAO), etc. The main advantages of such programs include cyber risks, prevention, and avoidance of consequences. At the same time, in the course of the research, deficiencies in the functioning of such programs were identified, the main of which are: destruction of information, errors in data entry, and violation of control limits. This leads to an imbalance of work.

We found that successful cyber-attacks on information data cost organizations a lot of money. It found that in 2022, USD 4.91 million was lost to phishing, USD 4.89 million - to business email compromise, USD 4.55 million - to third-party software vulnerabilities, USD 4.50 million - to stolen or compromised credentials, USD 4.18 million - an intruders. Therefore, it is important to allocate significant costs for the provision and operation of accounting security programs in Ukraine. The four most commonly used technologies for secure operations were identified as endpoint security software, virtual private networks (VPNS), SD-WANS, and network access control (NAO). The latest programs ensure the confidentiality, integrity, reliability and security of the data transmitted and significantly affect the successful work of accounting as a whole.

Thus, cybercrime is evolving every day, and threat analysis and modern tools are not keeping up. This makes it difficult to identify and maintain the cybersecurity of accounting information. Prospects for further research are to consider the problems and possible ways to solve them in the provision of a modern cyber security system for the protection of account data. These issues include social and behavioural issues, criminal activity in cyberspace, vulnerability and technical issues. They affect both the economic sector and others.

ADDITIONAL INFORMATION

AUTHOR CONTRIBUTIONS

Conceptualization: *Yatsko Maksym*
Data curation: *Svitlana Laichuk Yatsko, Liubov Koval*
Formal Analysis: *Olena Dovzhyk*
Methodology: *Yatsko Maksym, Serhii Harkusha*
Software: *Yatsko Maksym*
Resources: *Liubov Koval*
Supervision: *Svitlana Laichuk, Olena Dovzhyk*
Validation: *Svitlana Laichuk*
Investigation: *Svitlana Laichuk, Yatsko Maksym*
Visualization: *Yatsko Maksym*
Project administration: *Svitlana Laichuk*
Writing – review & editing: *Olena Dovzhyk*
Writing – original draft: *Svitlana Laichuk, Yatsko Maksym, Liubov Koval, Olena Dovzhyk, Serhii Harkusha*

REFERENCES

1. Abdullayeva, M., & Ataeva, N. (2022). Mortgage lending with the participation of the construction financing fund of the bank of the future. *Futurity Economics & Law, 2(1),* 35–44. https://doi.org/10.57125/FEL.2022.03.25.05
2. Balatska, V., & Opirskyy, I. (2023). Ensuring the confidentiality of personal data and supporting cyber security with the help of blockchain. *Electronic Professional Scientific Edition «Cybersecurity: Education, Science, Technique», 4*(20), 6–19. https://doi.org/10.28925/2663-4023.2023.20.619
3. Boyko, D. O., & Kryvko, K. G. (2020). Development of accounting in conditions of digitalization: theoretical aspects. In *Prospects for the development of accounting, auditing, taxation and of finance in conditions of digital transformation of the economy*

DOI: 10.55643/fcaptp.6.53.2023.4254

(pp. 10–12). Mykolayiv National Agrarian University. https://www.mnau.edu.ua/files/nauk_prof_konf/abstracts2020-18-05.pdf

4. Bushman, I. (2021). The development of the intellectual economy of the future: Trends, challenges of the future. *Futurity Economics & Law*, *1*(3), 33–42. https://doi.org/10.57125/FEL.2021.09.25.04
5. Cheong, A., Duan, H. K., Huang, Q., Vasarhelyi, M. A., & Zhang, C. A. (2022). The rise of accounting: Making accounting information relevant again with exogenous data. *Journal of Emerging Technologies, 19*(1), 1–20. https://doi.org/10.2308/jeta-10812
6. Curti, F., Gerlach, J., Kazinnik, S., Lee, M., & Mihov, A. (2023). Cyber risk definition and classification for financial risk management. *Journal of Operational Risk, 18*(2). https://ssrn.com/abstract=4474237
7. CyberEdge Group. (2022). *2022 Cyberthreat Defense Report*. https://cyber-edge.com/cyberthreat-defense-report-2022/
8. Danyk, Y. G., Vorobienko, P. P., & Chernega, V. M. (2019). *Fundamentals of cyber security and cyber defense.* O.S. Popov Odesa National Academy of Telecommunications. http://lib.istu.edu.ua/index.php?p=22&page=2&par=26&sort=title
9. Grigorevska, O. O. (2020). Protection of accounting information in terms of ensuring the cyber security of the enterprise. In *Achievements and prospects of modern scientific research* (pp. 582–584). Editorial EDULCP. https://er.knutd.edu.ua/handle/123456789/17377
10. Grishko, R. S. (2023). Cyber risks and key issues of cyber protection of the financial sector. In *Proceedings of the 10th All-Ukrainian scientific and technical conference of higher education graduates based on the results of research in 2022* (pp. 137−139). Dmytro MotornyiTavria State Agrotechnological University. http://elar.tsatu.edu.ua/bitstream/123456789/16548/3/Zbirka_%20FEB.pdf#page=137
11. Harkusha, S. (2019). Features of storage, archiving and protection of information in the process of organizing accounting. *Market Infrastructure*, 30, 478-485. https://repo.snau.edu.ua/bitstream/123456789/7038/1/%D0%93%D0%B0%D1%80%D0%BA%D1%83%D1%88%D0%B0.pdf
12. Harkusha, S. (2021). Protection of information and fraud prevention in the field of accounting support. *Economy and Society*, 33. https://doi.org/10.32782/2524-0072/2021-33-34
13. Kafi, M. A., & Akter, N. (2023). Securing financial information in the digital realm: Case studies in cybersecurity for accounting data protection. *American Journal of Trade and Policy, 10*(1), 15–26. http://surl.li/ldwjt
14. Kurniawan, Y., & Mulyawan, A. (2023). The role of external auditors in improving cybersecurity of the companies through internal control in financial reporting. *Journal of System and Management Sciences, 13*(1), 485–510. http://www.aasmr.org/jsms/Vol13/No.1/Vol.13.No.1.26.pdf
15. Lehenchuk, S., Vygivska I., & Hryhorevska, O. (2022). Protection of accounting information in the conditions of cyber security. *Problems of Theory and Methodology of Accounting, Control and Analysis*, 2(52), 40–46. https://doi.org/10.26642/pbo-2022-2(52)-40-46
16. Liubymov, M., Pedchenko, N., Artiukh-Pasiuta, O., Milka, A., & Prokhar, N. (2022). Development of the organization of accounting in Ukraine under modern conditions. *Scientific Bulletin of Poltava University of Economics and Trade. A Series of "Economic Sciences", 2*(106), 42-47. https://doi.org/10.37734/2409-6873-2022-2-6
17. Martsenyuk, V., Sverstyuk, A., Andrushchak, I., Chudovets, V., & Koshelyuk, V. (2021). Aspects of protection of accounting data in the conditions of use of innovation and information technologies. *Computer-Integrated Technologies: Education, Science, Production, 42*, 172–176. https://doi.org/10.36910/6775-2524-0560-2021-42-25
18. Muravskyi, V. V., & Pitel S. V. (2020). Hypothesis about the accounting platform of the enterprise cyber security organization. *The current state and prospects of development of the accounting information system in Ukraine, 1*, 140–141. http://dspace.wunu.edu.ua/bitstream/316497/42395/1/%D0%9C%D1%83%D1%80%D0%B0%D0%B2%D1%81%D1%8C%D0%BA%D0%B8%D0%B9.pdf
19. Muravskyi, V. V., Farion, V. Ya, & Hrytsyshyn, A. V. (2021). Quality of accounting information and principles of its cyber protection. *Scientific Notes of Ostroh Academy National University, "Economics" series, 23*(51), 103-109. https://journals.oa.edu.ua/Economy/article/view/3405/3102
20. Muravskyi, V. V., & Shevchuk, O. A. (2021). Principles of accounting in the implementation of cyber protection of enterprises. *Transformation of accounting, analysis, and control in the context of socio-economic challenges,* 1, 230–233.

http://dspace.wunu.edu.ua/bitstream/316497/45553/1/%D0%9C%D1%83%D1%80%D0%B0%D0%B2%D1%81%D1%8C%D0%BA%D0%B8%D0%B9%20%D0%92.%20%D0%92..pdf

21. Muravskyi, V., Shevchuk, O., Muravskyi, V., & Lapshinskyi, V. (2022). Improving the accounting policy of the enterprise for its cyber protection. *Herald of Economics*, *1*, 97–109. https://doi.org/10.35774/visnyk2022.01.097

22. Novitsky, V. (2020). Main menaces of information leakage of a commercial secret on the internet and analysis of the practice of protection of commercial secrets in the EU member states. *International scientific journal "Internauka." Series: "Juridical Sciences", 1*(28), 28–44. https://paper.researchbib.com/view/paper/278161

23. NCSI. (2023). *Top 10*. https://ncsi.ega.ee/

24. Omelchyk, O., Ivanashko, O., Sipko, L., Virna, Z., Saienko, V., & Tolchieva, H. (2022). Economic behavior of consumers during instability. *AD ALTA: Journal of Interdisciplinary Research*, *12*(02), 89–95. https://www.researchgate.net/publication/362850975_ECONOMIC_BEHAVIOR_OF_CONSUMERS_DURING_INSTABILITY

25. Otonne, A., Melikam, W., & Ige, O. T. (2023). Adoption of financial technology and performance of deposit money banks in Nigeria. *Futurity Economics & Law*, *3*(2), 95–114. https://doi.org/10.57125/FEL.2023.06.25.07

26. Popivniak, Yu. M. (2019). Cyber security and protection of accounting data in conditions of application of the latest information technologies. *Business Inform, 8*, 150–157. https://doi.org/10.32983/2222-4459-2019-8-150-157

27. Savkiv, U. S., & Kuzmin, T. L. (2023). Improvement accounting and reporting in the digital economy. *The Actual Problems of Regional Economic Development, 2*(19), 87–95. https://doi.org/10.15330/apred.2.19.87-95

28. Shyrokopoias, O. Yu. (2020). Reflection of business security services on accounting and reporting accounts. *Economic Scope*, *153*, 128-133. http://srd.pgasa.dp.ua:8080/xmlui/handle/123456789/5427

29. Skrypnyk, M. I., & Grigorevska, O. O. (2020). Organization of accounting information protection in terms of cyber security. *Scientific Notes of Ostroh Academy National University, "Economics" series, 19*(47), 95–102. https://er.knutd.edu.ua/bitstream/123456789/17091/1/3057.pdf

30. Spilnyk, I., & Palukh, M. (2019). Accounting in the digital economy conditions. *The Institute of Accounting, Control and Analysis in the Globalization Circumstances*, 1-2, 83–93. https://doi.org/10.35774/ibo2019.01.083

31. Tarasenko, I., Saienko, V., Kirizleyeva, A., Vozniakovska, K., Harashchenko, L., & Bodnar, O. (2022). Comparative characteristics of the banking sector in Eastern Europe. *International Journal of Computer Science and Network Security, 22*(1), 639–649. https://doi.org//10.22937/IJCSNS.2022.22.1.84

32. Tesak, O. V. (2022). Accounting policy of the enterprise: Analysis of the risks of using blockchain technology in accounting and auditing. *Academic Visions*, 13. https://doi.org/10.5281/zenodo.7331052

33. Tomislav, K. (2018). The concept of sustainable development: From its beginning to the contemporary issues. *Zagreb International Review of Economics & Business, 21*(1), 67-94. https://doi.org/10.2478/zireb-2018-0005

34. Vasylyshyn, S. I., Hnatyshyn, L. B., & Prokopyshyn, O. S. (2022). Economic security as a component of accounting and analytical support for enterprise management: Theoretical aspect. *Taurida Scientific Herald. Series: Economics, 14*, 110-120. https://doi.org/10.32782/2708-0366/2022.14.14

35. Vdovichena, O., Vidomenko, O., Tkachuk, S., Zhuzhukina, N., & Lukianykhina, O. (2022). The use of information in the world economy: globalization trends. *Futurity Economics & Law, 2*(4), 4–11. https://doi.org/10.57125/FEL.2022.12.25.01

36. Verbivska, L., Al-Ababneh, H. A., Korbutiak, A., Panchenko, A., & Ippolitova, I. (2022). The impact of e-business on entrepreneurship development in the context of COVID-19. *WSEAS Transactions on Business and Economics*, *19,* 1824–1838. https://wseas.com/journals/bae/2022/d325107-1834.pdf

37. Viter, S. A., & Svitlyshyn, I. I. (2017). Protection of accounting information and cyber security of the enterprise. *Economy and Society*, *11*, 497–502. https://economyandsociety.in.ua/journals/11_ukr/80.pdf

38. Vysochan, O., & Hrytselyak, U. (2020). Prerequisites and problems for the digital transformation of the accounting and communication process. *Scientific View: Economics and Management, 3*(69), 132–138. https://doi.org/10.32836/2521-666X/2020-69-22

DOI: 10.55643/fcaptp.6.53.2023.4254

Лайчук С., Яцко М., Коваль Л., Довжик О., Гаркуша С.

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В БУХГАЛТЕРСЬКОМУ ОБЛІКУ В ЕПОХУ ЦИФРОВОЇ ЕКОНОМІКИ

У дослідженні підкреслюється важливість захисту даних бухгалтерського обліку в кіберпросторі, а саме впровадження й удосконалення комп'ютерних систем, які дають змогу вирішити проблему захисту інформації бухгалтерського обліку та інших ресурсів державного значення. Інформаційна безпека є актуальною проблемою сьогодення, оскільки кількість загроз в інформаційно-комунікаційному просторі щоразу збільшується. Провідну роль у забезпеченні інформаційної безпеки в бухгалтерських системах відіграють різноманітні сучасні програми, основним завданням яких є забезпечення конфіденційності, цілісності та автентичності переданих даних. Тому метою дослідження є виокремлення значення та ролі застосування безпечної системи для захисту від кіберзагроз у бухгалтерському обліку в сучасних умовах. Результати дослідження відображають процес кіберзахисту за допомогою програм захисту бухгалтерського обліку, їхню суть, ознаки, показники, перспективи застосування зараз і в майбутньому. Інформаційні системи бухгалтерського обліку формуються з конфіденційної та особистої інформації, яка може бути витоком, якщо її не захистити. Несанкціоноване використання інформації, що генерується бухгалтерськими системами, може призвести до таких негативних наслідків, як втрата інформації, некоректне введення даних та неправомірне використання конфіденційної інформації. Неналежний рівень інформаційної безпеки підвищує ймовірність маніпуляцій, фальсифікації або зміни бухгалтерських записів. Захист даних, що генерується бухгалтерськими системами, має вирішальне значення, а забезпечення її безпеки є пріоритетом для багатьох компаній.

Ключові слова: інформаційні війни, кіберзагрози, кібератака, інформаційна безпека, стратегії кібербезпеки, можливості та ризики

JEL Класифікація: M40, M15, C87