Advances in Social Science, Education and Humanities Research, volume 318

3rd International Conference on Social, Economic, and Academic Leadership (ICSEAL 2019)

Information system protection as a factor in maintaining the leading positions in the enterprise development

Olga Kozhusko
Simon Kuznets Kharkiv National University of Economics
Nauky avenue 9-A, 61166 Kharkiv
Ukraine
e-mail: Olga_Kozhusko_z@ukr.net

Svetlana Khaminich
SESE "Oles Honchar Dnipro National University"
72 Gagarin ave., 49000 Dnipro
Ukraine
e-mail: svetala1704@i.ua

Svitlana Alieksieieva
"Institute of vocational education and training of NAES of Ukraine"
Lane Vito Lithuania, 98th, 03045 Kyiv
Ukraine
e-mail: SV-05@ukr.net

Abstract Nowadays, the social and economic development of any country largely depends on the effective creative activity of its citizens. World trends in development, science, technology and production indicate that in the information society, further progress will be recognized solely by intellectual activity. Information support today needs all spheres of social activity, and the information activity itself requires clear regulation.
A special place among the problems regulating of information activity is the issue of the enterprise information security. This paper determines that the basic information object of a modern society is an enterprise, the nature of which is determined by the information and information infrastructure. The basic properties of the information are determined and on the basis of them the conceptual provisions of the information system protection of the enterprise are formed. Built a functional model of information system protection

1 Introduction

The main focus of the modern world scientific progress is the further informatization of separate sectors of the economy and society. Therefore, the current state of human development, many scientists characterize as the formation period of information society.

The rapid growth in the volume of information is due to the complication of, firstly, technologies and production processes, and secondly, social relations in all spheres of public and political life. Wide and operative access to information greatly increases the efficiency of its use. The introduction of the latest information technologies, global computer networks and mobile communications greatly accelerates the processes of obtaining, processing and analyzing information, and becomes an integral part of the management of all socio-political institutions and scientific and technological processes. This is especially important for Ukraine, which ratified the agreement with the European Union, received a guideline for its transformations - the parameters that the member of the European community must meet. The globalization tendencies that characterize the modern civilization era, first of all, are manifested in the information sphere. This Agreement automatically included Ukraine in the process of general informatization of society and the formation of a single global information market.

2 Conceptual provisions for the protection of the enterprise information system

The basic information object of a modern society is an enterprise whose nature of functioning is determined by the following informational properties: an information product that is the result of the activity of an individual and society, the composition and nature of information services, and the information infrastructure in which these elements function. Therefore, the concept of information security of any enterprise must meet the requirements of all these elements of the system. A fundamentally important element of enterprise information security is the protection profile. It is a community of typical security requirements for a certain class of objects for which it is

necessary to determine a certain level of information security. The entity (business structure) independently determines the level of its information protection. This reduces to the fact that the enterprise itself formulates, regulates and implements the following tasks for ensuring information security:

- Identification of the most likely threats and factors that affect the level of the business entity information security;
- Identify the most vulnerable places in the information system of the subject;
- Assessment of the risks associated with the probability of detecting and implementing threats;
- Development of measures to prevent and reduce the effects of a loss in the subject information infrastructure.

The information infrastructure of the enterprise includes the means of providing and realization of information products and services, as well as means of ensuring their effective functioning in the process of production and communication (transmission) of data. To classify threats to information security, distinguish three components: organizational and managerial; production-process and providing (Alamoudi and Kumar 2017; Dhillon and Backhouse 2000).

The vast majority of modern specialists believe that reducing the impact of destabilization factors-threats to enterprise security can be achieved through deliberate preventive information influence on possible subjects threats (first of all, competitors-companies). That is, forward-thinking information is the basis of security, including information.

At the same time, the level of information security is interpreted as the level of regulatory security of such objects as software tools, the means to provide access to data, the rights of users to perform work related to the modification and use of confidential information, the detection and counteraction of information leakage in relation to the emerging threats, carriers of which are the carriers of certain subjects. The use of a systematic approach to organizing the processes of providing information security of the enterprise based on the provisions of the theory of information, clarifying the concept of information resource and defining the information system as a supporting system for information resources - the most important task of increasing the effectiveness of the enterprise information security (Dhillon and Backhouse 2000).

From this point of view, according to many scientists (e.g. Albert and Dorofee 2002); Ponomarenko et al. 2008; or Anderson and Moore 2009), information is a set of data, each subset of which is characterized by such properties: objectivity, reliability, adequacy, timeliness, correctness, accuracy, utility, value. At the same time, it should be noted that in a variety of literary sources, only a certain part of them is allocated from a given set of properties, guided, first of all, exclusively by practical considerations. At the same time, it should be noted that in a variety of literary sources, only a certain part of them is allocated from a given set of properties, guided, first of all, exclusively by practical considerations. For example, the properties of adequacy and probability are combined into one - probabilities; objectivity and correctness - in the property of objectivity, etc. Analysis of other properties - the timeliness, accuracy, usefulness and value, to determine what information should be useful and valuable, and this in turn requires that it be accurate and timely.

Thus, the property of information, to a certain extent, characterizes a specific management function of an enterprise implemented by the entity that uses this information (Figure 1).

Thus, the information system acts as an instrumental tool (a set of tools) that ensures the safe development of the properties of information resources at all levels of enterprise management, and its subsystems act as a "dumping" means from the influence of threats (hazards) and provide protection of the main object - information enterprise and its properties at different levels of management.

3 Model of enterprise information system protection

The content of the information system security policy is determined by the information processing technology, models of violator and threats, peculiarities of the computing system, physical environment and other factors. As a result, if different systems of information processing are implemented in any system, then the security policy in such a system will consist of several substantially different parts, each of which will correspond to a specific information processing technology. As part of an information system overall security policy, tools for ensuring the confidentiality, integrity, observance and availability of the information being processed, as well as the rules of access differentiation governing the rules of user access and processes to system resources.

The security policy should provide for the complex use of legal and moral-ethical standards, organizational (administrative) measures, physical, technical (hardware and software) methods and means of information protection, as well as determine the rules and procedures for their application in the information system (Kurkin 2016). Security policy should be based on the principles of systematization, complexity of protection continuity, adequacy of mechanisms and measures of protection and their adequacy to threats, flexibility of protection system

management, simplicity and convenience of its use, openness of algorithms and mechanisms of protection, unless otherwise provided separately (Oleunic et al. 2011). See Figure 1 that follows.

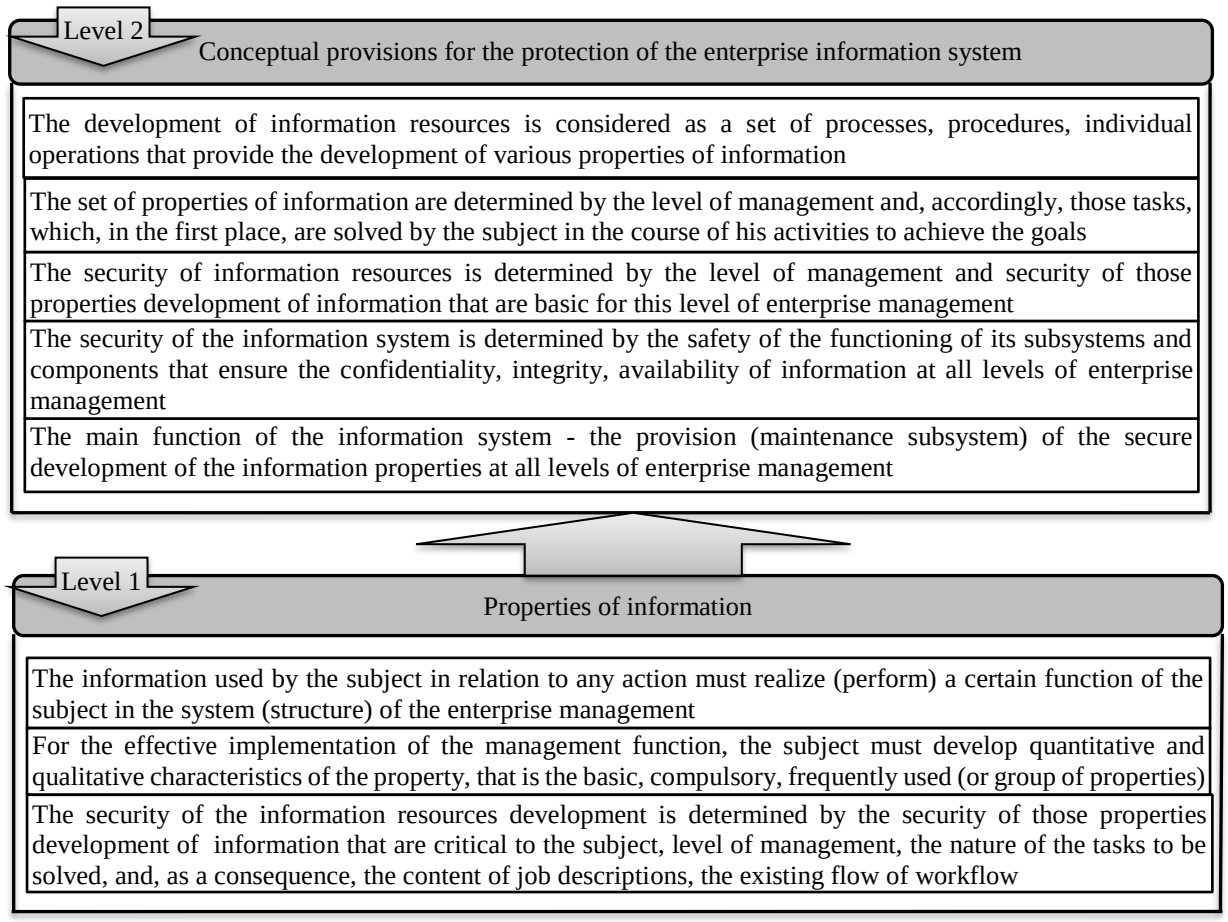

Fig. 1. The interconnection of the information properties and the conceptual provisions of the protection of the enterprise information system
Source: Own results

The implementation of these provisions in the company's information security system is possible through the adoption of a functional model for the protection of the enterprise information system (Figure 2).

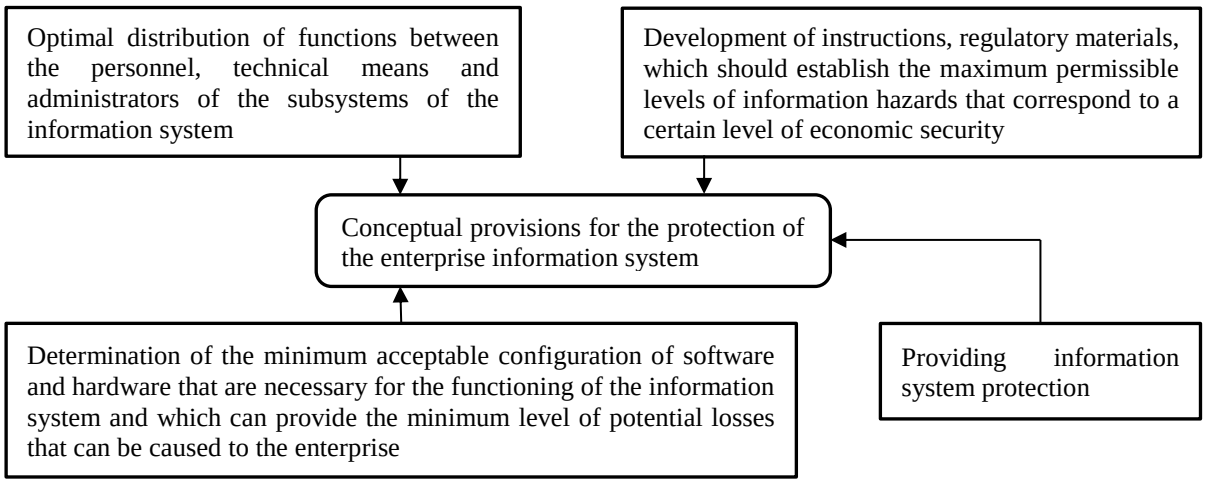

Fig. 2. Functional model for the protection of the enterprise information system
Source: Own results

The proposed model of information security allows us to detail it to different levels of enterprise management, to make changes in job descriptions of persons who are related to confidential information and to design possible levels of protection for various types of threats occurring in the external and internal environment of the enterprise.

Particular protection in the current conditions of the operation of the enterprise information system requires information that constitutes its commercial secret. The composition and amount of information constituting commercial secrets and methods of their protection are independently determined by the enterprise. Therefore, the right to protection of commercial secrets must be enshrined in the company's charter (Kozhushko 2014; or Kavun et al. 2013). This enables, on a legal basis, to build relationships with partners, their own employees, and to organize a regime of protection of commercial secrets at the enterprise. Ehe rights of enterprises to protect commercial secrets should be formalized in relations with the labor collective. Consequently, such a right should be enshrined in the articles of a collective agreement, which is concluded between the owner of the enterprise or the authorized body, on the one hand, and one or more trade unions or other authorized representatives for labor collective bodies on the other. It is desirable that these articles reflect the following provisions:

- The enterprise uses commercial secret in its activities;
- The staff of the enterprise undertakes to keep the trade secret;
- Each employee is personally disciplined and liable for the maintenance of commercial secrets to which he has access;
- The administration is obliged to create proper conditions at workplaces and to familiarize employees with the rules of preservation of commercial secret of the enterprise.

Since an individual labor contract is usually drawn up only by order, the personal obligations of the employee to protect the commercial secret of the enterprise are formalized by a separate document, for example, a written undertaking not to divulge the commercial secret of the enterprise (Korchevska et al. 2013). At the same time, in such a document it is desirable to foresee the duties of the employee on the non-disclosure of commercial secrets and after termination of employment relations. Particular attention should be paid to the formalization of legal relations to preserve commercial secrecy with creative workers: designers, inventors, and scientists. These relations should be based on laws on information, on copyright and related rights, on the protection of industrial property rights.

Equally important for the creation of a commercial secret storage regime is the formation of the enterprise information system, and, in particular, the order of circulation of information with commercial secrets, as well as storage, reproduction and destruction of documents - carriers of commercial information.

The next step in consolidating the company's rights to protect trade secrets should be the proper relationship with their counterparties. For this purpose, contracts of purchase and delivery of goods, components and raw materials, if they are subject to commercial secrecy, should provide for the preservation of confidential information regarding the terms of these contracts.

The ultimate goal is to increase the development of methods for increasing the stability of the information system by minimizing the risks associated with the task of damaging both the enterprise's activities and its information infrastructure and increasing the stability of all information processes, including methods and means for obtaining, input, processing and analysis of information.

4 Conclusions

In conclusion, it should be noted that the protection of the enterprise information system has always been one of the most important aspects in any company. And let the provision of information security can be perceived as a technical task in its essence, but in reality, it is the basis for doing business, as the competitive positions and financial health of any company can be threatened.

At the same time, along with the development of information technology, the scale of threats to corporate infrastructure is increasing. In its turn, it requires the operating provisions for the enterprise information system protection, as well as a clear model of its functioning. However, it should be taken into account that, in any given situation, organizational measures take on the content and form specific to each organization, and such measures will be aimed at ensuring information security in specific conditions.

References

Alamoudi D, Kumar A (2017) Information System Complexity and Business Value. International Journal of Economics and Management Sciences 6:400. doi: 10.4172/2162-6359.1000400

Alberts CJ, Dorofee A, Managing information security risks: the OCTAVE approach, 1st edn. (Addison-Wesley Longman Publishing Co., Inc., 2002), 471 p.

Anderson R, Moore T (2009) Information security: where computer science, economics and psychology meet. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 367:2717-2727. doi: 10.1098/rsta.2009.0027

Dhillon G, Backhouse J (2000) Technical opinion: Information system security management in the new millennium. Communications of the ACM 43(7):125-128.

Kavun S, Brumnik R (2013) Management of corporate security: new approaches and future challenges. Cyber security challenges for critical infrastructure protection. Ljubljana: Institute for Corporate Security Studies, pp. 141-151

Kavun S, Čaleta D, Vršec M, Brumnik R (2013) Estimation of the effectiveness and functioning of enterprises in boards of corporate security. European Journal of Scientific Research 6(104):304-323

Korchevska L, Zhosan G, Kavun S (2013) Social Responsibility as a Contextual Component of the Enterprise Economic Security. Journal of Finance and Economics 1(4):95-104.

Kurkin MV, Kozhushko OV, Zima OG, Ponicarov VD, Information Security and Protection of Intellectual Capital: a Manual, 1st edn. (Kiev: Nauka, 2016), 256 p.

Kozhushko O (2014) Semantic model of industrial enterprise intellectual capital protection management system. In The International Scientific and Practical Congress of Economists and Lawyers "The genesis of genius", pp. 123-126).

Oleunic UA, Kozhushko YaM, Balabukha AS (2011) Impact of the management of technical and social systems. Information processing systems 2:109-111.

Ponomarenko V, Kavun S, Conceptual foundations of economic security, 1st edn. (Kharkiv national university of economics, Kharkiv, 2008), 250 p.