Oleksandr Milov (Ukraine), **Stanislav Milevskyi** (Ukraine),
Hryhorii Kots (Ukraine)

ASSESSMENT OF THE UNEVEN USE OF INFORMATION RESOURCES IN THE BUSINESS PROCESS CIRCUIT

Abstract

An approach is proposed for assessing the uneven use of information resources in the organization's business processes. Formal representations of the organization's business processes and security systems are presented, reflecting both business operations carried out in a certain sequence and information resources that ensure the implementation of the relevant business operations, the place of information resources in the general outline of business processes is indicated. The circuits of the security system business processes of and the business processes of the main object of modeling are considered, including both business processes for managing security and business processes for ensuring security management. The assessment of the non-uniform use of information resources in a business process scheme is based on the consistent construction of an information resource incidence matrix for individual business operations, a frequency relationship matrix reflecting the sharing of information resources, and a matrix of derivatives in a discrete formulation. The proposed approach is demonstrated on a conditional example containing both the notional costs of information resources and weighting factors of the importance of business operations that reflect their criticality in the general contour of business processes. Estimates obtained as a result of applying the approach make it possible to group information resources, focusing on the frequency of their joint use in the business processes, which ultimately makes it possible to justify the choice of information resources for protection against threats from cyber intruders.

Keywords information resources, business process, security system, frequency matrix, discrete mathematics, threats, cyber-attacks

JEL Classification C65, G2, M15

О. В. Мілов (Україна), **С. В. Мілевський** (Україна), **Г. П. Коц** (Україна)

ОЦІНКА НЕРІВНОМІРНОГО ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ РЕСУРСІВ У КОНТУРІ БІЗНЕС-ПРОЦЕСІВ

Анотація

У статті запропоновано підхід до оцінювання нерівномірного використання інформаційних ресурсів у бізнес-процесах організації. Наведено формальні пояснення як бізнес-процесів і систем безпеки організації, що відображають виконання бізнес-операцій у певній послідовності, так і інформаційних ресурсів, які забезпечують виконання цих операцій. Визначено місце інформаційних ресурсів у загальній системі бізнес-процесів. Розглянуто контури бізнес-процесів системи безпеки та основного об'єкта моделювання, які містять у собі як бізнес-процеси для управління безпекою, так і ті, що пов'язані з забезпеченням цього управління. Оцінка нерівномірного використання інформаційних ресурсів у схемі бізнес-процесів заснована на послідовній побудові матриці інцидентності інформаційних ресурсів для окремих бізнес-операцій, частотної матриці відносин, що відображає спільне використання інформаційних ресурсів, і матриці похідних у дискретному формулюванні. Запропонований підхід продемонстровано на умовному прикладі, що містить як умовну вартість інформаційних ресурсів, так і вагові коефіцієнти важливості бізнес-операцій, що відображають їх значення в загальному контурі бізнес-процесів. Оцінки, отримані в результаті застосування підходу, дозволяють згрупувати інформаційні ресурси, орієнтуючись на частоту їх спільного використання в контурі бізнес-процесів, що зрештою дає змогу обґрунтувати вибір інформаційних ресурсів для захисту від кіберзловмисників.

Ключові слова інформаційні ресурси, бізнес-процес, система безпеки, частотна матриця, дискретна математика, загрози, кібератаки

Класифікація JEL C65, G2, M15

S. KUZNETS KHNUE

Founder

Simon Kuznets Kharkiv National University of Economics, Nauky avenue, 9-A, Kharkiv, 61166, Ukraine
http://www.hneu.edu.ua/

Received on: 2nd of December, 2019
Accepted on: 20th of December, 2019
Published on: 10th of April, 2020

Oleksandr Milov, Ph.D. in Technical Sciences, Professor of Cybersecurity and Information Technologies Department, S. Kuznets Kharkiv National University of Economics, Ukraine.

Stanislav Milevskyi, Ph.D. in Economics, Associated Professor of Cybersecurity and Information Technologies Department, S. Kuznets Kharkiv National University of Economics, Ukraine.

Hrihorii Kots, Ph.D. in Economics, Associated Professor of Cybersecurity and Information Technologies Department, S. Kuznets Kharkiv National University of Economics, Ukraine.

http://dx.doi.org/10.21511/ed.19(1).2020.02

INTRODUCTION

Information infrastructure is a central concept that defines the entire cycle of designing and operating a business system. The protection of information assets within the assets of an enterprise is a critical moment, the absence of which casts doubt on the very idea of the existence of an information structure. Therefore, the support and protection of the enterprise management system implies, first of all, the support and protection of the business processes themselves and the development of the infrastructure component of the business system, and in particular the information system, by overcoming the infrastructure and information fragmentation of the enterprise units (Evseev & Dorohov, 2011; Magomaeva, 2017; Milov & Korol, 2019; Stelmashonok, 2006).

The concept of information assets includes all technical and software, patents, trademarks and everything that allows employees to realize their production potential, as well as the relationship between the company and its major customers, government agencies, and other business entities. Protection of information assets consists in maintaining the integrity, accessibility and confidentiality of information in business systems (Evseev, Kots & Korol, 2015; Hamdan, 2013; Kotenko & Karsaev, 2001).

The analysis of possible threats showed that the information infrastructure should have the property of protecting the information used in business processes. This property characterizes the ability to provide protection against unauthorized (intentional or accidental) receipt, alteration, destruction or use of commercial, official or technological information.

The process-oriented approach to the creation (improvement) of the infrastructure for protecting information of business processes will allow us to consider the process of formation (development) of an information protection system as one of the auxiliary business processes that provide the basic processes of the enterprise. This makes it possible to develop an information protection infrastructure in close interconnection with the design of other business processes, which will undoubtedly increase their integration, flexibility, balance, and manageability (Rigin, 2012).

1. AIMS

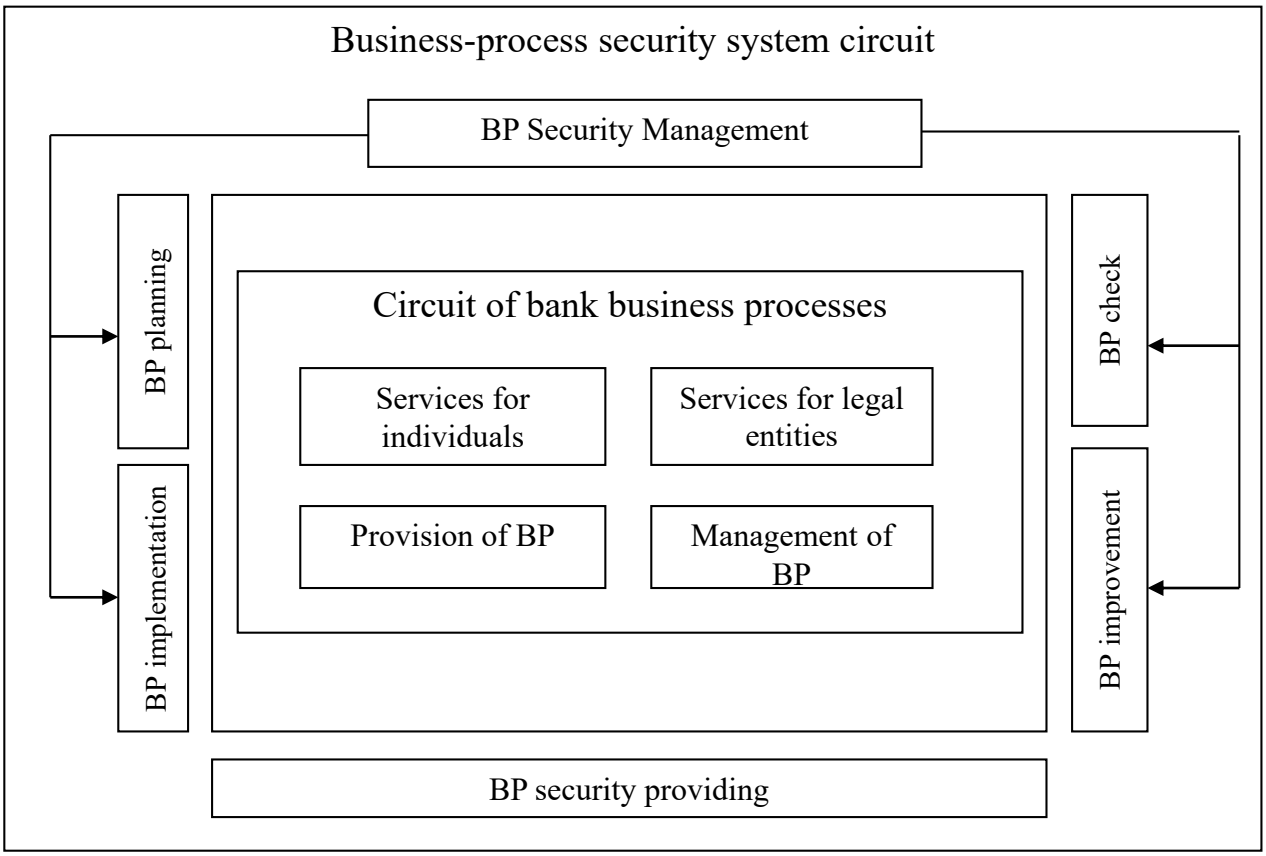
The existing systems of protection against business objects from cyberattacks are based on threat classifiers, which are largely focused on ensuring the security of information resources, as the goals of cyberattacks, and not on ensuring the security of business processes directly (Evseev, Rzayev, Mammadova, Samedov & Romashchenko, 2018; Yudin & Buchyk, 2015(a), 2015(b); Yudin, Buchyk, Chunarova & Varchenko, 2014). Because of this, a certain contradiction arises, consisting in the existence of a certain gap between the assessment of the security of the business process and the information resource used by it. This article attempts to jointly assess both information resources and the organization's business processes used, taking into account the fact that the same resource can be used in different business processes. The proposed approach is aimed at ensuring the security of business processes of the organization, allowing you to create a circuit of business processes of the security system (Evseev, 2016, 2019).

2. RESULTS

Consideration of the proposed approach should begin by presenting the outline of the organization's business processes, the security system and the place of information resources in them.

The circuit of the organization's business processes should be considered as the main object of cyber-attacks. An organization's business process circuit (BP) is a set of business processes and their implementation of information resources, the implementation of which in a given sequence leads to the achievement of the organization's goals, which can be described as follows:

http://dx.doi.org/10.21511/ed.19(1).2020.02



Source: Author's development.

Figure 1. The circuits of the business processes of the organization and the security system

$$S^{BP} = \left\{ \left\langle S^{BP_1}, IR^{BP_1}, T^{BP_1} \right\rangle, \ldots, \left\langle S^{BP_n}, IR^{BP_n}, T^{BP_n} \right\rangle \right\}, \quad (1)$$

where S^{BP} - is the loop of business processes as a set of BPs, each of which represents:

- S^{Bpi} - is the *i*-th business process, defined by the structure of relationships of individual business operations performed in a certain sequence;
- IR^{BPi} - a set of information resources of the *i-th* business process;
- T^{BPi} - a set of threats to the *i-th* business process.

Ensuring the protection of the organization's business processes can be represented similar to the BP contour, but not the security system. The security system business process circuit is a set of business processes and the resources necessary for them, the implementation of which ensures the normal functioning of the organization's business process circuit. This BP loop can be represented similarly, namely:

$$S^{BS} = \left\{ \left\langle S^{BS_1}, Rs^{BS_1}, T^{BS_1} \right\rangle, \ldots, \left\langle S^{BS_m}, Rs^{BS_m}, T^{BS_m} \right\rangle \right\}, \quad (2)$$

where S^{BP} is the circuit of business processes of the security system as a set of BPs, each of which represents, S^{BSi} - *i*-th business process defined by the structure of the links of individual business operations that are performed in a specific sequence in the security system, IR^{BSi} - a set of information resources protected by the *i*-th business process of the security system, T^{BSi} - a set of threats, the *i*-th business process of the security system provides protection against.

The relationship between information resources (IR) and the business processes in which they are used can be represented as an incidence matrix (A). Rows of this matrix correspond to information resources, and columns correspond to business processes. Matrix elements are defined as follows:

$$a_{ij} = \begin{cases} 1 \;\; if \;\; i-th \;\; resource \;\; is \;\; uaed \;\; by \;\; j-th \;\; process \\ \hline 0 \;\; in \;\; other \;\; cases \end{cases}. \qquad (3)$$

Let's consider a truncated version of the matrix of incentivities for the bank's business processes. As before, rows correspond to information resources, and columns correspond to business processes. Let there be 7 business processes and 5 information resources used in the framework of these business processes. The type of incident matrix for this case is presented in Table 1.

Table 1. Matrix of incidents of information resources for business processes

Source: Suggested by the authors.

Resources	Business processes						
	BP_1	BP_2	BP_3	BP_4	BP_5	BP_6	BP_7
R_1	1	1	–	–	1	1	–
R_2	1	–	1	1	–	1	1
R_3	–	1	1	–	1	–	1
R_4	1	1	–	1	1	–	1
R_5	1	–	1	1	–	1	–

The objective will be to ensure, with limited financial resources, the protection of as many business processes as possible through the protection of the information resources they use.

To solve this problem, the incident matrix must be supplemented with the cost indicators of each of the resources used (this is an estimate of the cost of protecting the corresponding resource). The incident matrix takes the following form (Table 2).

Table 2. Valuation of information resources incidental to business processes

Source: Suggested by the authors.

Resources	Business processes							The cost of the *i*-th resource (ci) (UAH)
	BP_1	BP_2	BP_3	BP_4	BP_5	BP_6	BP_7	
R_1	1	1	–	–	1	1	–	42.000
R_2	1	–	1	1	–	1	1	38.000
R_3	–	1	1	–	1	–	1	21.500
R_4	1	1	–	1	1	–	1	35.700
R_5	1	–	1	1	–	1	–	12.300

If we evaluate the cost of the corresponding business process based on the cost of the resources used by it, then in general terms the cost of the *j*-th business process can be calculated as:

$$C_j = \sum_{i=1}^{5} a_{ij} \cdot c_i. \qquad (4)$$

In the example, the costs of business processes are shown in the last line added (Table 3).

http://dx.doi.org/10.21511/ed.19(1).2020.02

Table 3. Business processes valuations

Source: Suggested by the authors.

Resources	Business processes							The cost of the *i*-th resource (ci) (UAH)
	BP_1	BP_2	BP_3	BP_4	BP_5	BP_6	BP_7	
R_1	1	1	–	–	1	1	–	42.000
R_2	1	–	1	1	–	1	1	38.000
R_3	–	1	1	–	1	–	1	21.500
R_4	1	1	–	1	1	–	1	35.700
R_5	1	–	1	1	–	1	–	12.300
Business process cost	127.300	99.200	71.800	86.000	99.200	92.300	95.200	–

Thus, using the incident matrix, an assessment was made of the value of business processes as the main activities (activities) of the company, bringing it surplus value.

It should be noted that business processes have different values for the organization, therefore, in addition to the cost indicators of the resources used, which can be entered into the used classification of threats, it is also necessary to set the importance (or value, or priority) of the corresponding business process. Supplementing the table used with weights of the importance of business processes (w_j), we can calculate the present values of business processes using the following expression (Table 4):

$$C_j = \sum_{i=1}^{5} a_{ij} \cdot c_i \cdot w_j . \qquad (5)$$

Table 4. Values of business processes

Source: Obtained by authors from previous tables.

Resources	Business processes							The cost of the *i*-th resource (ci) (UAH)
	BP_1	BP_2	BP_3	BP_4	BP_5	BP_6	BP_7	
R_1	1	1	–	–	1	1	–	42.000
R_2	1	–	1	1	–	1	1	38.000
R_3	–	1	1	–	1	–	1	21.500
R_4	1	1	–	1	1	–	1	35.700
R_5	1	–	1	1	–	1	–	12.300
Weight (value) of the business process (w_j)	1	1.2	1.1	1	1.25	1.3	1.1	–
Present value of a business process	127.300	119.040	78.980	86.000	124.000	119.990	104.720	

The obtained estimates of the present value of the organization's business processes make it possible to evaluate the value of business processes to determine the sequence of protection against cyber-attacks. However, it should be noted that the organization's business processes are not completely independent, since in the general case the same resource can be used in different business processes.

To correctly assess the relationship of the organization's business processes through shared resources and, based on this, determine the group of protected resources, we will use the methods of discrete mathematics and the theory of partially ordered systems (Gorbatov, 1976, 2000).

The intensity of the participation of information resources in the business processes of the organization will be characterized using the frequencies of their use. To do this, we introduce into consideration the frequency matrix of relations $F=[f_{ij}]_{n\cdot n}$ characterizing the model M, the incidence matrix of which is $A(M)=[a_{ij}]_{m\cdot n}$.

A frequency matrix of relations $F=[f_{ij}]_{n\cdot n}$ is a matrix, each row (column) of which is mutually associated with an information resource, and the element f_{ij} is equal to the number of business processes in which the i-th and j-th

information resources are used, if $i \neq j$, otherwise ($i=j$) - the number of business processes in which the i-th information resource is used. Moreover, if $i=j$, then f_{ij} is the natural frequency of the resource, if, then f_{ij} is the mutual frequency of the use of resources i and j. The greater the value of f_{ii}, the greater the importance of this resource for the organization's business processes. The frequency matrix F is symmetric with respect to the main diagonal. The greater the value of f_{ij}, the greater the importance of information resources of the i-th and j-th type for the contour of the company's business processes.

It can be shown that the frequency matrix of relations F, which characterizes the model, whose incidence matrix A satisfies the relation:

$$F=A^T \cdot A, \qquad (6)$$

where A^T – transposed matrix A.

For the above example, the frequency matrix of relations constructed with respect to information resources will have a dimension of 5x5 and will look as follows:

$$F = \begin{bmatrix} 4 & 2 & 2 & 3 & 2 \\ 2 & 5 & 2 & 3 & 4 \\ 2 & 2 & 4 & 3 & 1 \\ 3 & 3 & 3 & 5 & 2 \\ 2 & 4 & 1 & 2 & 4 \end{bmatrix}.$$

To build groups of business processes similar to each other in terms of information resources used, it is necessary to introduce the concept of a derivative over a pair of elements in a discrete formulation. Such a derivative is calculated according to the elements of the frequency matrix of relations as follows:

$$d_{ij} = \frac{f_{ii} - 2f_{ij} + f_{jj}}{f_{ij}}. \qquad (7)$$

This value shows the degree of uneven use of pairs of information resources in the circuit of the company's business processes. The matrix $D=|d_{ij}|$ has the following form:

$$D = \begin{bmatrix} 0 & 2.5 & 2.0 & 1.0 & 2.0 \\ 2.5 & 0 & 2.0 & 1.3 & 0.25 \\ 2.0 & 2.0 & 0 & 1.0 & 6.0 \\ 1.0 & 1.3 & 1.0 & 0 & 2.5 \\ 2.0 & 0.25 & 6.0 & 2.5 & 0 \end{bmatrix}.$$

The highest value in the resulting matrix is 6.0, corresponding to the pair (3, 5). As you can see from the original incident matrix, they are practically not shared in the business processes under consideration, therefore, joint protection of these resources will lead to the protection of different groups of business processes. While the resources included in the pair (2, 5) turn out to be similar in terms of using business processes. From this it follows that when building the protection of resource 2, it is necessary to protect resource 5, since they are used together in a group of business processes. An analysis of the obtained values of the matrix D will allow us to form groups of resources that require simultaneous protection for the normal functioning of the organization's business processes.

Thus, the proposed approach allows quantifying the uneven use of various information resources. Accounting for the resulting assessments can be used in constructing the circuit of business processes of the security system with the goal of efficiently distributing limited financial resources to protect the organization's business processes (Isaev, 2015; Weishaupl, Yasasin & Schiyen, 2015).

http://dx.doi.org/10.21511/ed.19(1).2020.02

CONCLUSION

The paper proposes an approach to assessing the uneven use of information resources in the organization's business processes. Formal representations of the business processes of the organization and the security system are given, the place of information resources is indicated. The assessment of the uneven use of information resources in the business process circuit is based on the construction of a frequency matrix of relations and the use of the concept of derivative in terms of discrete mathematics. The basis for their construction is the incidence matrix of information resources for business processes. The proposed approach is demonstrated using a conditional example. Estimates obtained as a result of applying the approach allow substantiating the choice of information resources for protection against threats of cyber-attacks.

AUTHOR CONTRIBUTIONS

Conceptualization: Oleksandr Milov.
Data curation: Stanislav Milevskyi.
Formal analysis: Oleksandr Milov.
Funding acquisition: Hryhorii Kots.
Methodology: Oleksandr Milov.
Project administration: Stanislav Milevskyi, Hryhorii Kots.
Investigation: Stanislav Milevskyi, Hryhorii Kots.
Resources: Stanislav Milevskyi.
Software: Stanislav Milevskyi.
Supervision: Oleksandr Milov.
Validation: Hryhorii Kots.
Visualization: Stanislav Milevskyi.
Writing – original draft: Oleksandr Milov.
Writing – review & editing: Stanislav Milevskyi, Hryhorii Kots.

REFERENCES

1. Evseev, S. (2016). Methodology for information technologies security evaluation for automated banking systems of Ukraine. *Ukrainian Scientific Journal of Information Security, 22*(3), 297-309. (In Ukrainian). http://dx.doi.org/10.18372/2225-5036.22.11103
2. Evseev, S. et al. (2019). Development of a methodology for building an information security system in the corporate research and education system in the context of university autonomy. *Eastern-European Journal of Enterprise Technologies, 3*(9), 49-63. (In Ukrainian). https://doi.org/10.15587/1729-4061.2019.169527
3. Evseev, S., & Dorohov, A. (2011). Information threats and safety in Ukrainian bank payment systems. *Russian journal of criminology, 16*(2), 68-75. (In Russian). Retrieved from http://cj.bgu.ru/reader/article.aspx?id=8111
4. Evseev, S., Kots, G., & Korol, O. (2015). Analysis of the legal framework for the information security management system of the NSMEP. *Vostochno-evropeyskiy zhurnal peredovyih tehnologiy, 5(3)*(77), 48-59. (In Ukrainian). https://doi.org/10.15587/1729-4061.2015.51468
5. Evseev, S., Rzayev, K., Mammadova, T., Samedov, F., & Romashchenko, N. (2018). Classification of cyber cruise of informational resources of automated banking systems. *Cybersecurity: Education, Science, Technique, 2*(2), 47-67. (In Ukrainian). https://doi.org/10.28925/2663-4023.2018.2.4767
6. Gorbatov, V. (1976). *Teoriya chastichno-uporyadochennyih system [Theory of Partially Ordered Systems]* (336 p.). Moskva: Sovetskoe radio. (In Russian)
7. Gorbatov, V. (2000). *Fundamentalnyye osnovy diskretnoy matematiki. Informatsionnaya matematika [Fundamentals of discrete mathematics. Informational mathematics]* (556 p.) Moskva: Nauka. (In Russian)
8. Hamdan, B. (2013). Evaluating the Performance of Information Security: A Balanced Scorecard Approach. *SAIS 2013 Proceedings*. Retrieved from https://pdfs.semanticscholar.org/c34a/895202bceb5377c1a0510452b554ed319225.pdf
9. Isaev, R. (2015). *Sekrety uspeshnykh bankov: biznes-protsessy i tekhnologii [Secrets of successful banks: business processes and technologies]* (222 p.) Moskva: INFRA-M. (In Russian)
10. Kotenko, I., & Karsaev, O. (2001). Ispolzovanie mnogoagentnyih tehnologiy dlya kompleksnoy zaschityi informatsionnyih resursov v kompyuternyih setyah [The use of multi-agent technologies for the comprehensive protection of information resources in computer networks]. *Izvestiya Yuzhnogo federalnogo universiteta. Tekhnicheskiye nauki - News of the Southern Federal University. Technical science, 4*(22), 38-50. (In Russian). Retrieved from http://old.izv-tn.tti.sfedu.ru/wp-content/uploads/PDF/2001_4(22).pdf

11. Magomaeva, L. (2017). Information resources as a strategic active in modern business systems. *Aktualnyye voprosy ekonomicheskikh nauk i sovremennogo menedzhmenta - Actual issues of economic sciences and modern management, 4,* 43-48. (In Russian). Retrieved from https://sibac.info/conf/economy/iv/85817
12. Milov, A., & Korol, O. (2019) Razrabotka ontologii povedeniya vzimodeystvuyuschih agentov v sistemah bezopasnosti [Development of an ontology of the behavior of interacting agents in security systems] (pp. 832-842). *4th International Congress on 3D Printing (Additive Manufacturing) Technologies and Digital Industry* (11-14 April, 2019). (In Russian)
13. Rigin, V. (2012). Informatization in the aspect of a process-oriented approach to the enterprise management. *Problems of Territory's Development, 2*(58), 86-91. (In Russian). Retrieved from http://pdt.vscc.ac.ru/article/940?_lang=en
14. Stelmashonok, E. (2006). Organizatsiya informatsionnoy zashchity biznes-protsessov [Organization of information protection of business processes]. *Applied informatics, 2*(2), 42-57. (In Russian). Retrieved from http://www.appliedinformatics.ru/r/articles/article/index.php?article_id_4=877
15. Weishaupl, E., Yasasin, E., & Schiyen, G. (2015). IT Security Investments Through the Lens of the Resource-Based View: A new Theoretical Model and Literature Review. *European Conference on Information Systems*. https://doi.org/10.18151/7217521
16. Yudin, O., & Buchyk, S. (2015). Classification of Threats to State Informative Resources of Normatively-Legal Aspiration. Methodology of Construction of Classifier. *Ukrainian Information Security Research Journal, 17*(2), 108-116. (In Ukrainian). http://dx.doi.org/10.18372/2410-7840.17.8759
17. Yudin, O., & Buchyk, S. (2015). *Derzhavni informatsiini resursy. Metodolohiia pobudovy klasyfikatora zahroz [State information resources. Methodology for building the threat classifier]* (212 p.). Kyiv: NAU. (In Ukrainian). Retrieved from https://er.nau.edu.ua/bitstream/NAU/31911/1/Monogr_klas_zagroz_Yudin_Buchyk.pdf
18. Yudin, O., Buchyk, S., Chunarova, A., & Varchenko, O. (2014). Methodology of construction of classifier of threats to state informative resources. *Science-Based Technologies, 2*(22), 200-210. (In Ukrainian). http://dx.doi.org/10.18372/2310-5461.22.6820

http://dx.doi.org/10.21511/ed.19(1).2020.02