DOI: https://doi.org/10.36910/6775-2524-0560-2021-42-25
УДК: 004.05(075.8)
[1]**Марценюк Василь Петрович**, д.т.н., професор,
https://orcid.org/0000-0001-5622-1038
[2]**Сверстюк Андрій Степанович**, д.т.н., професор,
https://orcid.org/0000-0001-8644-0776
[3]**Андрущак Ігор Євгенович**, д.т.н., професор,
https://orcid.org/0000-0002-8751-4420
[3]**Чудовець Віталій Васильович,** к.е.н., доцент,
https://orcid.org/0000-0001-6043-479X
[3]**Кошелюк Віктор Андрійович,** к.т.н., доцент,
https://orcid.org/0000-0002-4136-5087
[1]Університет Бєльсько-Бяли, Польща
[2]Тернопільський національнийний медичний університет імені І.Я. Горбачевського, Україна
[3]Луцький національний технічний університет, Україна

ASPECTS OF PROTECTION OF ACCOUNTING DATA IN THE CONDITIONS OF USE OF INNOVATION AND INFORMATION TECHNOLOGIES.

Марценюк В.П., Сверстюк А.С., Андрущак І.Є., Чудовець В.В., Кошелюк В.А. Аспекти захисту бухгалтерських даних в умовах використання інноваційно-інформаційних технологій. У статті розглядається проблеми сучасного стану кібербезпеки і ідентифікації кіберзагроз у сфері застосування облікових даних, формулювання заходів з мінімізації ризиків викрадення, пошкодження або втрат конфідентційної інформації бухгалтерського обліку в кіберсередовищі його вікористання та ведення.
Ключові слова: кібербезпека, кіберсередовище, захист бухгалтерської інформації, кіберзагроза, кіберзахист.

Марценюк В.П., Сверстюк А.С., Андрущак И.Е., Чудовець В.В., Кошелюк В.А. Особенности технологии защиты от несанкционированно установленных мониторинговой программных продуктов. В статье рассматривается проблемы современного состояния кибербезопасности и идентификации киберугроз в сфере применения учетных данных, формулирование мер по минимизации рисков краж, повреждения или потери конфиденциальной информации бухгалтерского учета в киберпространстве его использования и ведения.
Ключевые слова: кибербезопасность, киберсреда, защита бухгалтерской информации, киберугрозы, киберзащита.

Martsenyuk V.P., Sverstyuk A.S., Andrushchak I.Ye., Chudovets V.V., Koshelyuk V.A. Aspects of protection of accounting data in the conditions of use of innovation and information technologies. The article examines the current state of cybersecurity and identification of cyber threats in the use of credentials, the formulation of measures to minimize the risk of theft, damage or loss of confidential accounting information in the cyber environment of its use and maintenance.
Key words: cybersecurity, cyberenvironment, protection of accounting information, cyberthreat, cybersecurity.

Formulation of the problem. The system of cyber protection of accounting information is a set of measures at the state level and at the level of an individual enterprise, designed to ensure the security and protection of such information, as well as the automated accounting system at the enterprise as a whole, from cyber threats. With general and specific threats, we single out the means of protection against them of a general and specific nature. At the same time, we divide the whole set of them into organizational, technical, personnel and legal measures. The key here is the availability of funds for the implementation of these measures - the larger the budget, the higher the chances of minimizing cyber risks (provided the successful use of financial resources).

Note that one of the main difficulties in combating cyber threats is that, according to Telstra, 78% of companies today do not have a clear plan to respond to possible threats. To protect against cyber threats, companies most often use network antiviruses (63.9%), network access control (59.8%), SSL / TLS devices (platforms) for decryption (59.4%) and intrusion detection (prevention) systems. Outsourcing of individual information security functions (intrusion testing, threat analysis, real-time network security monitoring, etc.) is also considered as an option. Prospects for further research in this area are the search for criteria and evaluation of the success of the implementation of measures to protect accounting information and ensure its cybersecurity [1].

Analysis of research. The rapid development of modern information technologies, which began in the late XX - early XXI centuries, contributed to their introduction into almost all spheres of human life and mass (often even uncontrolled) use, as well as the formation of a single innovative information and digital space. At the same time, the number of offenses, abuses and other cyber threats aimed at various aspects of the activities of various enterprises operating in each of these spaces has grown quite rapidly. Information about all the facts of economic activity of the enterprise, which is formed in the system of its accounting, is

characterized by a high degree of value and is a guarantee of stability, development and efficiency of such enterprise, but only if it is reliably protected. However, total automation, which has not bypassed the field of accounting and provides for the introduction of specialized innovative modern technologies and programs for its maintenance, despite the undeniable advantages, threatens the leakage of certain information, hacking attacks, hacking information networks, various frauds, etc. all accounting data that is processed and stored in a digital environment. Under such conditions, the enterprise provides a certain type of information security - cybersecurity.

Presentation of the main material and the justification of the results. Problems of cybersecurity (identification and grouping of cyber threats, taking measures to minimize or eliminate them, building an adequate system of protection of accounting information at the enterprise) are currently little studied. Many of them, against the background of intensifying competition and the invention of new information technologies, remain unresolved and require close consideration and attention of scientists, especially in the context of taking into account the domestic peculiarities of accounting in enterprises. First of all, we note that the deepening of automation of accounting - an inevitable and, in general, a positive phenomenon, because it can significantly save enterprise resources, improve information processing, flexibility, mobility, innovation and efficiency of the accountant, accelerate its digital transformation, provide access to a wide range of modern accounting programs, cloud solutions and other information technology tools, etc. One of the downsides of using computer technology is the vulnerability of credentials to cyber threats, which can be minimized by using the right security practices. In general, the composition and scope of accounting data, which are considered a trade secret at the enterprise, as well as the procedure for their protection, the head (owner) of the enterprise determines independently within the current legislation, because [2].

Security is defined as the degree of protection against criminal activity, danger, damage and / or loss. Analyzing the research of scientists, along with cybersecurity we meet the term "information security". We agree with the approach of R. von Solms and J. van Niekerk, who insist on the differences between these concepts. And cybersecurity goes beyond simple information security and provides security for various assets of the enterprise (not only information), which are at risk when using such an enterprise computer systems and telecommunications networks. At the same time, information security, as a process of maintaining the confidentiality, integrity and accessibility of information, along with electronic information, includes the protection of information resources that are processed and stored without the use of computer technology. In our study, we consider cybersecurity, and only in the field of protection of accounting information, which is not just stored on a separate user's computer, but circulates in cyberspace - an environment consisting of information systems around the world, including networks that connect these systems.

A survey of IT security workers conducted by the Cyber Edge Group found that in 2019, an average of 78% of cyber threats were successful (about 63% of all businesses were exposed to such threats), with Spain leading the way (93.7%), Saudi Arabia (91.5%). The main sources of danger today are malware, phishing attacks, extortion programs, abuse related to user accounts (including identity theft), denial of service (DoS-/DDoS-attacks), web attacks-applications, spam, botnets, data breaches, insider threats, physical manipulation (damage, theft, data loss), information leakage, cryptojacking (a new type of threat, which is the unauthorized use of someone else's computer to extract cryptocurrency), cyber espionage and , and suppliers of cyber security as of the second quarter of 2018 - Cisco, Palo Alto Networks, Fortinet, Sheck Point [3].

Websites and web applications, servers (physical and virtual) and data warehouses are the most vulnerable to cyber threats in enterprises, and laptops and mobile devices are the least protected. An important indicator of information security in the cyber environment of a country is the Global Cybersecurity Index (which is calculated on the basis of legal, technical, organizational indicators, as well as capacity building and cooperation). Ukraine lags behind the leaders in this indicator and occupies only 54 positions among 175 countries, being approximately on a par with Uzbekistan, Moldova, Azerbaijan. In general, the number of detected and registered cybercrimes in Ukraine in 2018, compared to the previous year, decreased slightly.

This was mainly due to the improvement of the situation in Kyiv and Kyiv region. Instead, in such oblasts as Zaporizhia, Odesa, and Mykolayiv, the number of cybercrime crimes has increased significantly. In general, Mykolaiv, Odesa and Kyiv became the three regions with the highest rate of cybercrime in Ukraine in 2018. According to gender, 67% of domestic cybercriminals are men and, accordingly, 33% of cybercrimes are committed by women. In terms of types of cybercrime (according to the articles of the Criminal Code of Ukraine), their distribution is as follows: 63% - fraud, 35% - unauthorized interference with computers, 2% - infringement of copyright and related rights.

Note that in order to effectively combat cyber threats, including in the field of protection of accounting data in enterprises, it must be one of the priorities of public policy, approved at the legislative level. The main domestic regulations on the regulation of issues related to the safe operation of cyberspace participants are:

1) Law of Ukraine "On Basic Principles of Cyber Security of Ukraine" (dated 05.10.2017 No. 2163-VIII);

2) Law of Ukraine "On Ratification of the Convention on Cybercrime" (dated 07.09.2005 No 2824-IV);

3) Cyber Security Strategy of Ukraine (decision of the National Security and Defense Council of Ukraine of January 27, 2016);

4) "On threats to cybersecurity of the state and urgent measures to neutralize them" (decision of the National Security and Defense Council of Ukraine dated 29.12.2016);

5) General requirements for cyber protection of critical infrastructure facilities (Resolution of the Cabinet of Ministers of Ukraine of June 19, 2019 No. 518).

At present, the Ukrainian regulatory framework is characterized by a lack of system, imperfection, inconsistency, divergence of approaches, fiscal orientation, moral obsolescence and needs further development and improvement in the use of digital technologies and protection of participants in the cyber environment.

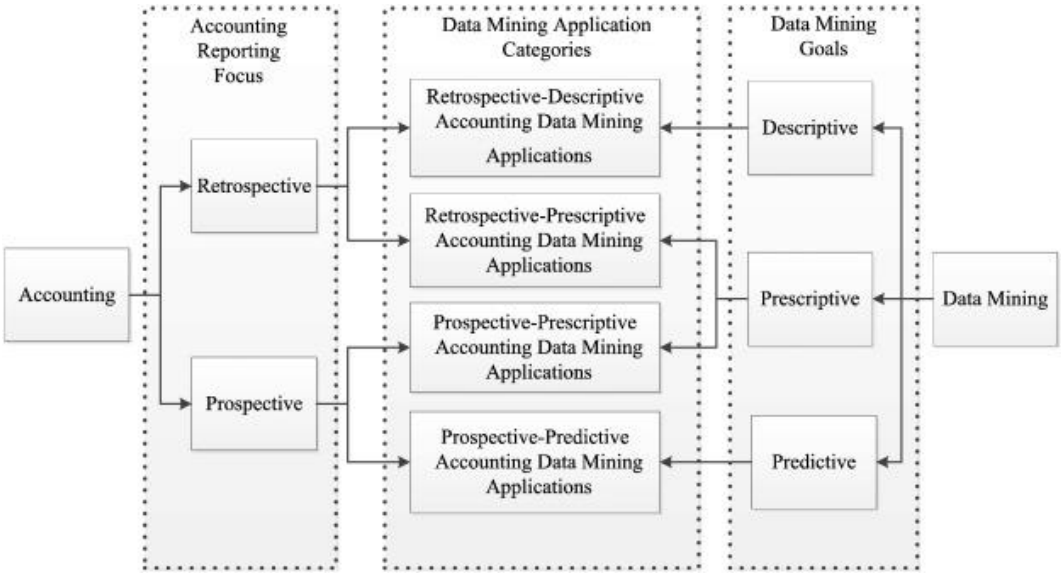
According to a study by Ernst & Young, the average loss of data integrity in the world in 2017 was $ 3.62 million. USA. At the same time, accounting and financial information ranks second in terms of attractiveness to cybercriminals after information about customers (12% of all cyber threats). It is a mistake to think that this only applies to large and medium-sized enterprises - the data of all businesses without exception are exposed to cyber threats, moreover, about 80% of all crimes in this area concern small enterprises.

Note that in order to form an effective system of measures to minimize cyber threats and adequate protection of accounting information, it is necessary, first of all, to determine the understanding of the concept of "threat". In studies of M.M. Alani finds the following interpretation of a threat: "a potential encroachment on security that exists in the presence of circumstances, opportunities, actions or events that may violate it and cause harm." O.A. Yevtushevskaya defines this term as "potential or actually possible actions in relation to information resources that lead to misappropriation of information." Derived from the threat is a cyber threat, which (considering the approaches in the economic literature and legislation) in the context of our study means an existing or potential event that threatens the participants of cyberspace in the field of accounting information system, leads to loss, damage, destruction or unauthorized use of accounting information [4].

Reasonable grouping of cyber threats is the next step to build a comprehensive system of cybersecurity of accounting information in the enterprise. O.A. Yevtushevskaya divides threats into external ones, the sources of which are competitors, criminal groups of hackers and terrorist groups, political structures, etc., and internal ones, personified by the administration and staff of the enterprise. In turn, internal threats researchers divide into (Pic.1):

1) computer fraud, computer forgery, providing confidential information to competitors;

2) technical threats, threats of obtaining false information, disclosure, other threats of imperfect organization. V.A. Let and V.V. Suppose that the list is properly supplemented by the type of threats that are associated with intentional errors that occur outside the business.



(Pic.1) Mining application in accounting

The source of threat in this case may be, for example, a business partner or a developer of specialized software. In addition to the classification of threats to accounting information by the source of their occurrence, which is found in the works of scientists most often, scientists also identify the following signs of grouping hazards:

- by manifestation and consequences;
- by type; on purpose;
- by the nature of occurrence;
- information technology;
- by object of influence;
- by cause;
- by time; by probability.

In parallel with the definition and classification of cyber threats, as well as the identification of ways in which data security can be compromised in the enterprise, it is also important to outline the main prerequisites for the occurrence of such threats to accounting information [5]:

1) use of unlicensed or unverified software for accounting and reporting, neglect of its vulnerabilities;
2) use of weak tools for authentication of users of accounting information;
3) neglect of the rules of protection of work computers or other devices from which access and work with credentials take place;
4) use of working devices for non-working purposes;
5) lack of basic knowledge of cybersecurity of accountants;
6) incorrect prioritization and lack of proper support from the management system of the enterprise;
7) neglect of the rules of storage of accounting data and their periodic redundancy;
8) ignoring the existing risks and negative experiences of other market participants;
9) the absence of an appropriate specialist in the protection of accounting information at the enterprise;
10) a long list of persons who have access to data, the lack of delimitation of user rights;
11) complex tax and business environment of the enterprise.

World experience shows that the biggest problems in the use of effective means of combating cyber threats today are the difficulties of their implementation and integration, lack of relevant specialists (low level of awareness of cybersecurity), financial resources, effective market solutions, support from the enterprise management system, continuous improvement ways to perform malicious actions, etc. To these we will add the limitations typical of the domestic business environment: imperfect legislation in the field of cybersecurity, political risks, corruption and protectionism. It should be noted that the largest funds for cybersecurity today are allocated by companies from Mexico (15.9% of the IT budget), Brazil (15.9%) and South Africa (14.9%).

L. Kolobov and I. Kolesnikov divide measures to protect confidential information into legal, physical, technical and psychological, O.A. Yevtushevskaya - for physical, hardware, software and cryptographic, A.P. Wild allocates organizational and technical, organizational and regime measures for the organization of protection and security of accounting data and personnel work. Similar to the latter approach is followed by S.A. Viter and I.I. Svitlyshyn, which distinguish organizational measures, technical measures and personnel work. According to these authors, the system of these measures must meet the criteria of software support, protection of information confidentiality, personal responsibility, secrecy, complexity, effective control of access to credentials. V.A. Starling to the elements of protection of accounting information includes legal, technical, software and organizational. In this case, "the ratio of elements and their content provide the individuality of the information protection system of the enterprise and guarantee its reliability." A slightly different view - in I.L. Grabchuk, who distinguishes between the means of protection of accounting information in electronic form means of logical and physical security [6].

Following the world trends, the accounting of more and more domestic enterprises is subject to automation and digitalization using such modern tools and technologies as blockchain, cloud and fog technologies, artificial intelligence, Internet of Things, mobile computing, machine learning and more. Each of these technologies, in addition to the general list of threats listed above, is characterized by specific risks to accounting information, which are a consequence of the nature and characteristics of the operation of a technology. For example, when using mobile devices for accounting, the specific risks will be: poor awareness and culture of using devices, their loss and theft; inability of network engineers to quickly eliminate vulnerabilities; purchase of a mobile device with pre-installed malware (every 36th mobile device is exposed to such a threat; problems of interaction with other programs. If we are talking about the Internet of Things, then the problems will be the identification of suspicious traffic, ensuring compliance with current security controls updating a large number of devices connected to the Internet, lack of properly qualified personnel, tracking access to data.

Cloud technologies for accounting and reporting are also not completely safe. Specific threats to accounting information here may be the inability to use previous versions of software, high dependence on the quality of service provision by providers, uncertainty about privacy and ownership of data in the cloud (lack of appropriate legal protection of information rights in the cloud) sources of threats. Speaking of blockchain technology, which predicts a great future in accounting and auditing, specific threats to information due to the peculiarities of this technology are the low level of privacy and confidentiality of enterprise data, lack of legally approved person responsible for maintaining a distributed database of operations, overload storage devices as a consequence of the inevitable growth of its volume [7].

Conclusion and prospects for further research

In today's world of advanced technologies, the introduction of the latter in the accounting process will not surprise anyone. In this case, the accounting information that is formed in this process - a special resource that requires careful protection, because its safe use depends on the information security of the entire enterprise. The results of the study show that today in the world cyber threats are exposed to a large number of enterprises, regardless of their size and type of activity. In recent years, cyberattacks have also become more frequent in Ukraine, which are due, among other things, to national economic characteristics, such as lack of proper legal framework, large share of enterprises using unlicensed accounting software products, neglect of automated workplace protection rules, lack of accounting specialists knowledge of the basics of cybersecurity. To minimize the negative impact of cyber threats, a comprehensive system of general and specific measures of organizational, technical, personnel and legal nature is proposed. At the same time, the criteria for evaluating the success of the implementation of these measures is the direction of our further research.

References

1. Alani M. M. Elements of Cloud Computing Security. A Survey of Key Practicalities. Switzerland : Springer, 2016. 55 p.
2. Kolobov L. Trade secret and the protection of trade secrets. / L. Kolobov, I. Kolesnikov // Civil law and process. 2016. No 5. S. 8–13.
3. Bawaneh S. S. Information security for organizations and accounting information systems. A Jordan banking sector case. International Review of Management and Business Re search. 2014. Vol. 3. Issue 2. P. 1174–1188.
4. Von Solms R., van Niekerk J. From information security to cyber security. Computers & Security. 2013. Vol. 38. P. 97–102 URL: https://www.sciencedirect.com/science/article/ pii/S0167404813000801?via%3Dihub
5. Wind SA Protection of accounting information and cybersecurity of the enterprise / S.A. Wind, II Svitlyshyn // Economy and Society. 2017. Vip. 11. S. 497–502.
6. National cyber security strategy and 2013–2014 action plan / Ministry of Transport, Maritime Affairs and Communications; Republic of Turkey. URL: https://sherloc.unodc. org/res/cld/lessons-learned/national_cyber_security_strategy_and_2013-2014_action_plan_html/National_Cyber_Secu- rity_Strategy_and_2013-2014_Action_Plan.pdf
7. ISO / IEC 27001: 2013. Information Technology. Protection methods. Information security management systems. Requirements / per. from English. A. Gorbunov. URL: https://pqm-online.com/assets/files/pubs/translations/std/iso- mek-27001-2013 (rus) .pdf