**УДК 657.6:008**

**JEL classification: M41, M42, D24**

**DOI: https://doi.org/10.35774/visnyk2021.02.129**

**Volodymyr MURAVSKYI,**
Doctor of Economics, Associate Professor
Professor of the Department of Accounting and Taxation,
West Ukrainian National University,
st. Lvivska, 11, Ternopil, 46020, Ukraine,
e-mail: vvvmur@gmail.com
ORCID ID: https://orcid.org/0000-0002-6423-9059

**Nataliia POCHYNOK,**
Phd, Associate Professor,
Acting Head of the Department of Accounting and Taxation,
West Ukrainian National University,
st. Lvivska, 11, Ternopil, 46020, Ukraine,
e-mail: natapochynok@gmail.com
ORCID ID: https://orcid.org/0000-0003-4416-3680

**Volodymyr FARION,**
Phd, Associate Professor,
Associate Professor of the Department of Accounting and Taxation,
West Ukrainian National University,
st. Lvivska, 11, Ternopil, 46020, Ukraine,
e-mail: farionvolodymyr@gmail.com
ORCID ID: http://orcid.org/0000-0001-9994-3073

# CLASSIFICATION OF CYBER RISKS IN ACCOUNTING

Muravskyi, V., Pochynok, N., Farion, V. (2021). Klasyfikatsiia kiberryzykiv u bukhhalterskomu obliku [Classification of cyber risks in accounting]. *Visnyk ekonomiky – Herald of Economics*, 2, 129–144. DOI: https://doi.org/10.35774/visnyk2021.02.129

Муравський В., Починок Н., Фаріон В. Класифікація кіберризиків у бухгалтерському обліку. *Вісник Економіки.* 2021. Вип. 2. С. 129–144. DOI: https://doi.org/10.35774/visnyk2021.02.129

***Annotation.***

***Introduction.*** *The complexity of information processes in accounting and the improvement of computer and communication technologies led to the variation of accounting information cyber threats. The traditional classification of cyber threats does not include*

© Volodymyr Muravskyi, Nataliia Pochynok, Volodymyr Farion, 2021.

*the multifaceted nature of accounting, and therefore is uninformative for the purposes of organizing effective cybersecurity of enterprises.*

***Purpose.*** *The main aim is to improve the classification of cyber risks through the generalization and systematization of cyber threats relevant to accounting information.*

***Methods.*** *In the process of the systematization of variable cyber threats in accounting, general scientific empirical, logical and historical methods of cognition of socio-economic processes were used. The article is based on general methods of research of socio-economic information from the standpoint of accounting and cybersecurity. The information basis of scientific research is historical resources about the cyber threats classification, scientific works of domestic and foreign scientists about dividing threats of accounting into types.*

***Results.*** *It is proved that effective cyberprotection of enterprises requires prompt and adaptive consideration of variable cyber threats in accounting. The classification of cyber threats of accounting information has been improved by distinguishing classification criteria: randomness, purposefulness, information and financial interest, territoriality, source, origin, objectivity, objectivity, scale, form of implementation, criminality, aspect, prolongation, latency, and probability. The importance of using the above classification of cyber risks, which comprehensively characterizes the cyber threats of accounting information, for the purposes of developing measures to prevent, avoid and eliminate potential consequences.*

***Discussion.*** *It is important to improve the classification of accounting information users for organize the enterprises cybersecurity, which requires further research and development of an actions set to ensure cyberprotection of the accounting system.*

***Keywords:*** *accounting, cybersecurity, classification of cyber threats, cyber risks of accounting information.*

**Formulas: 0, fig.: 2, tabl.: 1, bibl.: 22.**

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

**Наталія ПОЧИНОК,**
кандидат економічних наук, доцент,
виконуючий обов’язки завідувача кафедри обліку і оподаткування,
Західноукраїнський національний університет,
вул. Львівська, 11, м. Тернопіль, 46020, Україна,
e-mail: natapochynok@gmail.com
ORCID ID: https://orcid.org/0000-0003-4416-3680

**Володимир ФАРІОН,**
кандидат економічних наук, доцент,

доцент кафедри обліку і оподаткування,
Західноукраїнський національний університет,
вул. Львівська, 11, м. Тернопіль, 46020, Україна,
e-mail: farionvolodymyr@gmail.com
ORCID ID: http://orcid.org/0000-0001-9994-3073

# КЛАСИФІКАЦІЯ КІБЕРРИЗИКІВ У БУХГАЛТЕРСЬКОМУ ОБЛІКУ

***Анотація***

***Вступ.*** *Ускладнення інформаційних процесів в бухгалтерському обліку та удосконалення комп'ютерно-комунікаційних технологій призвели до варіювання кіберзагроз облікової інформації. Традиційна класифікація кіберзагроз не враховує багатоаспектність бухгалтерського обліку, а тому є малоінформативною для цілей організації ефективного кіберзахситу підприємств.*

***Мета статті*** *полягає в удосконаленні класифікації кіберризиків через узагальнення та систематизацію кіберзагроз, актуальних для облікової інформації.*

***Методи.*** *У процесі дослідження систематизації варіативних кіберзагроз у бухгалтерському обліку застосовані загальнонаукові емпіричні, логічні та історичні методи пізнання соціально-економічних процесів. Наукова стаття ґрунтується на базі загальних методів вивчення соціально-економічної інформації з позиції обліку та кібербезпеки. Інформаційною основною наукового дослідження є історичні джерела, що стосуються класифікації кіберризиків, наукові напрацювання вітчизняних та зарубіжних учених щодо поділу ризиків, що загрожують обліковій інформації, на види тощо.*

***Результати.*** *Доведено, що для ефективного кіберзахисту підприємств необхідне оперативне та адаптивне врахування варіативних кіберзагроз у бухгалтерському обліку. Удосконалено класифікацію кіберзагроз облікової інформації  за рахунок виокремлення класифікаційних критеріїв: випадковості, цілеспрямованості, інформаційного та фінансового інтересу, територіальності, джерела виникнення, походження, об'єктності, предметності, масштабності, форми реалізації, кримінальності, аспектності, пролонгованості, латентності, ймовірності, наслідків. Обґрунтовано важливість використання наведеної класифікації кіберризиків, яка всебічно характеризує кіберзагрози облікової інформації, для цілей вироблення заходів їхнього попередження, уникнення та усунення потенційних наслідків.*

***Перспективи.*** *З метою організації кібербезпеки підприємств важливим є удосконалення класифікації користувачів облікової інформації для цілей врахуванням варіативності кіберзагроз, що потребує подальших досліджень та вироблення комплексу дій із забезпечення кіберзахисту системи обліку.*

***Ключові слова:*** *облік, кібербезпека, класифікація кіберзагроз, кіберризики облікової інформації.*

**Формул: 0; рис.: 2; табл.: 1; бібл.: 22.**

**Introduction.** The digitalization of socio-economic processes has led to an increase in cyber threats. Since the accounting system is the generator of most economic processes in the enterprise, what cybersecurity requires foremost is accounting information. The variability of cyber threats is growing because of the increasingly complex accounting processes and improvements in computer communication processes. Theft of accounting data, especially that pertaining to trade secrets, has been the most common manifestation of external cyber threats. Internal threats to enterprise informational security are associated with malicious manipulations of accounting data aimed at gaining economic benefits or concealing certain actions or events.

The development of electronic communications has contributed to the spread of computer viruses geared towards harming the accounting system and enterprise management. The number of cyber threats associated with the installation of malicious software to gain unauthorized access to accounting data has gradually risen. Increasingly, the accounting system is becoming the target of cyber threats not only in its capacity as a communication channel for access to critical infrastructure of the enterprise, but also as the method of processing and transmitting accounting information. Popularity of social networks and messengers leads to an increased likelihood of accounting data being leaked to third parties. Consequently, direct cyberattacks against the enterprise accounting system are becoming more frequent. Fraudulent actions of third parties related to obtaining illegal economic benefits have become even more widespread.

Improvement in the methods of executing hybrid conflicts alone results in more complex, permanent, extensive and varied cyber threats. The success of cyberattacks is ensured by using a set of different cyber threats aimed at maximizing the damage done to a business entity. Such threats to information security are detected continuously, which requires the enterprise to create a specialized unit or hire staff specializing in cyber security and integrate them into the organizational structure. Therefore, ensuring effective cyber security of accounting data necessitates the study of cyber risks grouped according to various classification features.

**Literature Review.** Scientific and journalistic sources of information on cybersecurity of enterprises use a generally accepted classification of cyber risks. Namely, commonly recognized types of cyber risks include malicious software and viruses, web attacks, web application attacks, phishing, hardware failure, spam, botnet attacks, data breaches, insider threats, data leakage, information leakage, identity theft, cryptojacking, extortionist programs, cyber espionage and others.

For example, the journalistic indexing publishing house «The 2019 Kearney Global Services Location Index» uses a simplified classification of cyber risks into: Hacking, Malware, Social, Error, Physical, Misuse [1] (Fig. 1).

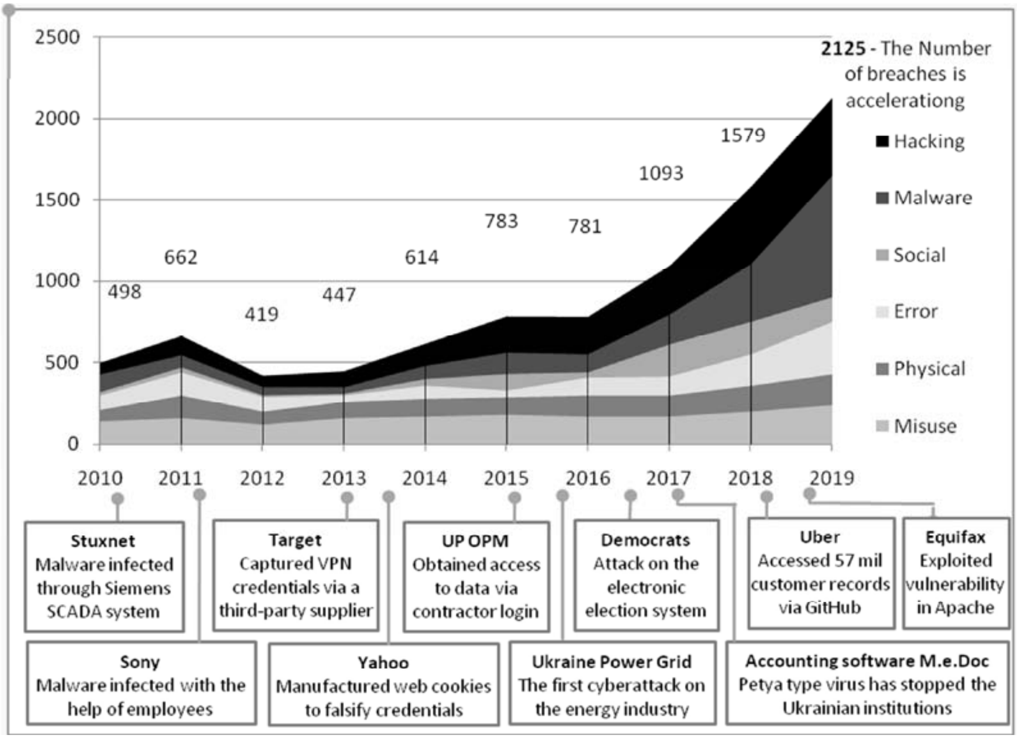

Fig. 1. Classification of Large-scale cyber threats (2010-2019)

Source: [1]

The number of large-scale cyberattacks related to outsourcing increased from 498 to 2125 incidents over 10 years (2010-2019). Among the notable attacks, we can highlight the one on the energy sector of Ukraine in 2016 done through the systems of accounting for utility payments, and the spread of the Petya encoder virus through the update of accounting software in Ukraine in 2017 [1]. The cyber risks growing in accounting system requires positioning an accounting as the basis for enterprises cybersecurity. Pandemic expectations and the associated distancing of work duties have led to a transformation of priorities in the execution of cyber threats. The method of inflicting damage to cybersecurity of business entities has also changed due to the complexity of information processes at the enterprise.

The current classification of cyber risks and their manifestation during the COVID-19 pandemic is shown in Fig. 2.

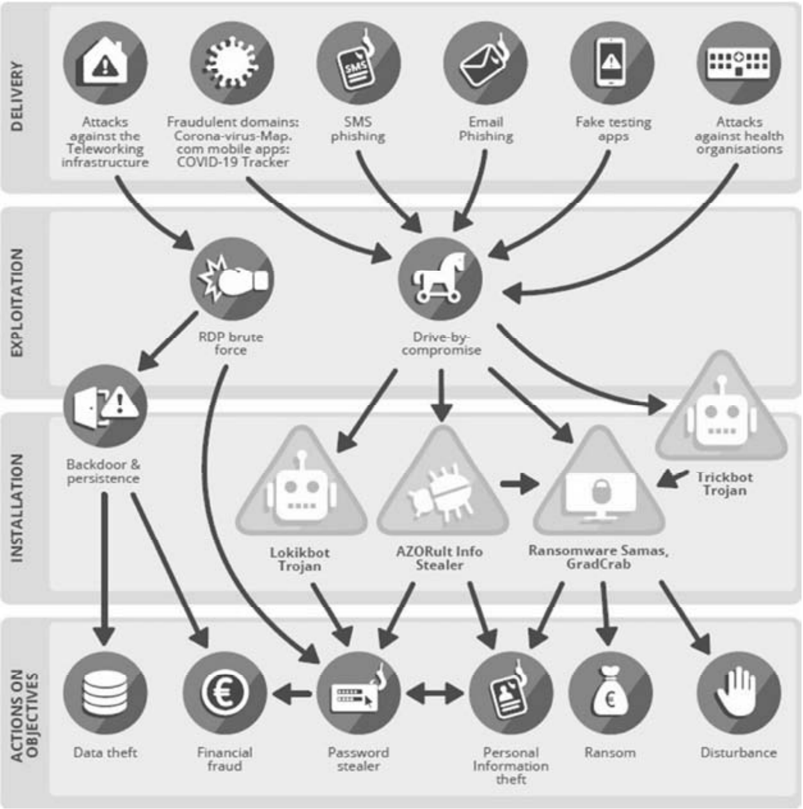

Fig. 2. Cyber risks under the conditions of the COVID-19 pandemic
Source: [2]

Official statistics use the classification of cyber risks by form and methods of execution. Such grouping of cyber threats is uninformative for the purposes of organizing the cybersecurity of enterprises. Back in 2012, Michael Schmitt classified cyber conflicts as part of international hostilities with the identification of various cyber threats to the operation of enterprises [3]. William Steingartner and Darko Galinec have continued this research and created a classification of cyber threats that helped to identify information risks in some countries exerting hybrid influence over others [4].

Nasir Mustafa has substantiated the growing number of various cyber threats in the conditions of pandemic expectations in the economy. The scientist has explained the change in the priorities of enterprise cybersecurity and the increasing likelihood of various cyber risks in the scenario of continuing COVID-19 pandemic and future crises [5]. Yu. Asieieva has summarized cyber risks in the context of developing Internet addiction in different groups of information users. It was revealed that the focus has shifted to individual cyber threats targeting the economic and psychological aspects of households' welfare [6]. Barry Sheehan, Finbarr Murphy, Arash Kia and Ronan Kiely have developed a model for assessing the vulnerabilities of enterprise cybersecurity based on the classification determining the likelihood of cyber threats targeting medical institutions in Europe [7]. Febin

Prakash, Kala Baskar and Harsh Sadawarti have viewed various cyber threats through the lens of cybercrime. Classification of cyber risks in terms of cybercrime identification has allowed scientists to suggest ways of ensuring enterprise cybersecurity [8]. Md Haque, Shameemul Haque, Kailash Kumar and Narendra Singh have systematized all the cyber risks of using Internet of Things technology. The scientists have concluded that most cyber threats can be avoided provided that the Internet of Things technology is used in conjunction with effective methods of information protection [9]. Similarly, R. V. Baranenko has chosen the classification features of cyber threats based on the distinction between “cyberattacks” and “cyberterrorism” [10].

The producing nature of accounting, which is the main generator of economic information at the micro-level, has been considered even less in the classification of cyber threats. There are only isolated works on distinguishing various cyber threats in the context of cybersecurity of accounting information. In particular, V. A. Shpak has developed the basic components of comprehensive enterprise cybersecurity in terms of legal, technical, software and organizational measures [11]. Given that collection of accounting information is the first stage of the accounting information process, the system of accounting reporting and data processing of the enterprise is often vulnerable and subjected to active cyber threats. Accounting reports are the basis for recording financial and economic processes in the prescribed forms - documents. The transfer of documents between the sender and the recipient is determined by a certain sequence, which is called document flow. All stages of reporting and document flow of accounting data are vulnerable to specific cyber threats, which can be grouped into:

- loss of the document or its components (appendices, explanations, individual letters or copies) due to theft or voluntary leaks to attackers;
- replacement of documents with similar (analogous) items with distorted data for the purpose of falsification or infliction of economic damage;
- violation of the integrity of the document, which limits its informational value;
- errors when working with documents during their creation and transfer;

deletion of documents to cause informational and economic damage to the enterprise [11, p. 185].

However, the scientist reduces most cyber risks to the violation of reporting and data processing procedures without taking into account the multifaceted nature of threats to information and economic security of enterprises.

In contrast to the research of cyber threats relevant to accounting documents, GyungMin Lee, ShinWoo Shim, ByoungMo Cho, TaeKyu Kim and Kyounggon Kim have investigated the idea of gradually growing risks of fileless and, accordingly, document-less cyberattacks [12]. As the digitalization of the economy increases, the need for paper and electronic documents abates. Modern cyberattacks are increasingly threatening electronic accounting databases.

S. A. Viter and I. I. Svitlyshyn have systematized the basic principles (software support, protection of confidential information, personal responsibility, secrecy, completeness, access control) by classifying cyber threats and measures (organizational, technical and personnel) to ensure cybersecurity of accounting data [13]. However, some of their cybersecurity postulates apply to all information processes and only partially take into account the accounting specifics of economic processes. Similarly, V. M. Rozheliuk divides cyber threats into internal and external and distinguishes different sub-types relevant to accounting [14]. However, the study does not sufficiently take into account the multifaceted nature of accounting cybersecurity. Having summarized the scientific proposals of more than twenty scientists on the definition of “cyber risks”, Grzegorz Strupczewski concluded that no studies comprehensively classify the threats to the enterprise accounting systems [15].

**Purpose.** The aim of the article is to improve the classification of cyber risks by generalizing and systemizing cyber threats relevant to accounting data.

**Results.** We find it prudent to agree with S.M. Denha and Yu. O. Veryha, who state that cyber threats to accounting should primarily be divided into two categories: intentional (fraud and sabotage) and accidental (errors and malfunctions) [16]. Intentional cyber threats are targeted activities to cause economic and information damage to the business entity. Intentional actions are always planned, premeditated and focused on achieving a clear goal, whereas accidental cyber threats are the result of unintentional errors made by the accounting personnel, an inefficient enterprise accounting system, imperfect information security, poor accounting policies at the enterprise, software and hardware malfunctions, etc. Such threats do not depend on the actions of attackers and lead to unforeseen loss (deletion) of accounting information or creation of favourable conditions for the manifestation of other cyber threats as a result of chance.

Intentional cyber threats can be divided into active and passive ones. Active threats entail inflicting harm on the enterprise or receiving economic gain through manipulation of accounting information. Active threats to the information security of the enterprise manifest in the form of cyberattacks and virus interventions, information fraud, insider sabotage and unauthorized transfer of accounting data. Instead, passive cyber threats are associated with unauthorized access to accounting data. They are usually latent, as they focus on adapting and integrating into the informational space of the enterprise for a long time.

Active and passive cyber threats to accounting should not be directly associated with the internal and external environment of the enterprise. Depending on the spatial manifestation of cyber threats with regards to the information system of the enterprise, it is advisable to distinguish between internal, intra-system and external types of threats. Threats differ in their origin and subjectivity of cyber risks. If the employees or owners (founders) of the enterprise are the cause of the cybersecurity violation, then the cyber risks are internal. Cyber threats are intra-system if they are initiated by persons who are not employed by the enterprise, but participate in a two-way information exchange with the accounting system. These include counterparties, controlling institutions, audit and consulting firms, banking and credit institutions, etc. External cyber threats come from the external environment and are caused by persons informationally and financially unrelated to the enterprise.

The principle of classifying cyber risks of the accounting system according to the criterion of location is similar. Depending on the relation between the location of the cyber threats’ instigators and the business entity targeted by the cyberattack, cyber risks are divided into internal (instigators are on the premises of the business entity); regional (in the city, region, state); national (in the country, associations of countries); international (instigators are abroad) risks.

However, cyber threats to accounting information are not always related to the activities of certain insiders or outsiders. Cyber risks quite often arise from other sources due to inaction or errors (malfunctions) of software and hardware. Accordingly, the sources of threat to the accounting system may include human activities, inaction of systems and technologies, or errors in information processes. Ineffective operation of software and hardware can lead to accidental leakage of confidential information, suspension of economic activity and emergence of "weak spots" in the cybersecurity system of the enterprise. Gaps in the cybersecurity of the enterprise information system, as well as errors in the algorithm for processing accounting information can be used by attackers to commit illegal acts.

This classification of cyber risks can be supplemented by grouping them by origin. Using the origin of cyber threats as the classification criterion, they are divided into [17, c. 53]:

- those associated with the loss (damage, leakage, concealment, deletion) of accounting data;
- those associated with the content of information files (incorporation of inaccurate, incomplete, substituted, distorted accounting data);
- those associated with informational influence (dissemination of false, negative accounting information to informationally influence owners, employees, contractors, etc. of the enterprise).

Identification of the sources of cyber threats contributes to the development of scenarios for their mitigation. Measures for preventive cyber protection of enterprises can be developed on the basis of the created scenarios of cyber threats manifestation, taking into account the individual characteristics of enterprise operation.

However, the cybersecurity of enterprises is much more reliant on the classification of cyber risks according to the goal (threat to information or information system of the enterprise). The goal of information cyber threats is to manipulatively gain access to accounting data. The information infrastructure remains beyond the consideration of attackers. Meanwhile, threats to the information system of the enterprise are focused on obtaining benefits or harming businesses; in such case, accounting data is used only as a means of gaining access to the informational space of the enterprise.

When classifying cyber risks, the goal system is divided into target groups related to software, hardware, personnel, regulatory and organizational support. Each type of threat is associated with ineffectiveness or low effectiveness of certain components of cybersecurity. For example, software threats are the result of errors in the installation and operation of computer programs created for automated processing of accounting data. Hardware threats are related to obsolescence or inefficient use of accounting automation hardware. Personnel threats are caused by insufficient professionalism of accounting staff, as well as the impossibility of training (retraining) and lack of motivation to use modern computer and communication technologies. Regulatory threats emerge due to the lack of opportunities to adapt automated accounting to the requirements of internal and external regulations. Organizational threats are associated with shortcomings in the organizational structure of the enterprise and the accounting department, which lead to accidental errors and vulnerabilities of the information system of the enterprise.

It is advisable to develop measures to prevent and eliminate cyber threats in accordance with the target classification. Therefore, it is necessary to use software, hardware, personnel, regulatory and organizational measures of cyber security.

The level of damage is related to the number of instigators and targets of cyber threats. According to the scale of cyber threats, they should be classified into: (a) general, which threaten the operation of the business entity as a whole; (b) local, which single out directions or areas of activity (operational, administrative, sales, financial, investment, etc.) of the enterprise; (c) targeted, focusing on individual accounting targets (noncurrent assets, cash, income, etc.).

At the same time, cyber threats must be classified according to the criterion of aspect. In terms of the aspects of cybersecurity of the accounting system, cyber threats should be grouped into: (a) threats to confidentiality (accounting data is accessed by persons without proper authorization); (b) threats to integrity (accounting data is distorted, destroyed or replaced); (c) availability threats (access to accounting data is restricted or blocked).

Different aspects of cyber threats are realized through a various forms of assaults. According to the form of manifestation of cyber risks, we can distinguish cyberattacks, cyber incidents, cyber espionage, cyberterrorism, and cyber wars, which have different motivations for cyber intervention and different methods of implementation. The national legislation of Ukraine defines cyberattack as “targeted (intentional) action in cyberspace, which is carried out by means of electronic communications (including information and communication technologies, software, hardware, other technical and technological means and equipment) and focused on achieving one or a combination of such goals: violation of confidentiality, integrity, availability of electronic information processed (transmitted, stored) in communication and / or technological systems, obtaining unauthorized access to such resources; violation of security, sustainable, reliable and regular operation of communication and / or technological systems; use of the communication system, its resources and means of electronic communications for cyberattacks on other subjects of cybersecurity” [18]. Cyberattacks are fundamentally different from other manifestations of cyber risks. A cyber incident is a single event or a set of accidental adverse events of an unintentional nature that damage the enterprise’s accounting system. Cyber espionage is unauthorized continuous multiple covert theft of accounting data. Cyberterrorism is terrorist activity aimed at malicious manipulation of accounting data and causing harm to the enterprise. Cyberwar is the destabilization of enterprise information systems and the use of accounting systems to create chaos in the economic activities of enterprises and people.

Forms of cyber threats to accounting differ in latency and duration of information intervention, which can also be used as classification criteria. In particular, cyberattacks and cyber incidents are visible and short-lived, cyber espionage is covert and long-term (or permanent), cyberterrorism and cyberwar are aggressive and long-term.

Moreover, all cyber risks can be classified into criminal and non-criminal [19, p. 105]. The classification criterion is the interpretation of cyber threats from the standpoint of criminal liability for their execution. The criminal risks of the accounting system are associated with illegal activities (hacker attacks, physical attacks, blackmail and fraud). All other cyber threats in the form of anthropogenic or technological errors and force majeure are considered non-criminal.

The consideration of legality of cyber threats to accounting makes it possible to identify the consequences of interfering in the cybersecurity of enterprises. According to the end result, cyber threats can be divided into those affecting information processes, causing difficulties in the operation of the accounting system, and destroying the enterprise management system. Non-criminal cyber threats mainly result in the theft or distortion of accounting data, while criminal cyber risks are focused on blocking certain information systems or interfering with the operation of business entities. Thus, the risks that cause difficulties in the operation of the accounting system and block the management system are destructive for the company.

Such cyber threats require a balanced approach to the organization of cybersecurity in terms of avoiding destructive risks. To successfully prevent cyber threats, it is important to determine their probability. Classification according to the probability of the cyber threats can divide them into unlikely, probable and inevitable ones. Thus, it is recommended to assess all cyber threats to accounting in terms of the probability of their manifestation in order to ensure effective cybersecurity of the enterprise. If necessary, the probabilistic classification of cyber threats can be expanded by using a larger number of categories depending on the ranges of probability: no probability (coefficient of occurrence - 0), low probability (0.1-0.3), average probability (0, 4-0.5), high probability (0.6-0.8), guaranteed onset (0.9-0.99), imminent onset (1).

The classification of cyber threats to accounting in the context of various classification criteria is generalized in Table 1. Measures to organize the cybersecurity of accounting information change depending on the type of cyber threats listed in the table and relevance for a particular business entity.

*Table 1*

**Generalized classification of cyber threat to accounting data**

| No. | Classification criterion | Type of cyber threat |
|---|---|---|
| 1. | Intent | - accidental,<br>- intentional. |
| 2. | Mode | - active,<br>- passive. |
| 3. | Information and financial interest | - internal,<br>- intra-system,<br>- external. |
| 4. | Location | - internal,<br>- regional,<br>- national,<br>- international. |
| 5. | Instigator | - human actions,<br>- inactivity of systems and technologies,<br>- errors in information processes. |
| 6. | Origin | those associated with:<br>- loss of data,<br>- creation of information file,<br>- information influence. |

*continuation of table 1*

| | | |
|---|---|---|
| 7. | Goal | - threats to accounting data,<br>- threats to the information system of the enterprise. |
| 8. | Target | - software support,<br>- hardware support,<br>- personnel support,<br>- regulatory support,<br>- organizational support. |
| 9. | Scale | - general,<br>- local,<br>- targeted. |
| 10. | Aspect | - threats to confidentiality,<br>- threats to integrity,<br>- availability threats. |
| 11. | Form of manifestation | - cyberattack,<br>- cyber espionage,<br>- cyber incident,<br>- cyber terrorism,<br>- cyber war. |
| 12. | Legality | - criminal (hacker attacks, physical attacks, blackmail and fraud),<br>- non-criminal (anthropogenic errors, technological errors, force majeure). |
| 13. | Duration | - short-term,<br>- long-term,<br>- continuous. |
| 14. | Latency | - covert,<br>- visible,<br>- aggressive. |
| 15. | Probability | - unlikely,<br>- probable,<br>- inevitable. |
| 16. | Consequences | - influencing information processing,<br>- causing difficulties in the operation of the accounting system,<br>- destroying the enterprise management system. |

Source: systemized and improved by the author.

Cyber threats can also be classified by gender and age of cybercriminals. In particular, according to statistics, 67% of cyber threats are perpetrated by male criminals (age: up to 25 years - 13%, 25-40 years - 39%, over 40 years - 15%) and, accordingly, 33% are perpetrated by women (age: up to 25 years - 6%, 25-40 years - 20%, more than 40 years - 7%) [20].

The relevance of age and gender distribution for the classification of cyber threats is substantiated in the research of Ioannis Tsimperidis, Cagatay Yucel and Vasilios Katos [21]. However, such a classification is not very useful in developing measures to ensure the cybersecurity of accounting data, as it involves the identification and division of cybercriminals, rather than cyber risks.

The suggested classification of cyber threats should be used in the organization of constant cybersecurity of enterprises. Each type of cyber threats to accounting data requires a specific method of prevention, avoidance and elimination of consequences [22]. As a result, cybersecurity is a dynamic and adaptive process that takes into account the differences in the manifestation of different cyber threats. Since the complexity of information processes and the advancements in computer and communication technologies are continuously changing along with socio-economic conditions of enterprise operation, the proposed classification of cyber threats to accounting data will need to be amended and supplemented.

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

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

## *Література*

1. The 2019 Kearney Global Services Location Index. Digital resonance: the new factor influencing location attractiveness. URL: https://www.kearney.com/digital-transformation/gsli/2019-full-report.
2. Main incidents in the EU and worldwide. ENISA Threat Landscape. URL: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-main-incidents.
3. Schmitt Michael. (2012). Classification of Cyber Conflict. Journal of Conflict and Security Law. 17 (2). 245-260. 10.1093/jcsl/krs018.
4. Steingartner William & Galinec Darko. (2021). Cyber Threats and Cyber Deception in Hybrid Warfare. Acta Polytechnica Hungarica. 18. 25-45. 10.12700/APH.18.3.2021.3.2.
5. Mustafa, Nasir. (2020). Cyber Risk and Covid-19: Managing Cyber Risks Arising From The Pandemic. Brighttalk Webinar Series. Project: Coronavirus CoV-19 to CoV-20 Pro. 10.13140/RG.2.2.12218.82886.
6. Asieieva, Yu. (2020). Problem questions of cyber-addictions classification. Psychology and Personality. 2. 23-40. 10.33989/2226-4078.2020.2.211910.
7. Sheehan Barry, Murphy Finbarr, Kia Arash & Kiely Ronan. (2021). A quantitative bow-tie cyber risk classification and assessment framework. Journal of Risk Research. 1-20. 10.1080/13669877.2021.1900337.

8. Prakash Febin, Baskar Kala & Sadawarti Harsh. (2019). Cyber Crime: Challenges and its Classification. International Multi-disciplinary Academic Research Conference (IMARC-2019). 2–4.
9. Haque Md, Haque Shameemul, Kumar Kailash & Singh Narendra. (2021). A Comprehensive Study of Cyber Security Attacks, Classification, and Countermeasures in the Internet of Things. 63-90. 10.4018/978-1-7998-4201-9.ch004.
10. Baranenko R.V. (2021). Cyber attacks as a form of cyber terrorism. Scientific notes of Taurida National V.I. Vernadsky University. Series: Technical Sciences. 1. 45-50. 10.32838/2663-5941/2021.1-1/07.
11. Шпак В.А. Організація захисту облікової інформації. Бухгалтерський облік, аналіз та аудит: проблеми теорії, методології, організації. 2015. № 2. С. 181-187. URL : http://nbuv.gov.ua/UJRN/boaa_2015_2_27.
12. Lee GyungMin, Shim ShinWoo, Cho ByoungMo, Kim TaeKyu & Kim Kyounggon. (2020). The Classification Model of Fileless Cyber Attacks. Journal of KIISE. 47. 454-465. 10.5626/JOK.2020.47.5.454.
13. Вітер С. А., Світлишин І. І. Захист облікової інформації та кібербезпека підприємства. Економіка та суспільство : електрон. наук. фах. вид. 2017. № 11. С. 497–502.
14. Рожелюк В.М. Заходи забезпечення захисту облікової інформації. Бухгалтерський облік, аналіз та аудит: проблеми теорії, методології, організації. К.: ПП «Рута», 2013. С. 335-340.
15. Strupczewski, Grzegorz. (2021). Defining cyber risk. Safety Science. 6. 135. 10.1016/j.ssci.2020.105143.
16. Деньга С. М., Верига Ю. О. Захист інформації в комп`ютерних інформаційних системах бухгалтерського обліку. Бухгалтерський облік і аудит. 2004. № 5. С. 59-65.
17. Зинкевич В., Штатов Д. Информационные риски: анализ и количественная оценка. Бухгалтерия и банки. 2007. № 1. С. 50–55.
18. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII. URL: http://zakon3.rada.gov.ua/laws/show/2163-19.
19. Волосович С., Клапків Л. Детермінанти виникнення та реалізації кіберризиків. Зовнішня торгівля: економіка, фінанси, право. 2018. № 3. С. 101–115. URL: http://nbuv.gov.ua/UJRN/uazt_2018_3_10.
20. Підсумки 2018 року в цифрах. URL: https://cyberpolice.gov.ua/results/2018.
21. Tsimperidis Ioannis, Yucel Cagatay, Katos Vasilios. (2021). Age and Gender as Cyber Attribution Features in Keystroke Dynamic-Based User Classification Processes. Electronics. 10. 835. 10.3390/electronics10070835.
22. Zadorozhnyi Z.-M., Muravskyi V., Shevchuk O. and Muravskyi V. The accounting system as the basis for organising enterprise cybersecurity. Financial and credit activity: problems of theory and practice, 3, 2020, 147-156. 10.18371/fcaptp.v3i34.215462.

## *References*

1. The 2019 Kearney Global Services Location Index. Digital resonance: the new factor influencing location attractiveness. URL: https://www.kearney.com/digital-transformation/gsli/2019-full-report.
2. Main incidents in the EU and worldwide. ENISA Threat Landscape. URL: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-main-incidents [In English].
3. Schmitt Michael. (2012). Classification of Cyber Conflict. Journal of Conflict and Security Law. 17 (2). 245-260. 10.1093/jcsl/krs018 [In English].
4. Steingartner William & Galinec Darko. (2021). Cyber Threats and Cyber Deception in Hybrid Warfare. Acta Polytechnica Hungarica. 18. 25-45. 10.12700/APH.18.3.2021.3.2 [In English].
5. Mustafa, Nasir. (2020). Cyber Risk and Covid-19: Managing Cyber Risks Arising From The Pandemic. Brighttalk Webinar Series. Project: Coronavirus CoV-19 to CoV-20 Pro. 10.13140/RG.2.2.12218.82886 [In English].
6. Asieieva, Yu. (2020). Problem questions of cyber-addictions classification. Psychology and Personality. 2. 23-40. 10.33989/2226-4078.2020.2.211910 [In English].
7. Sheehan Barry, Murphy Finbarr, Kia Arash & Kiely Ronan. (2021). A quantitative bow-tie cyber risk classification and assessment framework. Journal of Risk Research. 1-20. 10.1080/13669877.2021.1900337 [In English].
8. Prakash Febin, Baskar Kala & Sadawarti Harsh. (2019). Cyber Crime: Challenges and its Classification. International Multi-disciplinary Academic Research Conference (IMARC-2019). 2–4 [In English].
9. Haque Md, Haque Shameemul, Kumar Kailash & Singh Narendra. (2021). A Comprehensive Study of Cyber Security Attacks, Classification, and Countermeasures in the Internet of Things. 63-90. 10.4018/978-1-7998-4201-9.ch004 [In English].
10. Baranenko R.V. (2021). Cyber attacks as a form of cyber terrorism. Scientific notes of Taurida National V.I. Vernadsky University. Series: Technical Sciences. 1. 45-50. 10.32838/2663-5941/2021.1-1/07 [In English].
11. Shpak V.A. Orhanizatsiia zakhystu oblikovoi informatsii [Orhanizatsiia zakhystu oblikovoi informatsii]. Bukhhalterskyi oblik, analiz ta audyt: problemy teorii, metodolohii, orhanizatsii – Accounting, analysis and audit: problems of theory, methodology, organization. 2015. 2. 181-187. URL : http://nbuv.gov.ua/UJRN/boaa_2015_2_27 [In Ukrainian].
12. Lee GyungMin, Shim ShinWoo, Cho ByoungMo, Kim TaeKyu & Kim Kyounggon. (2020). The Classification Model of Fileless Cyber Attacks. Journal of KIISE. 47. 454-465. 10.5626/JOK.2020.47.5.454 [In English].
13. Viter S. A., Svitlyshyn I. I. (2017). Zakhyst oblikovoi informatsii ta kiberbezpeka pidpryiemstva [Protection of accounting information and cybersecurity of the enterprise]. Ekonomika ta suspilstvo : elektronne naukove fakhove vydannia – Economy and society: electronic scientific professional publication. 11. 497–502 [In Ukrainian].

14. Rozheliuk V.M. (2013). Zakhody zabezpechennia zakhystu oblikovoi informatsii [Measures to ensure the protection of accounting information]. Bukhhalterskyi oblik, analiz ta audyt: problemy teorii, metodolohii, orhanizatsii – Accounting, analysis and audit: problems of theory, methodology, organization. K.: PP «Ruta», 335-340 [In Ukrainian].
15. Strupczewski, Grzegorz. (2021). Defining cyber risk. Safety Science. 6. 135. 10.1016/j.ssci.2020.105143 [In English].
16. Denha S. M., Veryha Yu. O. (2004). Zakhyst informatsii v komp`yuternykh informatsiinykh systemakh bukhhalterskoho obliku [Information protection in computer information systems of accounting]. Bukhhalterskyi oblik i audyt – Accounting and auditing. 5. 59-65 [In Ukrainian].
17. Zinkevich V., Shtatov D. (2007). Informacionnye riski: analiz i kolichestvennaja ocenk [Information risks: analysis and quantitative assessment]. Buhgalterija i banki – Accounting and banks. 1. 50–55 [In Russian].
18. Zakon Ukrainy «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy» [Law of Ukraine «On Basic Principles of Cyber Security of Ukraine»]. вOctober 5, 2017. № 2163-VIII. URL: http://zakon3.rada.gov.ua/laws/show/2163-19 [In Ukrainian].
19. Volosovych S., Klapkiv L. (2018). Determinanty vynyknennia ta realizatsii kiberryzykiv [Determinants of the origin and implementation of cyber risks]. Zovnishnia torhivlia: ekonomika, finansy, pravo – Foreign trade: economics, finance, law. 3. 101–115. URL: http://nbuv.gov.ua/UJRN/uazt_2018_3_10 [In Ukrainian].
20. Pidsumky 2018 roku v tsyfrakh [Results of 2018 in figures]. URL: https://cyberpolice.gov.ua/results/2018 [In Ukrainian].
21. Tsimperidis Ioannis, Yucel Cagatay, Katos Vasilios. (2021). Age and Gender as Cyber Attribution Features in Keystroke Dynamic-Based User Classification Processes. Electronics. 10. 835. 10.3390/electronics10070835 [In English].
22. Zadorozhnyi Z.-M., Muravskyi V., Shevchuk O. and Muravskyi V. (2020). The accounting system as the basis for organising enterprise cybersecurity. Financial and credit activity: problems of theory and practice. 3. 147-156. 10.18371/fcaptp.v3i34.215462 [In English].

Статтю отримано 08 квітня 2021 р.
Article received April 8, 2021