УДК 336.6:004.58
JEL Classification: M15, M42, O33

TATAR M.[1], PEREPELYTSIA Y.[2]

INFORMATION SECURITY AUDIT FOR ENTERPRISES INFORMATION ASSETS PROTECTION IN GLOBAL CHALLENGES CONDITIONS

DOI: https://doi.org/10.32620/cher.2023.1.05

Formulation of the problem. In the modern conditions of global challenges, along with climate action failure, extreme weather, human environmental damage, there are cyberattacks and data fraud or theft, the spread of infectious diseases (pandemics), which resulted in the activation of digitalization processes of social, economic and political processes in general and business entities financial and economic activity in particular. Modern business processes cannot be imagined without the use of information assets, because today they are becoming the most valuable resource for business development. However, in the conditions of modern global challenges and the state of war, there are more and more threats associated with the loss of access by business entities to the information assets of their own business, therefore the topic of enterprise information protection is an urgent issue that requires research and practical recommendations development. *The aim of the research is* analysis the enterprise's information security audit process and the development of practical recommendations for securing the enterprise's information assets in the global challenges conditions. *The methods of the research*: logical and meaningful method, methods of comparison, systematization, induction and deduction, analysis and synthesis, coefficient method. *The hypothesis of the research* was assumptions about the possibility of determining the state of information security of business assets through the enterprise vulnerability indicator and securing its information assets by conducting an information security audit. *The statement of basic materials*. The place of Ukraine in the World Digital Competitiveness Ranking was analyzed and the main weak points are identified. The model of building an information security system is presented. The enterprise information security indicators are considered. It is proposed to identify the state of security of the enterprise's information assets using the company's vulnerability indicator. It is proposed to conduct an audit of the enterprise's information security in four interrelated stages, which will make it possible to protect the company's information assets from potential threats and attacks by intruders. *The originality and practical significance of the research* confirmed by research and substantiation of the importance of the enterprises information assets protecting in the conditions of martial law and recommendations for the information assets securing from potential threats using the enterprise vulnerability indicator and conducting regular information security audit. *Conclusions and perspectives of further research*. It was determined that the company's information threats can be identified using a vulnerability indicator, and the company's information assets can be secured by applying an information security audit of its assets. Further research will be aimed at a more extensive analysis of factors that can influence the determination of the enterprise's vulnerability and the emergence of potential costs from cyber attacks and data theft.

Keywords:
information security audit, global challenges, information asset, information system, vulnerability indicator, cyberattacks, business entities.

[1] **Татар Марина Сергіївна,** канд. екон. наук, доцент, доцент кафедри фінансів, обліку і оподаткування, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Tatar Maryna, Ph.D. of Economic, Associate Professor, Associate Professor of the Finance, Accounting and Taxation Department, National Aerospace University «Kharkiv Aviation Institute», Kharkiv, Ukraine.

ORCID ID: https://orcid.org/0000-0002-1111-7103

e-mail: m.tatar@khai.edu

[2] **Перепелиця Юліанна Геннадіївна,** здобувач другого (магістерського) рівня вищої освіти спеціальності 071 «Облік і оподаткування», Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», м. Харків, Україна.

Perepelytsia Yuliana, the recipient of higher education with the Master's degree, 071 Accounting and Taxation Speciality, National Aerospace University «Kharkiv Aviation Institute», Kharkiv, Ukraine.

ORCID ID: https://orcid.org/0000-0001-6684-161X

e-mail: y.g.perepelitsya@student.khai.edu

ЧАСОПИС ЕКОНОМІЧНИХ РЕФОРМ № 1(49)/2023 ISSN 2221-8440

АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ АКТИВІВ ПІДПРИЄМСТВ В УМОВАХ ГЛОБАЛЬНИХ ВИКЛИКІВ

Постановка проблеми. У сучасних умовах глобальних викликів поряд зі зміною клімату, екстремальними погодними явищами, викликаними людськими діями, є кібератаки та шахрайство або крадіжка даних, а також поширення інфекційних хвороб (пандемії), що мали наслідком активізацію процесів діджиталізації суспільно-політичних процесів в цілому та фінансово-господарської діяльності суб'єктів господарювання зокрема. Сучасні бізнес-процеси неможливо уявити без використання інформаційних активів, адже сьогодні вони стають найціннішим ресурсом для розвитку бізнесу. Проте в умовах сучасних глобальних викликів та воєнного стану виникає все більше загроз, пов'язаних із втратою суб'єктами господарювання доступу до інформаційних активів власного бізнесу, тому тематика захисту інформації підприємства є актуальним питанням, що потребує дослідження та розробки практичних рекомендацій. *Мета дослідження* спрямована на аналіз процесу аудиту інформаційної безпеки підприємства та розробку практичних рекомендацій щодо убезпечення інформаційних активів підприємства. *Методи дослідження*: логічно-змістовний метод, методи порівняння, систематизації, індукції та дедукції, аналізу та синтезу, коефіцієнтний метод. *Основною гіпотезою дослідження* стало припущення щодо можливості визначення стану інформаційної безпеки активів бізнесу через індикатор вразливості підприємства та убезпечення його інформаційних активів шляхом проведення аудиту інформаційної безпеки. *Виклад основного матеріалу*. Проаналізовано місце України в Світовому рейтингу цифрової конкурентоспроможності й визначено основні слабкі місця. Представлено модель побудови системи інформаційної безпеки. Розглянуто показники інформаційної безпеки підприємства. Запропоновано здійснювати ідентифікацію стану захищеності інформаційних активів підприємства за допомогою індикатора вразливості підприємства. Запропоновано проведення аудиту інформаційної безпеки підприємства у чотири взаємопов'язані етапи, що дозволить убезпечити інформаційні активи підприємства від потенційних загроз та атак з боку зловмисників. *Оригінальність та практична значимість* підтверджується дослідженням та обґрунтуванням важливості захисту інформаційних активів підприємств в умовах воєнного стану та рекомендаціями убезпечення інформаційних активів підприємства від потенційних загроз за допомогою індикатору вразливості підприємства та проведення регулярного аудиту його інформаційної безпеки. *Висновки та перспективи подальших досліджень.* Визначено, що ідентифікувати інформаційні загрози підприємства можна за допомогою індикатора вразливості, а убезпечити інформаційні активи підприємства рекомендовано шляхом застосуванням аудиту інформаційної безпеки його активів. Подальші дослідження будуть спрямовані на комплексний аналіз чинників, що можуть впливати на врівень вразливості підприємства та появу потенційних витрат від кібератак та крадіжки даних.

Ключові слова:

аудит інформаційної безпеки, глобальні виклики, інформаційний актив, інформаційна система, індикатор вразливості, кібератаки, суб'єкти господарювання.

Formulation of the problem. In the modern conditions of global challenges, along with climate action failure, extreme weather, human environmental damage, there are cyberattacks and data fraud or theft, the spread of infectious diseases (pandemics), which resulted in the activation of digitalization processes of social, economic and political processes in general and business entities financial and economic activity in particular. The availability of information creates numerous risks, each of which is aimed at establishing access to information assets, again, in order to obtain certain benefits. Information is the most widespread and needing protection resource in the company's activities, since it is the information assets that accumulate, update and store data about the company's creditors, debtors, suppliers, consumers of goods and/or services and other counterparties, and information of a technical and financial nature, representing a commercial value, the disclosure of which may harm the interests of the enterprise and cause the appearance of numerous risks for its activities, including reputational ones. The security of enterprise information assets (EIA) can be affected by many factors, which researchers often classify as sources of threats to the information resources security. In modern conditions, the main threat is uncertainty, which is explained by the current global challenges and martial law regime. It is quite logical that in such conditions, the potential possibility of capture of EIA by third parties is growing rapidly, which justifies the need

ЧАСОПИС ЕКОНОМІЧНИХ РЕФОРМ №1(49)/2023 ISSN 2221-8440

to develop practical recommendations for the EIA protection.

Analysis of recent research and publications. The results of studies of the business information assets protection features by conducting an audit of its information security are reflected in the papers of many researchers, such as: S.O. Hnatiuk, O.G. Korchenko, S.V. Kazmirchuk, V. M. Panchenko, S. V. Melnyk, S. M. Yaremko, O. M. Kuzmina, E. I. Lapinska, R. A. Kalyuzhny, A. A. Dmitriev, Y. V. Roy, N. V. Mazur, P. M. Skladanniy, V. I. Shulga and others. Most of the scientific developments revealed the features of the protection of business information assets without taking into account the latest political and economic changes, which are now having a significant negative impact on business activities. Therefore, the issue of EIA protection in the conditions of global challenges requires practical recommendations development.

Determining the need to involve specialists in the enterprise information security audit by calculating the indicator of the vulnerability of the enterprise was not considered in the above-mentioned scientific papers. This creates interest in the issue of protection of EIA and possible ways of securing them. Therefore, in the conditions of martial law, the search for effective tools to protect the company's information assets is currently an insufficiently resolved and multifaceted problem that requires complex research and effective proposals.

The purpose of the article is aimed at analyzing the enterprise's information security audit process and the development of practical recommendations for securing the enterprise's information assets in the global challenges conditions.

Presentation of the main research results. Unfortunately, Ukraine ranks low in 2017-2021 in the World Digital Competitiveness Ranking (from 64 countries) (Table 1). Due to the limited reliability of the data collected in 2022, Russia and Ukraine are not included in this edition of the Ranking.

Table 1 – **Ukraine ranks in the World Digital Competitiveness Ranking**

Overall and factors	Years				
	2017	2018	2019	2020	2021
Overall	60	58	60	58	54
Factors					
Knowledge	45	39	40	38	37
Technology	62	61	61	59	58
Future readiness	61	61	62	61	58

Source: developed by the authors based on [10]

The results of the rating confirm the need to increase Ukraine’s digital competitiveness and ensure information security, especially in order to adapt and face global challenges.

"Information security" as a concept first appeared at the end of the 80s of the 20th century and, in the context of an information threat, was studied by the German scientist H. Oderman [5].

The concept of information security as a state of protection of information and the infrastructure that supports it from accidental or intentional actions of a natural or artificial nature that can cause unacceptable damage to subjects of information relations, in particular, owners and users of information and infrastructure was provided by V.A. Luzhetsky [4].

Along with this, R.A. Kalyuzhnyi understands information security as a type of public informational legal relations regarding the creation, support, protection of safe living conditions desired for people, society and the state, special legal relations related to the creation, storage, distribution and using information [8]. It is worth noting that this interpretation most accurately describes the essence and importance of information security for both individuals and business entities and the state.

In this context, it is appropriate to present the interpretation of the concept of "information security" in the Ukrainian legislative framework. Thus, according to the Concept of the national informatization program, approved by the Law of Ukraine dated February 4, 1998 No. 75/98 [2], "information security" is an integral part of political, economic, defense and other components of national security. The objects of information security are information resources, telecommunications, channels of information exchange, functioning of telecommunication networks and systems, and other elements of the country's information infrastructure.

ЧАСОПИС ЕКОНОМІЧНИХ РЕФОРМ № 1(49)/2023 ISSN 2221-8440

ЧАСОПИС ЕКОНОМІЧНИХ РЕФОРМ №1(49)/2023 ISSN 2221-8440

Considering this, it can be assumed that the information security of each enterprise is an element of the information security of the state. Considering the essence of information security from this point of view, it is worth concluding that in the conditions of martial law, the information security of each individual enterprise acquires special importance, as a component of the state information security, which emphasizes the importance of its protection.

A generally accepted interpretation of the concept of "enterprise information security audit" has not yet been formed, however, it can be provided based on the essence of this concept. Thus, it can be determined that an enterprise information security audit is a process of collecting, systematizing and verifying information about the security of the EIA, with the aim of providing an objective assessment of the level of security of the company's information resources and developing practical recommendations for eliminating sources of threats to the enterprise's security, if they are detected.

The importance of protecting information systems is reinforced by the global trend towards an increase in the number of information attacks, which can cause significant material and reputational costs for the enterprise. According to the statistics of the InfoWatch portal [3], only in the first half of 2018 there were 1039 incidents of data leakage around the world. At the same time, in the same period of time in 2010, three times less similar cases (only 382 incidents) were recorded. These statistics clearly indicate that the information security of any company comes under new threats every year. The enterprise management must take timely measures for information protection of data, which will depend on the prospects for the enterprise development.

The presented in the article model of building an information security system (Figure 1) reflects the interaction of the main subjects and objects of information security, and their influence on the state of information security and the preservation of material or information assets.

In order to protect the enterprise from potential threats of such attacks, there is an actively developing practice of the enterprise information security audit, which makes it possible to objectively assess the level of security of the enterprise's information system. The classification of types of enterprise information security audit is shown in Figure 2.

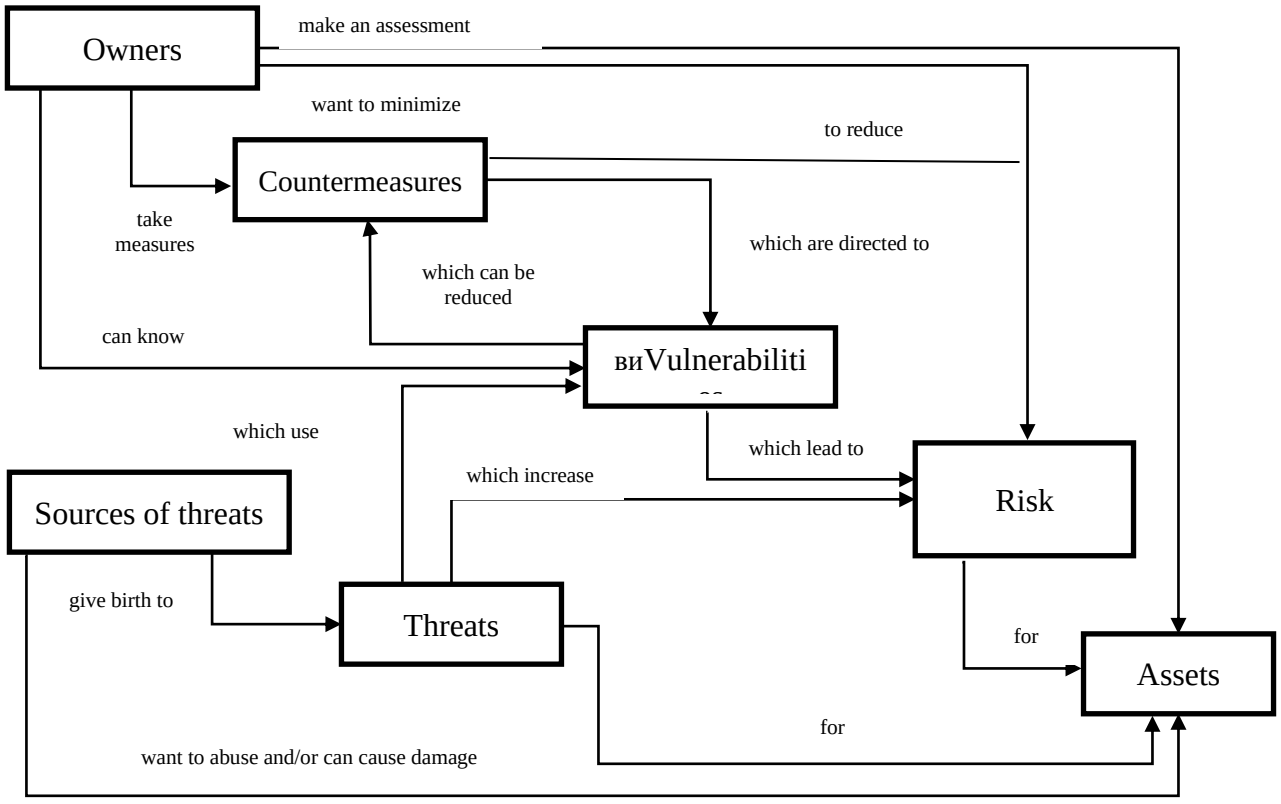

Figure 1 – The model of building an information security system
Source: developed by the authors.

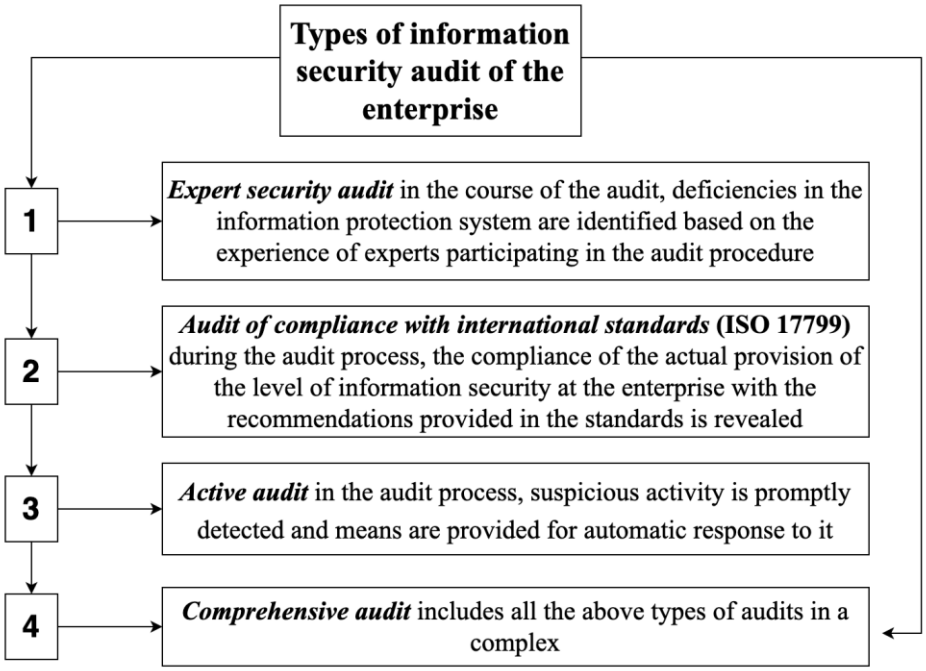

Figure 2 – Types of enterprise information security audit
Source: [1, 3]

As researchers [1, 3, 9] noted any of those types of audit can be carried out both individually and complex, depending on the specific needs of the business. In the conditions of global challenges and martial law, it is advisable to apply a complex audit, since this form of information security audit provides the maximum analysis of the security of the company's information assets.

Regardless of the enterprise's field of activity, its type, tasks and goals, an information security audit often affects the following work aspects:

- the rights of employees to access servers and databases of collective use;
- methods of confirming each user's login (authentication);
- principles of data backup;
- configuration and setting of network devices, data storage and transmission systems;
- the operation of antivirus and anti-spyware software, the availability of a license;
- theoretical and practical knowledge of company employees about data protection.

As a result, a complex audit of information security will help reveal how effective the company's personal and corporate data protection system is. If it has no weak points, the manager will receive confirmation of the security of the entire organization. But if the report shows hidden risks, then management needs to develop and implement an action plan to eliminate potential risks. In addition, high-quality analytics will help the company choose the most effective methods of data protection and reduce its costs in this area. However, regardless of the form of conducting a security audit, this process consists of four logically interconnected stages, presented in Figure 3.

Of course, all stages are important, but the second stage is the most important in the audit of the information security of the enterprise, since the quality of the security audit largely depends on the accuracy and completeness obtained in the process of collecting information.

The article proposes to consider the enterprise information security indicators (Table 2).

As indicators of information security level, such coefficients are also determined as:

– completeness of information (C), which is calculated as the ratio of the amount of information at the disposal of the person making the decision to the amount of information necessary for making this decision;

– accuracy of information (A), which is determined as the ratio of the amount of relevant (reliable) information to the total amount of available information;

ЧАСОПИС ЕКОНОМІЧНИХ РЕФОРМ № 1(49)/2023 ISSN 2221-8440

ЧАСОПИС ЕКОНОМІЧНИХ РЕФОРМ №1(49)/2023 ISSN 2221-8440

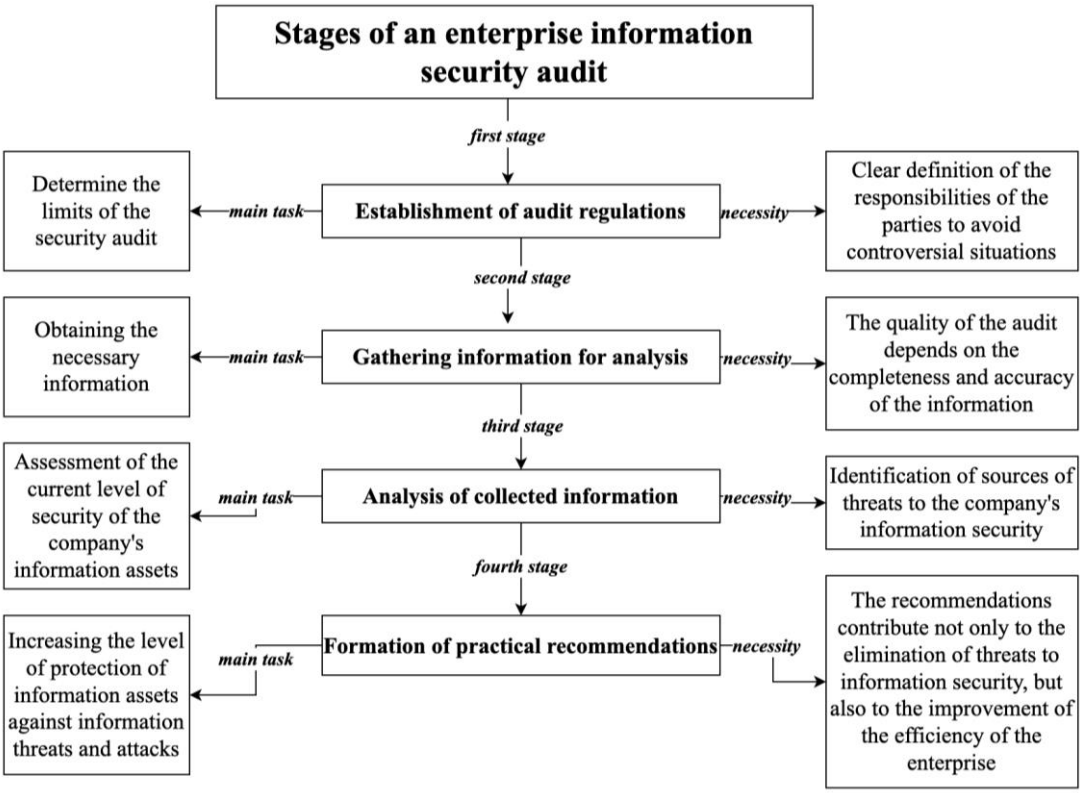

Figure 3 – Stages of an enterprise information security audit
Source: [1, 3].

Table 2 – **The enterprise information security indicators**

Indicator	Calculation formula
Information productivity coefficient (IPC)	$IPC = \frac{V_{ip}}{C_{ai}}$, where V_{ip} – volume of industrial production, hryvnias; C_{ai} – costs for the acquisition of information resources, hryvnias.
Information armament coefficient (IAC)	$IAC = \frac{C_{ai}}{N_{ea}} \times 100\%$, where C_{ai} – costs for the acquisition of information resources, hryvnias; N_{ea} – average number of employees, people Must be more than 20%.
Information security coefficient (ISC)	$ISC = \frac{C_{pi}}{C_{ai}} \times 100\%$, where C_{pi} – costs of the enterprise for the protection of information resources, hryvnias; C_{ai} – costs for the acquisition of information resources, hryvnias. Must be less than 20%.

Source: developed by the authors based on [9]

– inconsistency of information (I), which is determined as the ratio of the number of independent testimonies in favor of making a decision to the total number of independent testimonies in the total amount of relevant information.

For conducting the information security audit the enterprise needs to determine the degree of information security risk for attacks. It is assumed that the potential costs of an information attack cannot be determined without an IS audit. However, the company's financial results last year can give an idea of the company's vulnerability to attacks in the future. So, if the enterprise received a loss based on the results of the period's activities, first of all, the management will take actions to eliminate existing problems (repayment of debts, elimination of reputational risks, etc.), and not potential ones, which are the state of information

security. The unprofitable activity of the enterprise makes vulnerable not only its operational, financial and investment activities, but also creates potential threats of attacks on the information assets of the enterprise by fraudsters. Understanding the importance of ensuring the EIA security, it is possible to determine an indicator by which the enterprise should identify the state of information security and forecast potential costs for future periods. It is worth noting that the strategy of preparing the company for a potential attack on information assets and the amount of funds allocated in advance to attract information security auditors is more economically beneficial for the company than the actual information attack and the resolution of the consequences resulting from such attacks.

Therefore, this indicator of the company's vulnerability is a useful tool for the company to develop a risk management strategy for the following periods. The vulnerability indicator is expressed by the level of the financial result of the business (Table 3) and the corresponding level of the need to strengthen the control and security of the company's information assets.

Table 3 – **Indicator of enterprise information security according to the profitability of the enterprise**

№	Level of lost	Description	Necessity to ensure information security	Description
1	Small	(0-1% of the profit of the previous period)	Very low	At this stage, there is no urgent need to strengthen control over the company's information assets.
2	Moderate	(1-3% of the profit of the previous period)	Low	
3	Medium	(3-5% of the profit of the previous period)	Medium	At this stage, the cost of strengthening control over the company's information assets increases.
4	Large	(5-10% of the profit of the previous period)	High	At this stage, the company's information security is vulnerable. There is a need to strengthen control over the company's information assets.
5	Critical	(>10%)	Very high	At this stage, the company's information security is the most vulnerable. There is an urgent need to strengthen control over information assets

Source: developed by the authors

From the Table 3, we conclude that the financial result obtained by the enterprise in the past period is an indicator of the enterprise vulnerability to the procedure for conducting an information attack by fraudsters in the future. It should be noted that in the Table 3, the enterprise financial result is presented in the form of a loss, not a profit. This can be explained by the fact that in the conditions of martial law, shelling and irregular electric power outages become the cause of loss-making activities of enterprises.

Under the conditions of martial law, companies that are responsible for the country defense capability of need special attention, but such companies should not forget about their protection, namely their own information assets. The vulnerability indicators of the State Concern “Ukroboronprom” and some of its constituent enterprises, namely the Shepetiv Repair Plant, which specializes in the repair of rocket and artillery weapons systems, and the Artillery Weapons Design Bureau, whose main activity is the implementation of research, design and technological works aimed at creating modern samples of artillery and small-arms weapons and cartridges are calculated in Table 4.

From the Table 4, it can be concluded that enterprises providing defense capabilityof Ukraine are too vulnerable in 2021, due to which there is an urgent need to protect, in particular, the information assets of these enterprises in future periods.

Of course, it is possible to accurately determine the conduct of information attacks at the enterprise only with the involvement of specialists and conducting a detailed state of the enterprise's informational system, that is, an information security audit.

ЧАСОПИС ЕКОНОМІЧНИХ РЕФОРМ № 1(49)/2023 ISSN 2221-8440

Table 4 – **Determination of enterprises vulnerability indicator of the defense industry of Ukraine**

№	Enterprise	Financial result, thousand UAH		Level of vulnerability in 2021
		2020 year	2021 year	
1	SC "Ukroboronprom"	58890	(252709)	*Very high*
2	Shepetiv Repair Plant	85585	59461	*Very low*
3	Artillery Weapons Design Bureau	(11559)	8707	*Very high*

Source: developed by the authors based on [6]

The State Concern "Ukroboronprom" should pay attention to the state of its own information security, and the enterprises included in it and use the Tab. 1 in the forecast of risk management for the future period, because in the initial stages of an informational system threat, it is easier for management to cope with the consequences of potential attacks. Therefore, spending money on an information security audit is more appropriate than receiving losses from attacks and incurring reputational risks, declassifying internal information and losing potential customers.

Thus, it is proposed to carry out an audit of the company's information security, especially in strategic sectors of the economy, which will become an effective tool for protecting and securing the company's information resources from information attacks, especially in conditions of uncertainty caused by global challenges and martial law conditions. It is worth emphasizing that the audit of the company's information security is not a one-time event, but should take place on a regular basis, with a gradual increase in the protection of the company's information assets.

Conclusions and prospects for further research. Thus, it is proposed to apply the enterprise information security audit, which will make it possible to protect the information assets of the enterprise from potential threats and attacks by intruders. It is proposed to identify the state of information security using the vulnerability indicator. It was determined that it is advisable to conduct an information security audit comprehensively, using all possible types of audit. The audit process is proposed to be carried out in four interconnected stages. Further research will be aimed at a more extensive analysis of factors that can influence the enterprise information security audit and the formation of practical recommendations for ensuring the information assets security of enterprises of specific industries.

References

1. Korchenko, O.G., Hnatiuk, S.O., Kazmirchuk, S.V. and others. (2014). *Audit and management of information security incidents: training*. Manual. Kyiv: Center for Education and Science. and Science. editions of NA SB of Ukraine, 190.
2. The concept of the national informatization program (1998). Law of Ukraine No. 75/98. Retrieved from: https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80#Text. [Accessed 10 January 2023].
3. Kuzmina O.M., Yaremko S.A. (2020) Actual aspects of protection of information resources of business structures. *Bulletin of Khmelnytskyi National University*, 5, 238–242.
4. Lapinska Ye. I. (2019). Foreign experience of information protection in the field of entrepreneurship and its use in Ukraine. *State and Regions*, no. 3, pp. 174–177.
5. Martyn, O. (2012). Information security as a component of national security: theoretical approaches to its essence. *Information, communication, society*, 2, 1–2.
6. Official website of SC "Ukroboronprom". Financial reporting of enterprise 2020-2022. Retrieved from: https://ukroboronprom.com.ua/ [Accessed 10 January 2023].
7. Karpenko, E. A., Karpenko, O. V., Milka A. I. (2021). *Prospects for the development of accounting, analysis and auditing in the conditions of innovative information technologies*: a monograph.

ЧАСОПИС ЕКОНОМІЧНИХ РЕФОРМ №1(49)/2023 ISSN 2221-8440

Poltava: PUET, 410.

8. Roy, Y.V., Mazur, N.P., Skladanniy, P.M. (2018). Information security audit – the basis of effective protection of the enterprise. *Cybersecurity: education, science, technology*, 1, 86–93.

9. Shulga, V.I. (2015). Modern approaches to the interpretation of the concept of information security. *Efficient economy*, 4, 13.

10. World Digital Competitiveness Ranking. Available at: https://www.imd.org/centers/world-competitiveness-center/rankings/world-digital-competitiveness/ [Accessed 10 January 2023].

Література

1. Корченко О. Г., Гнатюк С. О., Казмірчук С. В. та ін. *Аудит та управління інцидентами інформаційної безпеки*: навч. посібник. Київ: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. 190 с.

2. Концепція національної програми інформатизації. Закон України № 75/98. 1998. URL: https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80#Text (дата звернення: 10.01.2023).

3. Кузьміна О. М., Яремко С. А. Актуальні аспекти захисту інформаційних ресурсів бізнес-структур. *Вісник Хмельницького національного університету*. 2020. № 5. С. 238–242.

4. Лапінська Є. І. Зарубіжний досвід захисту інформації у сфері підприємництва та його використання в Україні. *Держава та регіони*. 2019. № 3. С. 174–177.

5. Мартин О. Інформаційна безпека як складова національної безпеки: теоретичні підходи до її суті. *Information, communication, society*. 2012. № 2. С. 1–2.

6. Офіційний сайт ДК «Укроборонпром». Фінансова звітність підприємства за 2020-2022. URL: https://ukroboronprom.com.ua/.

7. *Перспективи розвитку бухгалтерського обліку, аналізу та аудиту в умовах інноваційних інформаційних технологій* : монографія / Є. А. Карпенко, О. В. Карпенко, А. І. Мілька [та ін.]. Полтава : ПУЕТ, 2021. 410 с.

8. Рой Я. В., Мазур Н. П., Складанний П. М. Аудит інформаційної безпеки–основа ефективного захисту підприємства. *Кібербезпека: освіта, наука, техніка*. 2018. №1(1). С. 86–93.

9. Шульга В. І. Сучасні підходи до трактування поняття інформаційна безпека. *Ефективна економіка*. 2015. № 4. С. 13.

10. World Digital Competitiveness Ranking. URL: https://www.imd.org/centers/world-competitiveness-center/rankings/world-digital-competitiveness/ (дата звернення: 10.01.2023).

Стаття надійшла до редакції : 25.01.2023 р.

Стаття прийнята до друку: 31.03.2023 р.

Бібліографічний опис для цитування :

Tatar M., Perepelytsia Y. Information security audit for enterprises information assets protection in global challenges conditions. *Часопис економічних реформ*. 2023. № 1(49). С. 35–43.