

Estimation of Structural-Topological Characteristics in Information Security System

Liubov Chagovets, Svitlana Prokopovych,

Economic Cybernetics Department
Simon Kuznets Kharkiv National
University of Economics
Kharkiv, Ukraine
liubov.chahovets@hneu.net,
prokopovichsv@gmail.com

Vita Chahovets,

Economic and Management Department
Kharkiv State University of Trade and Foods
Kharkiv, Ukraine,
chagovec.v@ukr.net

Abstract—The paper describes the main components that characterize the state of economic security, including information security company. Indicators of enterprise information security and its threats are analyzed. The analysis of methods and models for assessing company information security was made. The evaluation model of enterprise information security by mathematical tools was provided. It increases the quality of management solutions for the enterprise. The decomposition management model of enterprise information security system was developed by way structural modeling. The results can be used to evaluate the information components of enterprise economic security.

Keywords—*economic security; methods; models; information security.*

I. INTRODUCTION

Today, information technologies are the most important in ensuring the efficiency of enterprises. It should be noted, that information security issues have intensified on account of the massive use of new information and communications technologies due to the global tendency of the amount of information attacks increasing and significant financial and material losses. The company management should implement modern security system to provide the information security and leak prevention. The system has to combine different information protecting methods in a single set against attacks to protect the entire information environment - local networks, Internet exits, databases set. The company management should care about creating an integrated, modern system of protection of the confidential information component to ensure the preservation of information and the impossibility of its leakage beyond the company boundaries. The system must combine different information protecting methods against attacks into a single set, must protect the entire information environment: local networks, access points to Internet, databases, working files etc.

The development and implementation of security system will eliminate illegal activity aimed at capturing sensitive information. It will lead to a sharp deterioration of enterprise's economic situation, reputation and position in the competitive environment. Taking into account that in today's world a large share of attacks falls on the information component, in the development of the overall security system of the enterprise the biggest attention is paid precisely to the creation of a system of protection of information security. It is aimed at protecting against

leakage, disclosure, loss of information, as well as at preventing unauthorized access to it by third parties.

The objective of the paper is the development of a set of models of assessment of the company security information component, which will improve the quality of decision making concerning economic security.

II. LITERATURE REVIEW

It is advisable to develop complex of models with the analysis of conceptual foundations of information security management in enterprise system. The problem of information security modeling and separate components of economic security of control systems were carried out by a number of scientists whose research results are presented in [1]–[7], [9]–[12].

In articles [5]–[10] is showed that the information security management system is the core of the overall management system. It provides the basis for risk analysis identified for the design, implementation, monitoring, maintenance and improvement of information security activities. The system consists of many components: organizational structures; policy; planning action; duties; procedures; processes and resources as demonstrated in [10]–[12]. In papers the number of practical solutions is suggested. The practical issues are carried out to achieve the goal of company information security: to classify the information resources at the enterprise; to develop the algorithm of the information system requirements; to allocate the responsibilities for each process; to develop the system of information security risks evaluation; to select the employees who will have access to information resources with a high risk of information leakage; the risk management system for information security is developed (methods, measures and their assessment); set of technical, administrative, management measures to reduce the threat of information leakage; Constant control over the state of information leakage risks is conducted; the physical security of the company personnel is carried out.

The information security depends on a set of factors (external and internal), and on their dynamic impact and ensuring the safety of resources as demonstrated in [5]–[12]. Figure 1 presents all vectors of influence between the following factors: threats to the information security that may arise and may be implemented as a result of the confidential information leakage; the vulnerability levels of

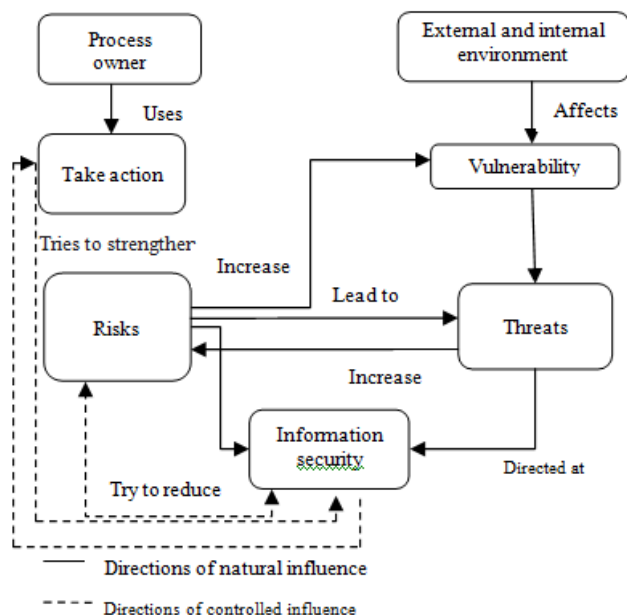


Fig. 1. Scheme of the enterprise's information security factors relation

the information security system that will affect the possibility of a threat; risks that foresee the losses for the enterprise as a result of confidential information disclosure.

The objects of protection include language information, various types of documents (both electronic and paper), technical communication facilities, and rooms intended for confidential meetings, software tools and other valuable information objects of the enterprise. In order to stop the aggressor's attack on the company's secret information, the management organizes an algorithm for the risk management process, which is the basis of the company information security system.

Creating an effective model of information security system uses an integrated approach that aims at reduction of internal and external threats, taking into account probable time and resource limits.

One of the methods of assessing information security is based on risk management [8], [10]. It is necessary to determine the resources of the information system, that in the process of evaluating the information system agreeing with the authors [8]. It is necessary to divide these resources and external elements with which the interaction is carried out. Resources can be computer facilities, software, and data. Objective factors of the model are: threats to information security of enterprises, characterized by the probability of implementation; vulnerabilities in the information system or system of countermeasures (information security systems); risk - a factor reflecting the potential damage to the organization as a result of the threat of information security: leakage of information and its misuse (the risk reflects probable financial losses - direct or indirect) according to [8].

If we consider the system of the enterprise information security in terms of the process approach, then it can be presented as a risk management process (Fig. 2), which covers the following components:

1) *Description of business processes.*

2) *Review and risk analysis.* As a result, the set of potential acute threats and recommendations for their prevention were considered [8]–[12].

3) *The process of risk assessment consists of the following steps:* description of the object and protection measures; resource identification and determination of its quantitative indicators; analysis of threats to information security; vulnerability assessment; assessment of existing and foreseeable means of information security.

4) *Measures planning.* The purpose of planning measures to minimize risks is to determine the timing and list of measures to exclude or minimize the loss in case of risk minimization.

5) *Implementation of measures to minimize risks.* The results of this process are risks minimization measures and time of their implementation.

6) *Assessment of the information security management system effectiveness* is a system process for obtaining and evaluating objective data on the current state of the system, actions and events occurring in it.

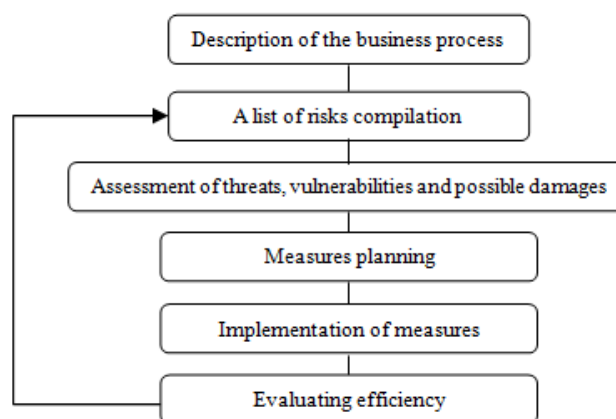


Fig. 2. Model of risk management process for the information security system

This approach is quite widespread in management practice, but it has a significant drawback: the evaluation of the risk of occurrence of events is difficult due to the problematic collection of source data that contain all possible variants of events.

III. PROBLEM FORMULATION

The analysis of the literature sources concerning the information security models of the enterprise has shown that insufficient attention is paid to the evaluation and justification of the decisions taken on enterprise information security (ISE) from the point of view of mathematical modeling. The conceptual scheme of research, which includes the following main stages (Fig. 3), has been developed, taking into account exactly modern mathematical methods and models of information security of the enterprise.

At the first stage of the research there is the formation of a research information space with the definition of the main indicators of the work efficiency and the state of economic security of the enterprise and its information component.

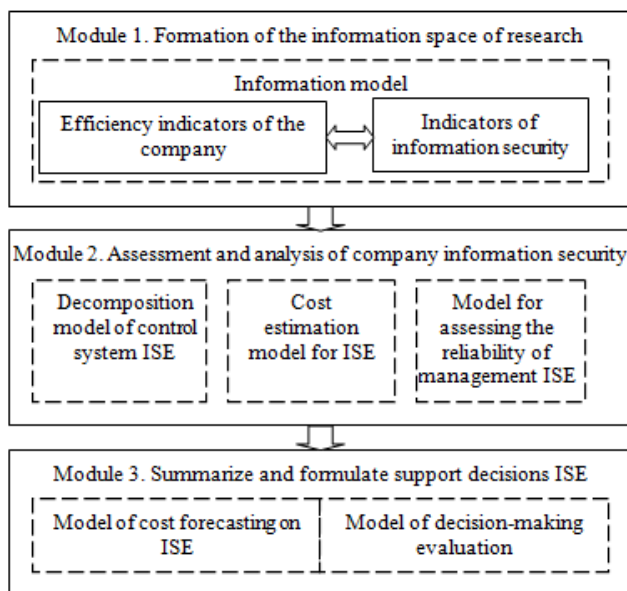


Fig. 3. Conceptual scheme of information security assessment of the enterprise

The second step of the research involves the assessment and analysis of information security. The models of decomposition and estimation of information security costs are developed. By means of these models a general assessment of the information component of the company's economic security and the assessment of the reliability of the information security management system are carried out at this stage.

The third step of the research is to summarize and formulate solutions to support enterprise information security—a generalized model, consisting of a model for forecasting the costs for enterprise information security and of a model for evaluating decisions, is under developing.

IV. METHODS, FINDINGS

At present, many models have been developed that are applied in the field of information security. They can be classified according to different features and criteria. For example, according to the implementation we should distinguish between mathematical models, according to the parameters of the model description—deterministic, stochastic, fuzzy, etc. In order to create a model, they are divided into forecasts designed and purpose optimized.

However, it should be emphasized that at present there is no universal model of information security. It solves only a part of the problems identified as priorities, not taking into account the uniqueness of each system, which is in a constant change, under the influence of many factors, which are often difficult not only to describe, but also to identify in advance. Therefore, the paper suggests a new perspective on the development of a security system using the program BPwin (Fig. 4).

The first step is to create a context diagram, which is a general description of the system and its interaction with the external environment. Contextual diagram "Developing Information Security System" is characterized by input properties of information, legal and administrative

measures for the development of information security system, a security service unit involved in the development of a security system, as well as obtaining recommendations on the protection of information, information security, protection systems information and data arrays to provide security. Initially, a process is created in the form of main activity and four areas, of which the following are distinguished: management (normative and legislative basis); internal management of processes (subjects of responsibility); incoming informative database; output effective information.

This kind of diagram has an initial character. The main work is the basis and has a "black box" underneath, in the middle of which there is a clear and consistent hierarchy of activity. In our case, the main process has five levels: the formation of information security functions; company awareness of potential threats to information security; resource provision of information security; methods and measures of the information protection. It can be noted that at this stage internal management who are managers and administrators responsible at all stages for building an information security system and levels of decomposition process. These categories of workers are responsible for developing, analyzing, calculating and implementing those measures that can improve the protection of the company's sensitive data. The basis of the legislative framework is the laws of Ukraine "On Information", "On the Protection of Information Data" and various external and internal orders of the company management.

The first decomposition diagram is divided into four consecutive stages, each of them is of great importance. The second is a threats analysis. The stage is very important from the standpoint of analytics, because some threats can significantly degrade the status, and the reputation of the organization. The third stage has the main purpose of planning actions for information security and emergency actions. Therefore, special attention should be paid to the development of measures that will be used in emergencies.

The last stage of work is the choice of technical equipment for information security. At the stage, taking into account all the conclusions and recommendations of the previous stages of the work "Formation of the information protection functions", the selection, testing, analysis and adoption of technical basis for protection against unauthorized data of an external attack is carried out.

As a result of such inspections, it is possible to obtain indicators of the equipment effectiveness, and the vulnerability of information data as a result of the aggressor attack. Expert evaluations of the conducted tests can provide clear recommendations for choosing or replacing the technical protection base.

Let's return to the first stage of the decomposition. It also includes several measures. They can be performed both sequentially and in parallel with each other. The latter type is more practical because it takes much less time for such activities if the work is carried out in parallel. This type of work includes five action lines, which will help in the end to get a clear plan to protect the information array at the enterprise. Such actions include:

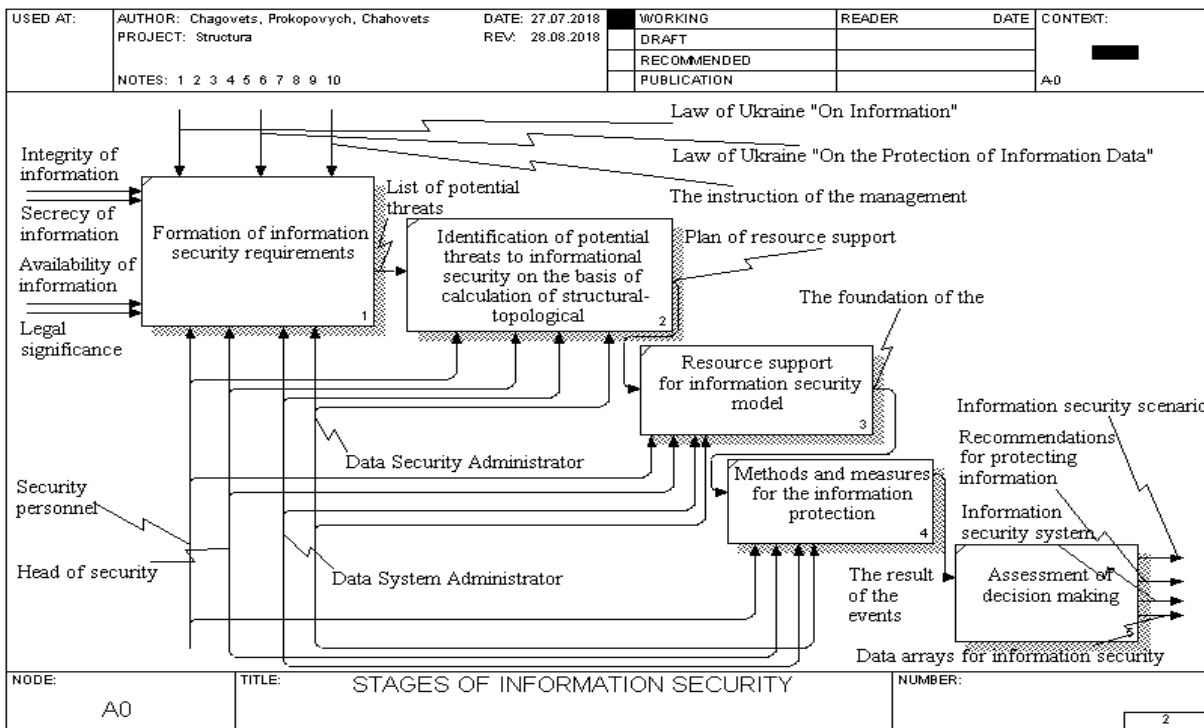


Fig. 4. Scheme of decomposition of the stages of information security providing

1) *Availability of information.* The main purpose is to determine the information from the whole array of data, which is a potential threat to the enterprise as a result of leakage to the aggressor.

2) *Development.* This direction is characterized by the fact that a detailed planning of data protection measures is carried out. It is the organizational component that is the leverage that should be "tightened" from all edges. The more attention is paid to this area, the better the implementation of such protective measures will be.

3) *Calculation.* In the course of work, the collection of data array, its processing, analysis and calculation of those indicators is done. It will reflect the real magnitude of the threat as a result of its implementation. The indicators of the potential loss of each type of information and indicators of the state of the enterprise as a result of such a drain are calculated.

4) *Priority.* The basis of this type of work is to define the information that is a secret for any person who does not control the process of managing the company. Such information is given the highest priority of secrecy. Then the information is collected in one array; the leakage of such information will lead to difficult financial and moral state of the company. And then the information is classified by the level of secrecy. This structuring is very important because the flow of information in the enterprise is very large, and therefore such a classification will help to increase the level of the data security.

5) *Structural work.* The actions in this direction will be aimed at the distribution of information for official duties of each structural unit at the enterprise. Delegation of authority is very important for high productivity in the company. So, you can identify those units that will perform their daily work. Upon termination of work at all stages,

we obtain the final plan for the information protection at the enterprise.

The second stage in developing a security system at the enterprise is the awareness of the organization about potential threats to information security. Awareness of the organization about potential threats to information security includes four stages: a model for assessing losses from potential threats; classification of threats; sources of threats.

The results of the first three measures form the foundation for developing a model of resource security. The first three works may interact closely with each other, because one indicator (the threat) is the basis for classifying, analyzing and reviewing sources.

Let's examine in details how the model of estimation of losses from potential threats is visualized. This stage has the following areas of development: financial harm from the disclosure of secret information; moral and material damage; financial costs to restore the violated information resources. Such a thorough analysis will reflect the losses in groups and there is an opportunity for so-called clusterization of losses from which it is possible to allocate clusters with a high degree of losses, medium and low. Sources of threats can be external and internal. The first type includes: potential criminals and hackers; unscrupulous partners; technical staff of service providers; communication facilities; low-quality software tools for information processing; low-quality technical means of collecting and processing information. Internal sources of threats include: the main personnel of the organization; representatives of the information security service; technical staff. At the end of damage evaluation, a model of resource provision for information security of the enterprise is developed.

The third stage of the main process decomposition is the resource support. The fourth stage is the development of methods and measures to protect the information. At this stage, taking into account all the analytics of the previous stages of work, our methods and measures of information protection are implemented in our model. They absorb two types – subjective and objective. The first type of information protection measures includes: legal measures; moral and ethical methods; administrative measures; physical methods. The second type of activities includes: technical facilities; software; hardware - software. This stage of work, like all previous levels and stages of decomposition, is regulated by the enterprise security department, data system administrator, data security administrator, and other personnel whose work is closely related to security. The last stage of building an information security system involves the creation of recommendations for managerial decisions on improving the effectiveness of the information component in the economic security of the enterprise.

As an example, let's look at the results of the evaluation of the structural characteristics, a company engaged in design, plan development, and construction. The organizational structure is depicted on Figure 5.

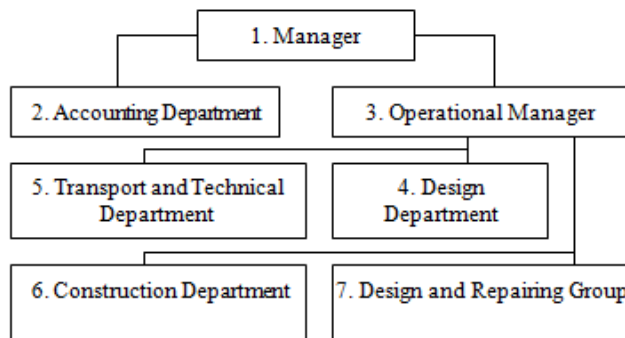


Fig. 5. Organizational structure of company

The adjacency matrix for the analyzed structure is shown on Figure 6.

	1	2	3	4	5	6	7
1	0	1	1	0	0	0	0
2	1	0	0	0	0	0	0
3	1	0	0	1	1	1	0
4	0	0	1	0	0	0	0
5	0	0	1	0	0	0	0
6	0	0	1	0	0	0	0
7	0	0	1	0	0	0	1
	2	1	5	1	1	1	1

Fig. 6. Matrix adjacency

The columns and rows matrix describe structural elements: 1—manager, 2—accountant, 3—deputy director, 4—design department, 5—transport and technical department, 6—construction department, 7—design and repairing group. Let's check this structure for connectivity. The connection of structure is estimated by the formula [11]:

$$C = \frac{1}{2} \sum_{i=1}^n \sum_{j=1}^n a_{ij} \geq n-1 \quad (1)$$

where n is number of structure's vertices, a_{ij} is the connection between the two elements.

It should be noted that the graph is not oriented, $C = 6$. From the above results the structure is connected, all the elements are interconnected. The index of structural redundancy is estimated by the formula:

$$R = \frac{1}{2} \left(\sum_{i=1}^n \sum_{j=1}^n a_{ij} \right) \frac{1}{n-1} - 1 \quad (2)$$

Substituting our data, the result for our structure is $R = 0$. This suggests that there is a minimum number of links in this system.

Then the index of uneven distribution of bonds is calculated by the formula:

$$\varepsilon^2 = \sum_{i=1}^n \rho_i^2 - \frac{4m^2}{n} \quad (3)$$

where ρ_i is the number of edges coming from the i -th vertex, m is the number of edges.

For the structure $\varepsilon^2 = 14$. Since this value is not too large, it can be concluded that the relationship is distributed almost evenly, that is, the possibilities of the structure are used practically as much as possible.

The matrix of distances will be as follows (Fig. 7).

	1	2	3	4	5	6	7
1	0	1	1	2	2	2	2
2	1	0	2	3	3	3	3
3	1	2	0	1	1	1	1
4	2	3	1	0	2	2	2
5	2	3	1	2	0	2	2
6	2	3	1	2	2	0	2
7	2	3	1	2	2	2	0

Fig. 7. Matrix of distances

Absolute compactness is calculated by the formula:

$$Q = \sum_{i=1}^n \sum_{j=1}^n d_{ij} \quad (4)$$

where d_{ij} — the minimum length of the path between the i -th and j -th vertices.

The absolute compactness of the structure is $Q = 80$. Let's calculate the relative compactness by the formula: $Q_{rel} = Q/Q_{min} - 1$, where Q_{min} are calculated by the formula: $Q_{min} = n(n-1)$. The relative compactness for our structure is 0.9. Structural compactness can also be characterized by another characteristic - the diameter of the structure. The diameter of the structure shows the maximum distance from one element of the structure to another and is the maximum of all d_{ij} . For the analyzed structure, the diameter is 3. Next, we need to calculate the degree of centralization of the structure:

$$\delta = (n-1)(2z_{max} - n) \frac{1}{z_{max}(n-2)} \quad (5)$$

where $z_{max} = \max\{z_i\}$. z_i is calculated by the formula:

$$z_i = \frac{Q}{2} \cdot \sum_{i=1}^n d_{ij} \quad (6)$$

The degree of centralization is 0.93. The calculations results of absolute and relative compactness make it possible to assert that this structure is not compact and can be improved. The degree of centralization is 0.93, which indicates the presence of the main element in the control system, on which the key security decisions depend and which is responsible for the work of practically all other elements—the security system departments. Thus, we can conclude that for this enterprise it is expedient to develop methods for delegation of managerial authority from senior management to operational level managers to improve the reliability of the enterprise security management system.

V. DISCUSSION AND CONCLUSION

Thus, the development of the proposed system corresponds to all norms and reflects the stages of its construction as in real conditions, the subjects and objects that interact at each stage and in each work. Such a model can become the basis of information security for enterprises. But it's worth noting that each organization should develop an individual security system, and take these examples into account. With the help of resources, qualifications, and modern software, the company creates a barrier for aggressors who intend to steal sensitive information.

Thus, the paper considers the decomposition of business processes for managing information security. In the work the indicators of information inertia as the most important in developing the general model of information security management are assessed. The scientific novelty of the research is that the complex of assessment models of the information security components of an enterprise has been improved on the basis of the structural topological analysis of organizational systems. Unlike existing models, the proposed set of models takes into account the indicators of information inertia. The decomposition of information security management processes in terms of refining business processes for managing information security has been further developed using structural analysis and design tools as CA AllFusion ERwin Data Modeler. This makes it possible to improve the quality of information security solutions.

The performed analysis is the basis for further research of various models and topologies of information security systems. It provides an opportunity to assess the effectiveness of the information security system, serves as the basis for modeling the static and dynamic characteristics of the system. These estimates are important safety features and reflect the level of reliability, stability and sensitivity of the system to the change in parameters. Quantitative evaluation of the linkage of elements in the system makes it possible to adjust the management structure in a short time and to improve the management of information security.

VI. FUTURE WORK

The obtained results form the basis for further scientific research, the main directions of which are: development of the most effective information security management structures of the enterprise; a study of potential security threats, vulnerabilities of the system and attacks based on the synthesis of dynamic quantitative and qualitative characteristics, which will enable to develop effective strategies for their prevention.

REFERENCES

- [1] L. Guryanova et al. "Modeling of the enterprise functioning stability using the automatic control theory apparatus." *Eastern-European Journal of Enterprise Technologies*, Vol. 4, issue 3(88), pp. 45-55, 2017. DOI: <https://doi.org/10.15587/1729-4061.2017.108936>.
- [2] L. O. Chagovets and N. O. Usov. "Sy`stema bezpeky` informaciyi yak skladova ekonomichnoyi bezpeky` pidpry`emstva [Information security system as a component of the enterprise economic security]," in *Materialy` Vseukrayins`koyi naukovoprakty`chnoyi konferenciyi molody`x ucheny`x ta studentiv «Rozvy`tok yevropejs`kogo prostoru ochy`ma molodi: ekonomichni, social`ni ta pravovi aspekty`» [Proceeding of Ukrainian Scientific and Practical conference of Young Scientists and Students "European space development by eyes of youth: economic, social and legal aspects"]*, 2016, pp.1598-1601. (In Ukrainian).
- [3] T. S. Klebanova, L. O. Chagovets and O. V. Panasenko. *Nechitka logika ta nejronni merezhi v upravlinni pidpry`emstvom [Fuzzy logic and neural networks in enterprise management]*. Kharkiv, Ukraine: PH "INGEC", 2011. (In Ukrainian).
- [4] I. Buzko et al. "Artificial Intelligence Technologies in Human Resource Development," in *Proc. 14th Int. Scientific Conf. "Information Technologies and Management"*, 2016, pp. 26-29.
- [5] S. H. von Solms and W. J. Caelli. "A Model for Information Security Management," *Information Management & Computer Security*, Vol. 1 Issue: 3, pp.12-17, 1993.
- [6] D. L. Nazareth and J. Choi. "A system dynamics model for information security management," *Information & Management*, Vol. 52, issue 1, pp 123-134, 2015.
- [7] R. Von Roessing. "The ISACA Business Model for Information Security: An Integrative and Innovative Approach." in *Proc. Information Security Solutions Europe 2009 Conf.*, 2009, pp. 37-47.
- [8] S. V. Kavun, V. V. Nosov and O. V. Mazhaj. *Informacijna bezpeka [Information Security]*. Kharkiv, Ukraine: PH KHNUE, 2008. (In Ukrainian).
- [9] Mohd Asri Mohamad Stambul and R. Razali, "An assessment model of information security implementation levels," *Proc. of the 2011 International Conf. on Electrical Engineering and Informatics*, Bandung, 2011, pp. 1-6.
- [10] A. A. Ly`tvynyuk. "Osnovy` informacijnoyi bezpeky`. Kompleksna sy`stema zaxy`stu informaciyi: struktura, vstanovlennya ta pidtry`mka funkcionuvannya [Basic of information security. Integrated information security system: structure, installation and maintenance of the operation]." *Visnyk 19 Central`noyi vy`borchoyi komisiyi*. 2008. http://www.cvk.gov.ua/visnyk/pdf/2008_4/visnik_st_08.pdf (In Ukrainian).
- [11] "Strukturnyj analiz organizacionnoj struktury [Structural analysis of organizational structure]." *LearnManage*. <http://www.learnmanage.ru/lmans-708-1.html>. (In Russian).
- [12] A. P. Moore, R. J. Ellison and R. C. Linger (2001) *Attack Modeling for Information Security and Survivability* [Online]. Available: https://resources.sei.cmu.edu/asset_files/TechnicalNote/2001_004_001_13793.pdf