

Mishchuk Ie.

IMPROVEMENT OF THE METHODOLOGY FOR ASSESSING THE SAFETY OF THE ECONOMIC AND INFORMATION INTERESTS OF THE ENTERPRISE

Об'єктом дослідження є процес оцінювання безпеки економіко-інформаційних інтересів підприємства. У роботі уточнено її дефініцію. Ураховано, що ключовими об'єктами захисту виступають інформація, а також рівень використання інформаційних систем, при якому вони виконують усі покладені на них завдання, що сприяє досягненню загальних поточних і стратегічних економічних інтересів підприємства. З огляду на це, запропоновано в складі даного виду безпеки диференціювати безпеку інформації та безпеку інформаційної системи. Обґрунтовано, що оцінка рівня безпеки економіко-інформаційних інтересів підприємства повинна враховувати економічні наслідки недосягнення її бажаного рівня. Такі наслідки проявляються в нестачі прибутку до оподаткування. Остання має місце через використання застарілих інформаційних систем (порівняно з підприємствами-конкурентами) та недостатнє фінансування забезпечення функціонування діючих інформаційних систем. Установлено індикатори складників безпеки економіко-інформаційних інтересів підприємства. Наведено приклад вибору індикаторів для підприємств добувної галузі. Показано, що такий розповсюджений серед науковців індикатор як сума інформаційних витрат, використана в абсолютному вираженні, не відображає адекватно реальний стан рівня забезпечення економіко-інформаційних інтересів підприємства та, відповідно, їх безпеки. У роботі запропоновано коефіцієнт рівня безпеки економіко-інформаційних інтересів як відношення нестачі прибутку до оподаткування до мінімально необхідної для підприємства суми прибутку. Визначено шкалу переведення отриманих значень у лінгвістичні терми. На відміну від загальноприйнятої практики, показано, що мінімальний та катастрофічний рівні безпеки представляють собою низький та середній рівні небезпеки відповідно.

Результатом даного дослідження є удосконалена методологія оцінювання рівня безпеки економіко-інформаційних інтересів підприємства, в якій ураховані економічні наслідки для підприємства від недотримання даного виду безпеки. Застосування розробленої концепції розширює можливості управлінської аналітики, дозволяючи більш адекватно оцінити рівень безпеки економіко-інформаційних інтересів для прийняття управлінських рішень, спрямованих на його підвищення.

Ключові слова: рівень безпеки, економіко-інформаційні інтереси, індикатори безпеки, інформаційні системи, нестача прибутку.

Received date: 14.11.2019

Accepted date: 05.12.2019

Published date: 28.02.2020

Copyright © 2020, Mishchuk Ie.

This is an open access article under the CC BY license

<http://creativecommons.org/licenses/by/4.0>

1. Introduction

The information component of the economic security of the enterprise is important for the successful functioning of the enterprise, therefore it occupies a key place in the structure of economic security [1, 2]. So, at the end of June 2017, Ukrainian enterprises of various forms of ownership and sectors of the economy, as well as business entities of other countries subjected to large-scale hacker attacks: their work was blocked by the DOS/Petya.A virus. The number of cases of computer infection with this virus as a percentage of the total in Ukraine is 75.24 %, Germany – 9.06 %, countries outside Europe – 2.94 % [3]. Despite the influence of information systems on the results of not only managerial work, but also of the entire production process, there are no unified approaches to assessing their safety, justifies the relevance of the study. So, *the object*

of research is the process of assessing the safety of the economic and information interests of the enterprise. *The aim of research* is improvement of the methodology for assessing the security of economic and information interests of the enterprise.

2. Methods of research

The dialectic method, the analysis and synthesis method are used – in the study and generalization of scientific concepts for determining and evaluating the information component of the economic security of an enterprise.

3. Research results and discussion

The security of economic and information interests is characterized by a state in which such a level of use of

information systems is achieved that they fulfill all the tasks assigned to them, contributes to the achievement of the current and strategic economic interests of the enterprise. This, unlike the existing ones, in particular [4, 5], does not contain an emphasis on users of the system. Given the concretization of the objects of protection, let's believe that it is more appropriate to differentiate information security and information system security within this type of security.

Non-compliance with the regime for ensuring the security of economic and information interests depends on the level of costs of informatization [6, 7]. However, it is obvious that the implementation of threats to this type of security generate a loss of profit. Therefore, the concept of assessing the security of economic and information interests has been proposed, in contrast to the well-known assessment of the protection of computer systems and information technologies [8, 9] based on the methodology of the authors of [10]. This technique involves the assessment of the lack of profit obtained in case of failure to achieve the relevant safety indicators of their normative values. However, paradoxically, its developers did not apply this technique to the information component of security. Using the principle underlying it, instead of the lack of operating profit or the *EBITDA* value as in [10], let's consider it more expedient to assess the lack of the *EBT* indicator – earnings before tax. The choice of this particular indicator is due primarily to the fact that it has the same analytical advantages and net profit, but it can be applied to enterprises with different tax systems. So, let's propose the shortcoming of the electronic computer for the safety of the economic and information interests of the enterprise to be defined as the maximum shortcoming, estimated by its components:

$$\Delta EBT(SEII) = \max\{\Delta EBT(SE); \Delta EBT(SEI)\}, \quad (1)$$

where $\Delta EBT(SEII)$ – the lack of the EBT sum for the safety of economic and information interests of the enterprise, c. u.; $\Delta EBT(SE)$ – the lack of the amount of electronic computers for the security of enterprise information, c. u.; $\Delta EBT(SEI)$ – the lack of the amount of EBT for the security of the enterprise information system, c. u.

In order to assess the indicators of the shortage of electronic computers, it is necessary to establish appropriate indicators that embody a specific type of economic interest, which corresponds to a certain type of security. It is advisable to take into account that at industrial enterprises (such as, for example, mining enterprises), those decision-makers are highly qualified and experienced specialists in their field. The same applies to analysts and other management personnel responsible for processing incoming information. The above is due to a balanced personnel policy of these enterprises. At the same time, many scientists propose indicators such as coefficients of completeness, accuracy, inconsistency, or relevance of information to assess the safety associated with information. Let's believe that their use is more appropriate when choosing management measures, while being significant in the financial sector (including budgeting) and in making strategic decisions. However, for industrial enterprises, the observance of high values of these coefficients is difficult only in individual critical cases associated with a lack of time and the need for

a quick response from the management team of the enterprise. In general, in the mode of current functioning, the information exchange on the operational activities of Ukrainian industrial enterprises is established in such a way that it does not adversely affect their economic security. Therefore, the above coefficients are not considered in this paper. But it is more appropriate to update the assessment of indicators related to the impact on the economic interests of the enterprise of the consequences of the implementation of information threats. These include: a round of insider information, loss of resources through unscrupulous actions of individuals through manipulations in the information space, as well as failures in the operation of information systems. It is possible to assess the effect of a leak of insider information (trade secrets) on the lack of an *EBT* indicator, as well as on other economic indicators, if there is a realized fact of such a leak. The consequences of non-observance of trade secrets differ depending on two groups of circumstances. The first group is determined by the content of information that was disclosed without the consent of its disclosure or lost in another way. The second group is determined by the fact that competitors (or other interested parties) will have time to use such information before the company implements appropriate measures to minimize (eliminate) these consequences. It should be borne in mind that the information classified by the enterprise as a trade secret may contain a variety of data: terms of mergers and acquisitions, terms of business contracts, loan terms and the like. So the cost of this information and the severity of the consequences of its disclosure are different. At the same time, the presence of laid-off workers for disclosing insider information is not an indicator that clearly characterizes the decrease in security associated with information. On the one hand, on the contrary, such an indicator testifies to the purposeful activity of the enterprise to identify such persons, and therefore to work to maintain a certain level of security. In addition, working employees of the enterprise are not the only source of information leakage, besides them, previously dismissed employees, buyers, suppliers and other stakeholders of the enterprise may be such entities. Moreover, in modern conditions of development of information technologies, the technical capabilities of unauthorized (illegal) seizure of information constituting a commercial secret are expanding. On the other hand, as indicated above, the deterioration of the economic results of the enterprise due to unauthorized information leakage is probabilistic, and the extent of such deterioration depends on the content of the information and the specifics of the enterprise. The most sensitive to the consequences of the disclosure of insider information (trade secrets) are enterprises which shares are quoted on the market. In addition, to assess the security of information, it is advisable to have a certain data set of a retrospective nature, while at the industrial enterprises of the extractive industry such incidents are practically absent, which makes it impossible to accumulate statistical data. Given all of the above, information security assessment is updated for enterprises which shares are listed on the stock market, as well as those enterprises which value is significantly affected by their reputation. In this regard, for enterprises that are investigated in this work, this type of security is not further evaluated.

The security of an information system can be assessed using various indicators. To determine the most appropriate of them, it is necessary to take into account the goal of ensuring this security subspecies. This goal is to contribute to the achievement of the economic interests of the enterprise by directly qualitatively and efficiently fulfilling all the tasks assigned to it by the enterprise information system. Obviously, achieving such a goal requires corresponding costs, which can be one-time and systematic. One-time costs are mainly capital costs for the acquisition, installation of an information system, consulting services for training personnel to use it, and some others.

When a company management decides to acquire a new, modern information system that would contribute to the achievement of its strategic interests, it is necessary to evaluate the amount of relevant investments. However, unlike the authors of [7], let's believe that it is impractical to consider the absolute amount of costs for an information system. Without taking into account the additional effect obtained from the use of this information system, such an amount will only reduce the financial result of the period in which it is incurred. In addition, the introduction of modern information systems at industrial enterprises is a large-scale investment project, which will take several years to recoup. In this regard, the amount of such investments is not advisable to take into account when assessing the security of the current economic interests of the enterprise. Instead, it is more appropriate to take into account those expenses that are mainly systematic and arise in the current period.

Systematic costs associated with maintaining the functioning of this information system at a high level and its development, which includes the costs of its maintenance, maintenance (including the cost of labor of the relevant IT specialists), modernization, if necessary, and the like. However, they should be taken into account in relation to a specific base by determining a certain coefficient. However, not all existing coefficients are considered appropriate for use. In particular, let's consider the use of the profitability of the information system, in which net profit and expenses related to the functioning of the information system to be related, to be insufficiently justified to assess the security of economic and information interests or its parts. This is explained by the fact that an increase in this profitability can be achieved by reducing costs associated with the content of the information system. However, such measures usually lead to an increase in the vulnerability of the latter and, as a result, a decrease in the overall level of security.

It should be noted that at Kryvbas mining and processing plants (except for the joint-stock company Southern Mining and Processing Plant, Kryvyi Rih, Ukraine), automated SAP ERP systems are introduced, which are one of the most advanced not only in managing financial flows, but also in production and technological processes. Therefore, their use helps to increase the overall productivity of the enterprise, obviously. In this regard, let's propose to take into account the coefficient of labor productivity ratio in the current amount of expenses for maintaining the information system at the proper level (ITs) when assessing the deficiency of the EBT indicator for the security of the information system. At the same time, the sum of such expenses should not be equal to zero: $ITs \neq 0$. If a situation does occur, then a conclusion is drawn about the

danger in the enterprise information system. Otherwise, it is advisable to evaluate the value of the ratio of labor productivity (LPr) to the current amount of expenses for maintaining the information system at the proper level (ITs). As the limiting (minimum) value of this coefficient ($L(K_{IT})$), let's establish its industry average value during the evaluation period. Provided that the obtained liminal values ($L(K_{IT})$) exceed the actual value of this coefficient ($K_{IT}a$): $L(K_{IT}) > K_{IT}a$, it is necessary to establish the amount of shortage of the EBT indicator according to the proposed formula:

$$\begin{aligned} \Delta EBT(K_{IT}) &= EBTa - EBTa \cdot \frac{K_{IT}a}{L(K_{IT})} = \\ &= EBTa \cdot \left(1 - \frac{K_{IT}a}{L(K_{IT})} \right), \end{aligned} \quad (2)$$

where $\Delta EBT(K_{IT})$ – the lack of the EBT indicator by the ratio of labor productivity to the current cost of maintaining the information system at the proper level, c. u.; K_{IT} – the value of the ratio of labor productivity in the current amount of expenses for the maintenance of the information system at the proper level, h.

In addition, one should take into account the fact that the authors of [10] point out that enterprises in the extractive industry, use less modern information systems compared to SAP ERP, annually lose 10 % of the profitability of their activities. Therefore, for such enterprises, it is necessary to additionally determine the magnitude of the EBT shortage obtained by using outdated information systems ($\Delta EBT(IT)$):

$$\Delta EBT(IT) = 0.1 \cdot OCa, \quad (3)$$

where OCa – the actual amount of operating costs.

The amount of shortage of the EBT indicator for the security of the enterprise information system ($\Delta EBT(SEI)$) will be determined by the expression:

$$\Delta EBT(SEI) = \max\{\Delta EBT(K_{IT}); \Delta EBT(IT)\}. \quad (4)$$

Due to the fact that it is proposed not to separately determine information for industrial enterprises, in particular for enterprises of the extractive industry, the total amount of shortage of the EBT indicator for the safety of economic and information interests ($\Delta EBT(SEII)$) is equal to the lack of an EBT for information system security:

$$\Delta EBT(SEII) = \Delta EBT(SEI). \quad (5)$$

In the future, it is necessary to assess the limiting value of the EBT indicator for the safety of economic and information interests ($EBT(SEII)l$):

$$EBT(SEII)l = EBTa + \Delta EBT(SEI), \quad (6)$$

where $EBTa$ – the actual EBT value, c. u.

Let's offer the level of security of the economic and information interests of the enterprise ($P(SEII)$) determined by the expression:

$$P(SEII) = 1 - \frac{\Delta EBT(SEII)}{EBT(SEII)l}. \quad (7)$$

A qualitative interpretation of the results is carried out on a scale:

- when $P(SEII)=0$ – a catastrophic level of security of economic and information interests of the enterprise, it is the average level of danger;
- at $0 < P(SEII) < 0.25$ – a minimum level of security of the economic and information interests of the enterprise, it is also a low level of danger;
- at $0.25 \leq P(SEII) < 0.5$ – a low level of security of economic and information interests of the enterprise;
- at $0.5 \leq P(SEII) < 0.75$ – an average level of security of the economic and information interests of the enterprise;
- at $0.75 \leq P(SEII) < 1.0$ – a high level of security of the economic and information interests of the enterprise;
- when $P(SEII)=1.0$ – a very high level of security of economic and information interests of the enterprise.

4. Conclusions

The definition of security of economic and information interests and its classification has been clarified. The methodology for assessing this type of security has been improved based on the ratio of the maximum amount of shortfalls in the profit of electronic computers resulting from the use of outdated information systems and insufficient funding to ensure the functioning of existing information systems in the limiting value of electronic computers. Application of the developed concept expands the capabilities of managerial analytics, allowing more adequately assess the level of security of economic and information interests for making managerial decisions aimed at increasing it.

References

1. Mantsurov, I. H., Nusinova, O. V. (2011). Pobudova hierarkhichnoi struktury skladovykh ekonomichnoi bezpeky pidpriemstv. *Efektivna ekonomika*, 9. Available at: <http://www.economy.nayka.com.ua/?op=1&z=680>
2. Denysenko, M. P. (2013). Alhorytm formuvannya systemy ekonomichnoi bezpeky turystychnoho pidpriemstva. *Investytsii: praktyka ta dosvid*, 24, 92–95.
3. Strutynska, V. (2018). Khakerski ataky: chy ye zhyttia pislya nykh? *Nadzvychna sytuatsiia+*. Available at: <https://ns-plus.com.ua/2018/07/05/hakerski-ataky-chy-ye-zhyttia-pislya-nyh-2/>
4. Marushchak, A. I. (2011). Informatsiino-pravovi napriamy doslidzhennia problem informatsiinoi bezpeky. *Derzhavna bezpeka Ukrainy*, 21, 92–95.
5. Kharchenko, L. S. (2004). *Informatsiina bezpeka Ukrainy: Hlo-sarii*. Kyiv: Tekst, 136.
6. Shynkarenko, A. Yu., Stavytskyi, O. V. (2017). Kiberbezpeka yak odyin z mekhanizmiv zabezpechennia stabilnoho rozvytku ekonomiky v Ukraini. *Aktualni problemy ekonomiky ta upravlinnia*, 11. Available at: <http://ape.fmm.kpi.ua/article/view/102862/97979>
7. Nusinov, V. Ya., Astafieva, K. O., Nusinova, O. V. (2015). *Otsinka rivnia ekonomichnoi bezpeky pidpriemstva na vsikh etapakh rozvytku*. Kryvyi-Rih: FOP Cherniavskiy D. O., 187.
8. *Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD* (1985). Available at: <http://csrc.nist.gov/publications/history/dod85.pdf>
9. *Information Technology Security Evaluation Criteria. Vol. 1.2. – Office for Official Publications of the European Communities* (1991). London: Department of Trade and Industry, 164.
10. Nusinova, O. V., Molodetska, O. M. (2011). *Kompleksna otsinka sotsialno-ekonomichnoi bezpeky pidpriemstv*. Kryvyi Rih: Dionis (FOP Cherniavskiy D. O.), 240.

Mishchuk Ievgeniia, PhD, Associate Professor, Department of Accounting, Taxation, Public Administration and Administration, Kryvyi Rih National University, Ukraine, ORCID: <http://orcid.org/0000-0003-4145-3711>, e-mail: tdutybz.077@gmail.com