УДК 657.8:004

JEL classification: M41, M42, D24

DOI: https://doi.org/10.35774/visnyk2021.01.083

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

Vasyl MURAVSKYI,
Lecturer in the Department of Economic Cybernetics and Informatics,
West Ukrainian National University,
11 Lvivska str., Ternopil, 46020, Ukraine
e-mail: vasylmur@gmail.com
ORCID ID: https://orcid.org/0000-0002-9625-9572

Oleh SHEVCHUK,
Phd, Associate Professor,
Head of the International Students' Department,
West Ukrainian National University,
11 Lvivska str., Ternopil, 46020, Ukraine
e-mail: ikaf@ukr.net
ORCID ID: http://orcid.org/0000-0002-7352-7001

CLASSIFICATION OF STAKEHOLDERS (USERS) OF ACCOUNTING INFORMATION FOR THE ENTERPRISE CYBERSECURITY PURPOSES

Muravskyi V., Muravskyi V., Shevchuk O. (2021). Klasyfikatsiia steikkholderiv (korystuvachiv) oblikovoi informatsii dlia tsilei kiberzakhystu pidpryiemstva [Classification of stakeholders (users) of accounting information for the enterprise cybersecurity purposes]. *Visnyk economiky – Herald of Economics,* 1, 83–96. DOI: https://doi.org/10.35774/visnyk2021.01.083

Муравський В., Муравський В., Шевчук О. Класифікація стейкхолдерів (користувачів) облікової інформації для цілей кіберзахисту підприємства. *Вісник економіки.* 2021. Вип. 1. С. 83–96. DOI: https://doi.org/10.35774/visnyk2021.01.083

Annotation

Introduction. *The intensification of cyberrisks due to global hybrid conflicts, the COVID-19 pandemic, and economic imbalances threatens the accounting system as the*

© Volodymyr Muravskyi, Vasyl Muravskyi, Oleh Shevchuk, 2021.

main generator of economic information, which requires the organization of an effective system of enterprises cybersecurity. It is necessary to understand cyberthreats impact on the functioning of different types of stakeholders for development of the effective cybersecurity.

Purpose. *The main purpose is to research and improve the classification of accounting information users for the enterprises cybersecurity and minimize the variable cyberrisks that threaten different groups of stakeholders.*

Methods. *General scientific empirical, logical and historical methods of cognition of reality in the process of researching the relevance of variable cyberthreats for different types of stakeholders were used. The research is based on general methods of studying economic processes, facts and phenomena from the standpoint of accounting and enterprises cybersecurity. The information base of the research is historical documents on the classification of stakeholders, scientific works of domestic and foreign scientists about dividing users of accounting information into types, and so on.*

Results. *It is proved that the classical scientific views on the classification of accounting information users are ineffective for the purposes of enterprises cyberprotection, as they do not take into account the activation of relevant for the digital economy of variable cyberthreats. It is proposed to classify accounting information users by the following criteria: the ability to manage the activities of the business entity, the right of access, the likelihood of cyberthreats, the ability to dispose of the access right, access to accounting objects, functional law, information processing, economic activity, age, organizational and legal form, type of communication channels used, frequency of information acts.*

Discussion. *The use of the proposed stakeholders' classification helps to identify cyberrisks; prevent, avoid and minimize cyberthreats consequences, relevant to each type of accounting information users, which requires further research about enterprises cybersecurity.*

Keywords: *accounting, stakeholders, cybersecurity, accounting information, classification of information users, cyberrisks.*

Formulas: 0, fig.: 0, labl.: 3, bibl.: 11.

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

Василь МУРАВСЬКИЙ,
викладач кафедри економічної кібернетики та інформатики,
Західноукраїнський національний університет,
вул. Львівська, 11, м. Тернопіль, 46020, Україна
e-mail: vasylmur@gmail.com
ORCID ID: https://orcid.org/0000-0002-9625-9572

ISSN 2786-4537 (print). Вісник економіки № 1, 2021 р.
ISSN 2786-4545 (online). Herald of Economics № 1, 2021

Олег ШЕВЧУК,
кандидат економічних наук, доцент,
начальник відділу по роботі з іноземними студентами,
Західноукраїнський національний університет,
вул. Львівська, 11, м. Тернопіль, 46020, Україна
e-mail: ikaf@ukr.net
ORCID ID: http://orcid.org/0000-0002-7352-7001

КЛАСИФІКАЦІЯ СТЕЙКХОЛДЕРІВ (КОРИСТУВАЧІВ) ОБЛІКОВОЇ ІНФОРМАЦІЇ ДЛЯ ЦІЛЕЙ КІБЕРЗАХИСТУ ПІДПРИЄМСТВА

Анотація

Вступ. *Активізація кіберризиків унаслідок глобальних гібридних конфліктів, пандемії COVID-19, економічних дисбалансів загрожує системі бухгалтерського обліку як основному генератору економічної інформації, що потребує організації ефективної системи кіберзахисту підприємств. Для вироблення дієвих заходів мінімізації кіберзагроз необхідне розуміння їхнього впливу на функціонування стейкхолдерів у розрізі різних видів.*

Мета статті *полягає у дослідженні та удосконаленні класифікації користувачів облікової інформації для цілей забезпечення кіберзахисту підприємств та мінімізації варіативних кіберризиків, що загрожують різним групам стейкхолдерів.*

Методи. *У процесі дослідження актуальності варіативних кіберзагроз для різних видів стейкхолдерів використані загальнонаукові емпіричні, логічні та історичні методичні прийоми пізнання дійсності. Дослідження базуються на основі загальних методів вивчення економічних процесів, фактів та явищ з позиції бухгалтерського обліку та кібербезпеки підприємств. Інформаційною базою дослідження стали історичні документи щодо класифікації стейкхолдерів, наукові праці вітчизняних та зарубіжних учених у частині поділу користувачів облікової інформації на види тощо.*

Результати. *Доведено, що класичні наукові погляди на класифікацію користувачів облікової інформації є недієвими для цілей забезпечення кіберзахисту підприємств, оскільки не враховують активізацію актуальних для цифрової економіки варіативних кіберзагроз. Запропоновано класифікувати користувачів облікової інформації за критеріями: можливості управляти діяльністю господарюючого суб'єкта, правом доступу, імовірності появи кіберзагроз, можливості розпоряджатися правом доступу, доступу до облікових об'єктів, функціонального права, порядку обробки інформації, виду економічної діяльності, віку фізичних осіб, організаційно-правової форми юридичних осіб, виду застосовуваних комунікаційних каналів, частоти інформаційних актів.*

Перспективи. *Використання запропонованої класифікації стейкхолдерів сприяє виявленню кіберризиків; попередженню, уникненню та мінімізації наслідків кіберзагроз, актуальних окремо для кожного виду користувачів облікової інформації, що потребує подальших наукових досліджень у частині забезпечення кібербезпеки підприємств.*

Ключові слова: *облік, стейкхолдери, кібербезпека, облікова інформація, класифікація користувачів інформації, кіберризики.*

Формул: 0, рис.: 0, табл.: 3, бібл.: 11.

Introduction. Accounting forms an integrated information environment that connects the users of accounting information into a single system. Accounting professionals fill in the system with information resources, and information agents (stakeholders) receive and use the resources for making management decisions. At each stage of accounting information processing at the internal and external levels of accounting and management interaction, the information environment of an enterprise is threatened by cyber threats.

Global hybrid conflicts, the COVID-19 pandemic, and the growing corruption of the economy have led to increased cyber risks in the field of accounting. Increasing in cyber-attacks as a part of hybrid wars involves manipulating, distorting, and replacing credentials to inflict economic damage for large enterprises and sectors of economy, ultimately damaging to the country's economic security. Pandemic changes in the work process distanced and isolated workers that required active information exchange between the workplaces of specialists and information base of enterprises. Performing functional responsibilities, active communication services usage has attracted the attention of cybercriminals, whose goal is to steal trade secrets and intellectual property of the enterprise. Economic imbalances and corruption threats to businesses have a similar impact on accounting processes that lead to significant reductions in the business cybersecurity costs. As a result, the number of vulnerabilities in the cybersecurity system of accounting and management has increased significantly.

Therefore, the active development of computer and communication technologies in the digital economy has led to a variety of cyber threats due to the expansion of facilities and vulnerabilities in information system of enterprises. The variability of cyber risks directly depends on the type of stakeholders. Grouping users of credentials by different criteria for the cybersecurity purposes allows them to develop adequate methods to prevent, avoid and eliminate cyber-attacks more effectively.

Literature Review. The basic criterion for dividing users of accounting information into internal and external ones is the spatial location of stakeholders involved in the information environment of the enterprise. Internal staff and enterprise management of various levels are the main users of accounting information and moderators of management decisions, and are subject to frequent cyber-attacks consequently. As analyzed in [1, p. 87-88], the scientists quite often consider information related only to the functioning of employees and owners (founders) of the enterprise as an object of cyber risk, so in terms of the cybersecurity they recognize only internal users of accounting information at enterprises. According to the EY Global Information Security Survey, personal information of employees, and information about owners and managers is the main object of cyber-attacks at enterprises (17% and 11%, respectively). In addition, 34% of businesses were exposed to active cyber threats due to negligence or ignorance of employees who are internal stakeholders (Table 1). In harmony with the EY Global Information Security Survey, most cyber-attacks (38%), are organized by current or fired employees [2].

ISSN 2786-4537 (print). Вісник економіки № 1, 2021 р.
ISSN 2786-4545 (online). Herald of Economics № 1, 2021

Table 1

Objects and vulnerabilities of business cybersecurity

Object of a cyber-attacks	Fraction of enterprises	Cybersecurity's vulnerabilities	Fraction of enterprises
Staff's personal information	17 %	Negligent / uninformed employees	34 %
Information about financial and monetary transactions	12 %	Outdated security controls	26 %
Strategic plans	12 %	Unauthorized access by unauthorized persons	13 %
Information about owners and managers	11 %	Related to using of cloud computing	10 %
Customers' information	11 %	Related to smartphones / tablets	8 %
Research and development information	9 %	Related to social networks	5 %
Merger and acquisition information	8 %	Related to Internet of things	4 %
Intellectual property	6 %		
Supplier's information	5 %		

Source: based on [2].

However, accounting information, that related to external financial and economic processes, is the object of cyber-attacks more often in the context of intensifying global hybrid conflicts and the COVID-19 pandemic (information about financial and monetary transactions – 12% of enterprises, information about customers – 11%, information about mergers and acquisitions – 8%, information about suppliers – 5%). 13% of businesses found that cyber threats were due to unauthorized access by persons, which are external to the information system of the enterprise [2]. As a result, only the internal positioning of the cybersecurity is a limitation of its important mission in the formation of the comprehensive system of enterprise information and economic security.

At the same time, there are few scientific papers that significantly expand the users of accounting information in need of the cybersecurity. For example, N. Shishkova defined the list of ways of the cybersecurity in the context of separation on internal and external users. However, there is no explanation for the differences in providing cyber protection for different groups of stakeholders [3, p.121-122].

K. Borymskaya positions fiscal service as an important stakeholder of accounting information that is threatened by cyber-attacks. The scientist proposes the system of the cyber protection, that provides definition of confidential information, improvement of job descriptions, using "digital signatures" for tax purposes, using software and hardware in the process of communication with fiscal service [4, p.17-18]. In return, A. Rasche and D. Esser developed information security standards separately for internal users and various external ones. According to the scientists the users are recommended to use standards in obtaining and processing accounting information to protect it [5, p.255]. A similar opinion is supported by C. Chikutuma, who justified the feasibility of forming integrated reporting as an effective communication channel for information transmission to both internal stakeholders

and external ones. The researcher substantiates the demand for secure demarcation of information needs in different user groups to maintain trade secrets and ensure cyber protection of reporting entities [6]. The research was continued by V.Shpak with developing a method of protecting the document flow of the enterprise in the framework of information exchange with internal information contractors and external ones. The author substantiates the concept of confidential documents with different access rights to stakeholders [7, p.186].

However, the differentiation of users according to the criterion of spatial location in relation to information environment of the enterprise makes it difficult to effectively ensure the cyber protection of enterprises due to the possibility of relating certain stakeholders to internal and external ones. It is difficult to develop tools for minimizing cyber threats when it is impossible to clearly cluster the subjects of security processes.

A large-scale study of scientific positions regarding the options for classification of accounting information users was conducted by I. Chukhno. Based on the identified conflicts in the traditional classification of users on internal and external, the author proposes to proceed from the ability of stakeholders to manage the activities of the business entity. Accordingly, the researcher identified three groups of accounting information users:

1) persons, who make management decisions;

2) persons, who do not make management decisions, but have a financial interest;

3) persons without financial interest [1, p.88].

Sharing the opinion of scientist, it should be noted that the division of stakeholders on the basis of financial and managerial interest solves the problem of their association with internal persons or external ones. The staff together with the owners (founders), regardless of the spatial relationship to the information environment of the enterprise, can be both internal and external stakeholders.

O. Lagovska, S. Lehenchuk, B. Kuz, S. Kucher were the first to classify stakeholders of accounting information for the cybersecurity purposes into users with full right, limited right and those who use freely published reporting [8, p.28]. A. Shchyrska has a similar position on separation of insiders and outsiders as accounting information users with or without access rights to accounting information, respectively [9, p.215].

Also Y. El-Ebiary and N. Alawi examining the risks of accounting as part of information system of the enterprise, determine the need to classify stakeholders according to the probability of cyber threats. Depending on the relevance of certain cyber threats for each three types of accounting information users (with high, medium and low probability), variable methods of the cybersecurity are needed [10].

Hereby, the classical approaches to the classification of accounting information users are ineffective for the purposes of the enterprise cybersecurity. In other words, cyber threats may not change for stakeholders within a single classification group. So, for the purposes of the enterprise cybersecurity, more thorough study of other criteria for the classification of accounting information users is relevant in order to develop adequate means of a comprehensive cybersecurity system.

Purpose. The main purpose of the article is to study and improve the classification of accounting information users for the goals of the enterprise cybersecurity and minimization of variable cyber risks that threaten different groups of stakeholders.

ISSN 2786-4537 (print). Вісник економіки № 1, 2021 р.
ISSN 2786-4545 (online). Herald of Economics № 1, 2021

Results. The main criterion for dividing users into groups for the purposes of the enterprise cybersecurity, to which these scientists pay attention, is the level of access to accounting information. The level of access should be interpreted as the maximum possible amount and type of credentials that are provided to users for processing, inasmuch their professional and behavioral characteristics. The right to receive accounting information under such conditions is directly related to the accessed possibility to trade secrets of the enterprise and derives from the accounting type (financial, management, etc.). According to this criterion, it is advisable to distinguish stakeholders with absolute access, full access, limited access and access to free information:

1) Users with absolute rights are management staff with unlimited access to accounting information used for long-term management of the enterprise. Such users embrace the maximum available array of data that generated by management and financial accounting.

2) Users with full rights have access to confidential information in a particular area of management, or financial and economic activities of the enterprise. For example, management personnel use management accounting credentials of a strategic or tactical nature to make strategic and tactical management decisions.

3) Users with limited access are provided with the right to implement subject-functional actions in relation to the enterprise, information on an individual aspect that is provided for using. In particular, fiscal institutions receive tax reporting and request additional accounting information in the form of primary and synthetic documents, etc. if it necessary.

4) Users with free access do not need a request to obtain the right for exploiting accounting information. They use publicly available data. Such accounting information does not contain confidential information and is mainly prepared by financial accounting.

If it is possible, to dispose of the access right to accounting information, stakeholders should be classified into right providers (given the right to receive and dispose data) and right holders (holders of information access rights). The users of information quite often can belong to both groups at the same time. The right holder on the rights of subcontracting may delegate (transfer the right of access) the authority to process information to other persons. For example, potential investors receive accounting information and pass it to investment brokers. Therefore, the right holder can be the creditor.

Based on the implementation of the access right to accounting information, it is also advisable to distinguish the following classification criteria: access to accounting objects, functional rights and the order of information processing. According to the object direction, stakeholders are given the right to process information only about certain objects of accounting. For example, it is advisable to allow a cashier to work with the functional menu of computer programs for accounting and management of cash and banking transactions. Other objects of accounting remain inaccessible to the narrowly specialized specialist. The regulation of functional powers provides for the limited implementation of accounting functions: filling out primary documents, conducting control procedures, generalizing accounting data in registers, conducting tax calculations, etc. Depending on their job responsibilities, stakeholders may be prohibited from processing credentials, including: viewing or entering information; verify (conduct) data, change information that has taken effect; delete accounts; transfer indicators to the next stages of processing.

In accordance, the users of accounting information should be classified suitably to the following security criteria: functional rights (work with primary documents, control procedures (including inventory), systematization of data, analysis of indicators and decision-making; definition of accounting policy); processing of accounting information (entering, editing, conducting, summarizing, transmitting and archiving data); object of accounting (non-current assets, inventories, cash, receivables, accounts payable, capital, wages, taxes and fees, income and expenses or more detailed objects). Stakeholders are often endowed with combined rights. The smaller is the company, the greater is the concentration of user accounting information rights. In small businesses one person can perform all accounting processes, that involves obtaining full rights to operate information. Individual business entities that simultaneously perform economic, accounting and management functions, are holders of absolute rights, as the right holder and the recipient is the one person.

The next classification feature of the stakeholders' division from standpoint of the need to provide the cybersecurity is the type of economic activity. Stakeholders representing different types of economic activity are also exposed to variable cyber risks (Table 2).So, users of accounting information should be grouped by sector of the economy.

Table 2

Relevance of cyber threats for different sectors of economy

Sector	Maim threats	Trend in 2020 / 2019	Factors Influence
Individuals / Households	Fishing Information Leakage Data Theft	=	Self-isolation as a way to combat COVID-19 has contributed to the decentralization of the IT environment and the isolation of Internet users who are exposed to cyber threats and pay less attention to the cybersecurity.
Industry	Malicious Software (Malware) Web Application Attacks Insider Threat (unintentional abuse)	=	Theft of credentials containing trade secrets is a significant threat to this sector. Cyber-attacks on supply chains and industrial control systems are also a reason to suspend the production process
Multidisciplinary Business	Web Application Fishing Malicious Software	+	Workers' remote work as a way to combat COVID-19 has intensified Fishing attacks, threatening the loss of confidential credentials.
Public Administration, Defense, Social Services	Malicious Software Fishing Web Application Attacks	+	Using cloud services has led to an increase in cyber threats to the administrative sector of state. Social services were cyber-attacked through financial assistance services to citizens during the COVID-19 pandemic.
Finance / Banking Business / Insurance	Web App Attacks Insider Threat (unintentional abuse) Malicious Software Data Theft	=	The multifaceted nature of the financial sector in economy makes it difficult to clearly identify cyber threats, as different areas of financial and banking services may be exposed to completely different cyber risks in the field of accounting.

ISSN 2786-4537 (print). Вісник економіки № 1, 2021 р.
ISSN 2786-4545 (online). Herald of Economics № 1, 2021

Continuation of Table 2

Healthcare / Medicine	Malicious Software Insider Threat (unintentional abuse) Web App Attacks	+	Cyber threats to health care have become more relevant due to the interest of fraudsters in the information and financial resources allocated to the fight against the COVID-19 pandemic.
Education	Malicious Software Demanding Program Web App Attacks	+	Increasing the activity of cyber espionage campaigns due to the interest in accounting and scientific resources related to the COVID-19 study.
Information and Communication	Web App Attacks Insider Threat (unintentional abuse) Malicious Software	=	As the number of digital media grows, cyber risks of changing public information to control public opinion become relevant.
Arts, Entertainment and Games	Web App Attacks Malicious Software Fishing	=	The transition from licensing to subscription sales of intellectual works for gaming industry via the Internet has made this sector more attractive to cybercriminals.

Source: systematized on the basis of [11].

According to the research by the Union Agency for the cybersecurity in 2020 cyber threats to all economic activities have increased significantly, due to isolation, distancing, growth of information and financial resources to overcome the COVID-19 pandemic. Cyber risks for various sectors of economy could be completely different, for example for households – Fishing, Information Leakage, Data Theft, and for industry –Malware, Web AppAttacks, Insider Threat (unintentional abuse) [11].

The type of actual cyber threats for each sector of economy also depends on the affiliation of stakeholders to individuals or legal entities. When dividing accounting information users into individuals and legal entities, it is necessary to take into account age parameters, organizational and legal form, respectively. Differentiated cyber threats are inherent in individuals of a certain age. Diverse age groups of stakeholders are characterized by special behavioral characteristics, that increase the impact of certain cyber risks. According to the age structure of stakeholders, it is advisable to rank them into groups: junior (up to 35 years old), middle (36-50 years old), senior (51-65 years old) and elderly (over 66 years old).

Younger users mainly receive information through social networks and messengers that requires limited use of them for business and management purposes. The middle age group is the most active among other stakeholders in using software to handle accounting information, as well as specialized in Internet pages. Such people are mostly at risk of virus and hacker attacks, which requires using anti-virus programs. Older stakeholders are more likely to be attacked by Fishing and Spam attacks via e-mail, as well as using payment services and bank cards. It is advisable to use firewalls, spam filters and additional verification systems for electronic transactions. Elderly users are more susceptible to fraudulent use of telephones (calls and messages), which requires the use of specialized software to filter telephone traffic.

It is clear that the isolation of cyber threats for each age group is conditional, but these risks are the most likely and typical for the relevant stakeholders at the same time. Due to

the age and behavioral characteristics users of accounting information are protected from some cyber risks and susceptible to others.

In the contrast to the age structuring of individuals, it is advisable for legal entities to apply the classification according to their organizational and legal form. In order to strengthen the cybersecurity of legal entities, it is expedient to divide into joint-stock companies (use and be sure to disclose large amounts of accounting information in accordance with law), companies (limited liability to counterparties), government agencies and institutions containing confidential information containing state secret), associations of enterprises (using a system of complex permanent communications between members of the association), non-entrepreneurial entities (have a significant informational impact on the social, cultural, domestic, religious functioning of society) [12, p.129].

Each group of business entities has different features of processing accounting information. Depending on the type of organizational and legal form, cyber threats are also different. For example, state institutions are subject to significant hacking attacks in order to steal state secret or harm national security. The separation of these groups makes it possible to identify the most likely cyber risks and develop preventive measures to ensure the cybersecurity.

An important criterion for classifying stakeholders is the type of communication channels used in terms of access to accounting information. Most modern business communications are implemented over the Internet. Accordingly, users (senders, recipients) of accounting information should be divided into persons who apply e-mails (various e-mail services), data exchange algorithms between accounting software products (e.g., data synchronization 1C: Accounting and MEDoc), social networks and messengers (Facebook, VK, Viber, Whatsapp, Telegram, etc.), file sharing and cloud storage (Dropbox, OneDrive, Google Drive, etc.), internal data network (local area network), physical media (paper documents, flash media, CDs).

The complexity of control actions depends on the type of communication channel traditionally used by stakeholders. Users of accounting information who exploit several channels of transmission (receipt) of information are exposed to more complex and frequent cyber risks. Information operations of some stakeholders, such as those using social networks and messengers, require permanent cyber security. Conversely, users of information on physical media are almost not exposed to cyber risks.

The classification of stakeholders by type of communication channels should also be used to restrict access to certain Internet services in the process of implementing functional responsibilities to prevent cyber threats. Additionally, there may be a nationwide ban for using Internet resources that could threaten country's cybersecurity. For example, in Ukraine, access to social networks VK, Odnoklasniki, mail.ru, file sharing and search engine Yandex, accounting software 1C: Accounting and many others have been banned as their usage may lead to the loss of information that contains trade and military secrets.

Besides the type of communication channel, the frequency of information acts is important for the cybersecurity. Depending on the frequency of requests or receipt of credentials, the likelihood of cyber threats increases. Therefore, it is advisable to separate stakeholders, to assess the necessary cybersecurity measures, from permanent (synchronization of information occurs on a regular basis), frequent (daily information exchange), periodic

ISSN 2786-4537 (print). Вісник економіки № 1, 2021 р.
ISSN 2786-4545 (online). Herald of Economics № 1, 2021

(transmission and receipt of information occurs at certain intervals: every week, end of month or quarter, etc.) and single communications (after the need for accounting information, for example, the investor once a year to search for investment objects).

The generalized classification of accounting information users is shown in table 3 by criteria: the ability to manage the activities of the business entity, the right of access, the likelihood of cyber threats, the ability to dispose of the right of access, access to accounting objects, functional law, information processing, economic activity, age of individuals, organizational and legal form legal entities, type of communication channels used, frequency of information acts.

Table 3

Classification of accounting information stakeholders in order to ensure the cybersecurity of enterprises

№	Classification criterion	Type of stakeholder
1.	Type of economic activity	Individuals / Households; Industry; Diversified Business; Public Administration, Defense, Social Services; Finance / Banking Business / Insurance; Healthcare / Medicine; Education; Information and Communication; Arts, Entertainment and Games
2.	Ability to manage the activities of the business entity	Persons who make management decisions; persons who do not take management decisions, but have a financial interest; persons without financial interest
3.	The right to access accounting information	With absolute rights; with full rights; with limited access; with free access
4.	The probability of cyber threats	With a high probability; a medium probability; a low probability
5.	Ability to dispose the right of access	Right provider; right recipient
6.	Access to account objects	With the right to access information about non-current assets; stocks; cash; receivables; payables; capital; salary; taxes and fees; income and expenses; more detailed objects
7.	Functional law	With the right to work with primary documents; carrying out control procedures; data systematization; analysis of indicators and decision-making; definition of accounting policies
8.	The order of information processing	With the right to: data entry; data editing; data management, data generalization, data transfer and archiving
9.	Age of an individual	Younger age group; middle age group; senior age group; elderly age group
10.	Organizational and legal form of a juristic entity	Corporations; business associations; government agencies and institutions; business associations; on-entrepreneurial entities
11.	Type of used communication channels	What to use: email; algorithms for data exchange between accounting software products; social networks and messengers; file sharers and cloud storage; internal data network; physical media
12.	Frequency of information acts	With permanent; with frequent; with periodic; with singles

Source: developed by the author.

Except for the proposed options for the division of stakeholders, the company's management can independently add to the list of arbitrary types of accounting information users that will meet security needs. Instead, some classification criteria, such as the number of full-time employees or the amount of profit, that are decisive in identifying different types of entities, do not affect the likelihood of cyber risks.

In the conditions of digital economy formation, economic entities carry out economic activity with minimal involvement of human resources. Information and economic processes in e-business enterprises are largely automated, and, therefore, the number of employees does not affect the manifestation of cyber threats and business profitability. The amount of profit also does not determine the likelihood of cyber threats. The need for the cybersecurity is similar for commercial, state, municipal or public institutions. Therefore, a separate classification of stakeholders by level of profitability is impractical for the organization of information security. Similarly, other criteria traditionally used to classify businesses are not relevant for the purposes of the cybersecurity at enterprises that requires further scientific substantiation and research.

Conclusions. Activation of cyber threats due to global hybrid conflicts, COVID-19 pandemic, economic imbalances, requires the organization of an effective system of enterprises' cyberdefense. The main object of cyber-attacks in digital economy is accounting information. Cyber threats are manifested at all stages of processing of accounting information and its transmission to users (stakeholders). To develop effective measures to minimize cyber threats, it is necessary to understand their impact on the functioning of stakeholders in terms of their various types.

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

Using the proposed classification of stakeholders helps to identify cyber risks; prevention, avoidance and minimization of the consequences of cyber threats, relevant for each type of accounting information users, that requires further research in terms of enterprises cybersecurity.

Література

1. Чухно І. С. Удосконалення класифікації користувачів звітності. *Облік і фінанси.* 2012. № 1. С. 85-90. URL: http://nbuv.gov.ua/UJRN/Oif_apk_2012_1_17.
2. Is cybersecurity about more than protection? EY Global Information Security Survey 2018–19. URL: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-global-information-security-survey-2018-19.pdf?download.
3. Шишкова Н. Л. Засоби підвищення керованості безпекою облікової інформації. *Економічний вісник Національного гірничого університету.* 2016. № 3. С. 119-127. URL: http://nbuv.gov.ua/UJRN/evngu_2016_3_17.

ISSN 2786-4537 (print). Вісник економіки № 1, 2021 р.
ISSN 2786-4545 (online). Herald of Economics № 1, 2021

4. Боримська К. П. Захист бухгалтерської інформації в обліковій політиці з метою оподаткування: організаційні аспекти. *Збірник наукових праць Національного університету державної податкової служби України.* 2013. № 2. С. 14-21. URL: http://nbuv.gov.ua/UJRN/znpnudps_2013_2_4.
5. Rasche, A. & Esser, D. (2006). From Stakeholder Management to Stakeholder Accountability. Journal of Business Ethics. 65. 251-267. 10.1007/s10551-005-5355-y.
6. Chikutuma, C. (2016). Integrated Reporting: A Story of Stakeholder Accountability. 5th International Conference on Accounting, Auditing, and Taxation (ICAAT 2016). DOI: https://doi.org/10.2991/icaat-16.2016.4.
7. 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.
8. Бухгалтерський облік в управлінні підприємством: навчальний посібник / О. А. Лаговська, С. Ф. Легенчук, В. І. Кузь, С. В. Кучер. Житомир: Житомирський державний технологічний університет. 2017. 416 с. URL: https://learn.ztu.edu.ua/mod/resource/view.php?id=17967.
9. Щирська А. Ю. Вимоги користувачів до якості облікової інформації. Економічний простір. 2018. № 139. С. 213-228.
10. El-Ebiary, Y. & Alawi, N. (2020). The Risks of Accounting Information Systems. International Journal of Engineering Trends and Technology. p. 2231-2381. DOI: https://doi.org/10.14445/22315381/CATI3P220.
11. Sectoral thematic threat analysis ETL2020. ENISA Threat Landscape. *European Union Agency for Cybersecurity.* URL : https://www.enisa.europa.eu/publications/sectoral-thematic-threat-analysis/at_download/fullReport. DOI: 10.2824/552242.
12. Муравський В.В. Вплив глобальних технологічних тенденцій на організацію обліку. *Вісник Тернопільського національного економічного університету.* 2017. № 4. С. 138–148. DOI: https://doi.org/10.35774/visnyk2017.04.138/

References

1. Chukhno I. S. (2012). Udoskonalennia klasyfikatsii korystuvachiv zvitnosti [Improving the classification of reporting users]. *Oblik i finansy. – Accounting and finance,* 1, 85-90. Retrieved from: http://nbuv.gov.ua/UJRN/Oif_apk_2012_1_17 [In Ukrainian].
2. Is cybersecurity about more than protection? EY Global Information Security Survey 2018–19. Retrieved from: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-global-information-security-survey-2018-19.pdf?download [In English].
3. Shyshkova N. L. (2016). Zasoby pidvyshchennia kerovanosti bezpekoiu oblikovoi informatsii [Means to improve the security of accounting information]. *Ekonomichnyi visnyk Natsionalnoho hirnychoho universytetu – Economic Journal of the National Mining University,* 3, 119-127. Retrieved from: http://nbuv.gov.ua/UJRN/evngu_2016_3_17 [In Ukrainian].
4. Borymska K. P. (2013). Zakhyst bukhhalterskoi informatsii v oblikovii polititsi z metoiu opodatkuvannia: orhanizatsiini aspekty [Protection of accounting information

in accounting policy for tax purposes: organizational aspects]. *Zbirnyk naukovykh prats Natsionalnoho universytetu derzhavnoi podatkovoi sluzhby Ukrainy. – Collection of scientific works of the National University of the State Tax Service of Ukraine,* 2, 14-21. Retrieved from: http://nbuv.gov.ua/UJRN/znpnudps_2013_2_4 [In Ukrainian].

5. Rasche, A. & Esser, D. (2006). From Stakeholder Management to Stakeholder Accountability. *Journal of Business Ethics.* 65. 251-267. DOI: https://doi.org/10.1007/s10551-005-5355-y [In English].
6. Chikutuma, C. (2016). Integrated Reporting: A Story of Stakeholder Accountability. 5th International Conference on Accounting, Auditing, and Taxation (ICAAT 2016). DOI: https://doi.org/10.2991/icaat-16.2016.4 [In English].
7. Shpak V.A. (2015). 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,* 2, 181-187. Retrieved from: http://nbuv.gov.ua/UJRN/boaa_2015_2_27 [In Ukrainian].
8. Bukhhalterskyi oblik v upravlinni pidpryiemstvom [Accounting in enterprise management] (2017); O.A. Lahovska, S.F. Lehenchuk, V.I. Kuz, S.V. Kucher. Zhytomyr: Zhytomyrskyi derzhavnyi tekhnolohichnyi universytet. 416 p. Retrieved from: https://learn.ztu.edu.ua/mod/resource/view.php?id=17967[In Ukrainian].
9. Shchyrska A. Yu. (2018). Vymohy korystuvachiv do yakosti oblikovoi informatsii [User requirements for the quality of accounting information]. *Ekonomichnyi prostir. – Economic space,* 139, 213-228 [In Ukrainian].
10. El-Ebiary, Y. & Alawi, N. (2020). The Risks of Accounting Information Systems. International Journal of Engineering Trends and Technology. 2231-2381. DOI: https://doi.org/10.14445/22315381/CATI3P220 [In English].
11. Sectoral thematic threat analysis ETL2020. ENISA Threat Landscape. European Union Agency for Cybersecurity. Retrieved from: https://www.enisa.europa.eu/publications/sectoral-thematic-threat-analysis/at_download/fullReport. DOI: https://doi.org/10.2824/552242 [In English].
12. Muravskyi V.V. (2017). Vplyv hlobalnykh tekhnolohichnykh tendentsii na orhanizatsiiu obliku [The impact of global technological trends on the organization of accounting]. *Visnyk Ternopilskoho natsionalnoho ekonomichnoho universytetu – Herald of Ternopil National Economic University,* 4, 138–148. DOI: https://doi.org/10.35774/visnyk2017.04.138 [In Ukrainian].

Статтю отримано 25 березня 2021 р.
Article received March 25, 2021