FORMATION OF THE INFORMATION SECURITY POLICY OF AN ENTERPRISE

Dmytro Diachkov, Candidate of Economic Sciences,
Poltava State Agrarian Academy

In the context of the globalization challenges, successful business conduct requires a faster availability of information on current market conditions, the financial position of competitors, the newest innovation developments, and the last development trends in specific areas of science and production.

At the same time, despite the many years of experience of various enterprises, they still remain vulnerable to unlawful encroachments of organized crime and individuals acting alone not only for the purpose of abduction of information, but also causing harm to the existing software components, technical-technological provision, and disclosure of commercial secrets. Therefore, ensuring the long-term information security of an enterprise and preserving its competitive advantages over the other organizations that play in the same market place, becomes an important necessity for further functioning of modern business entities.

The problems of construction and functioning of the information security system of the enterprises allowed us to consider in detail the most significant issues related to the construction of an effective information security policy for these business entities, which is especially important in today's processes of globalization and integration, because it is impossible to create favorable conditions for the safe and sustainable development of the enterprises without the application of the effective provisions countering unfair competition and various types of information threats.

The creation of an effective information security system requires the implementation of an integrated approach, the most important element of which is related to the formation and implementation of an information security policy.

Taking into account the results of the study of domestic and foreign scientists and researchers, the etymological and epistemological aspects of the concept of the

information security policy of the enterprise can be distinguished.

The term “information security policy”, according to the worldwide-known free online encyclopedia, can be defined as a set of requirements, rules, restrictions and recommendations, regulating the order of information activities in an enterprise and aimed at achieving and maintaining of its information security [10].

Yu. Kovalenko proposes to define the enterprise’s security policy as a set of guidelines, rules, procedures and practical methods of information security that regulate the process of management, protection and distribution of valuable information in an enterprise [7].

Another group of authors defines the duality of the concept of information security policy of an enterprise. On the one hand, they identify this policy with the general principles of working with information resources (databases) for each of the categories of users, and on the other, they characterize it as clearly defined rules of such activity [4, p. 76].

A modern enterprise should be able to properly build an information security policy, that is, to develop and effectively implement a set of preventive measures to protect confidential data and information processes. Such a policy, according to L. Vlasova, presupposes appropriate requirements for personnel, managers at all levels and even technical services [3, p. 14].

Foreign scientists often use the term “information security policy” to describe the perfect standard, with the help of which the expediency of costs, as well as the recoupment of these costs, for protecting resources can be determined. Consequently, the head of the enterprise needs to compare benefits with the costs prescribed in the information security policy to determine the effectiveness of spending [4, c. 82].

Security policy (information security policy of an enterprise) can be also considered as a collection of documented rules, procedures, practices or guidelines in the field of information security that guide the organization in its basic activities [6, p. 90].

A more technological approach to the consideration of the essence of information security policy defines it as “a set of rules for the protection of resources,

including information assets of distributed computer systems" [9].

In this context, special attention should be given to the definition of the information security policy, which arose as a result of the activity of a wide range of business entities. Thus, the top manager team of the one state-owned enterprise in a specially developed information security program determined the information security policy as a reliable provision of information security of the enterprise and, as a consequence, the prevention of material, physical, moral or other damage in the process of design and technological and information activities.

At the same time, top manager team of another organization considers this concept not only as a systematized presentation of high-level goals and objectives of information protection, which should guide the enterprise in its activities, but also as a set of basic principles, which provide a foundation for designing a management system for its information security, able to prevent business-threatening risks.

Some enterprises use international standards as the basis of the information security policy creation, in particular the US security standard "Trusted Computer System Evaluation Criteria" or "TCSEC standard", better known as the "Orange Book" [5].

Summarizing the above definitions, it is worthwhile to note three main aspects of the information security policy:

first of all, it is a set of laws, rules, practical recommendations and experience that determine management and design solutions in the field of enterprise information security;

secondly, effective management, protection and distribution of information in the system on its basis is carried out;

thirdly, it should cover all the features of the process of processing and protecting information, determining the behavior of the information system in various situations.

Thus, the term "information security policy" can be used both in a broad and a narrow sense. In a broad sense, the information security policy is defined as a system of documented management decisions to ensure the information security of an

enterprise. In the narrowest sense, the information security policy is understood as a local normative document that defines the information security requirements, the system of measures, or the procedure for actions, as well as the responsibility of the organization's employees and the core principles of the existing control mechanisms in business to ensure information security.

All this indicates that an important condition for success in protecting information resources of an enterprise is the creation of an atmosphere in the organization that is conducive to supporting the priority of information security. The information security policy is formed from the "top down": first of all, the enterprise's management determines the version of the information security policy, after which the policy is taken by middle and lower managers, and then by other personnel categories. However, in the considered approaches to the definition of the nature of information security policy, it is considered as a set of rules, norms of behavior, documents, instructions, standards, procedures for protecting information resources of an enterprise.

Nowadays ensuring information security of any enterprise implies the need for an effective information service delivery and management of all means of comprehensive information protection and adequate reflection of the threats to information security. The main objective of measures taken to protect information is to guarantee the integrity, reliability, accessibility and confidentiality of information in all its types and forms, including documents and data that are processed, stored and transmitted in information and computing systems, as well as in the telecommunications systems regardless of the type of these data carriers.

At the same time, the main prerequisite for the development of information security policy of an enterpise is related to the internal and external requirements.

Thus, the internal requirements include: the requirements of the eterprise's management system, ensuring competitiveness, demonstrating the interest of top management in ensuring enterprise information security, involving employees in the process of ensuring enterprise information security, reducing the cost of insurance payments, and economic feasibility of these measures. The external factors should

include as follows: the requirements of current legislation and of adopted standards, the requirements of customers and business partners, the necessity for certification, and the requirements of auditors etc. The information security policy is a high-level plan, which describes the goals and objectives of an enterprise's security activities. To create the information security policy of an enterprise, the following areas of information system protection should be used: protection of information system objects, protection of processes, procedures and programs of information processing, protection of communication channels, suppression of spurious electromagnetic emissions, and protection of system management.

However, it is suggested to pay attention to the existence of no less significant category requiring management and protection, which is related to intellectual resources and knowledge of employees of an enterprise. Taking into account the mentioned objects of protection, the information security policy of an enterprise requires the use of a new concept of its formation and implementation software, technical and technological support and implementation of the communication process. On the basis of the above considerations, it's reasonable to assume that the information security policy of an enterprise is the concept of the behavior of employees when carrying out various kinds of work with information resources, practical use of software, technical and technological support and implementation of the communication process. Consequently, the information security policy of an enterprise must be considered not only from the position of formalization (i.e. the development of documents, the creation of the information security plans, the establishment of rules and methods), but also from the point of formation of information relationships and the introduction of the user behavior model of the existing enterprise information system.

A proposed model for building an effective enterprise information security policy can be seen from Figure 1. In this context it is worth by saying that the given model is based on the adaptation of the currently valid international standards ISO 15408 and ISO 17799, as well as on the key aspects of the formation of the information culture of the enterprise [1, 2; 5, 11].

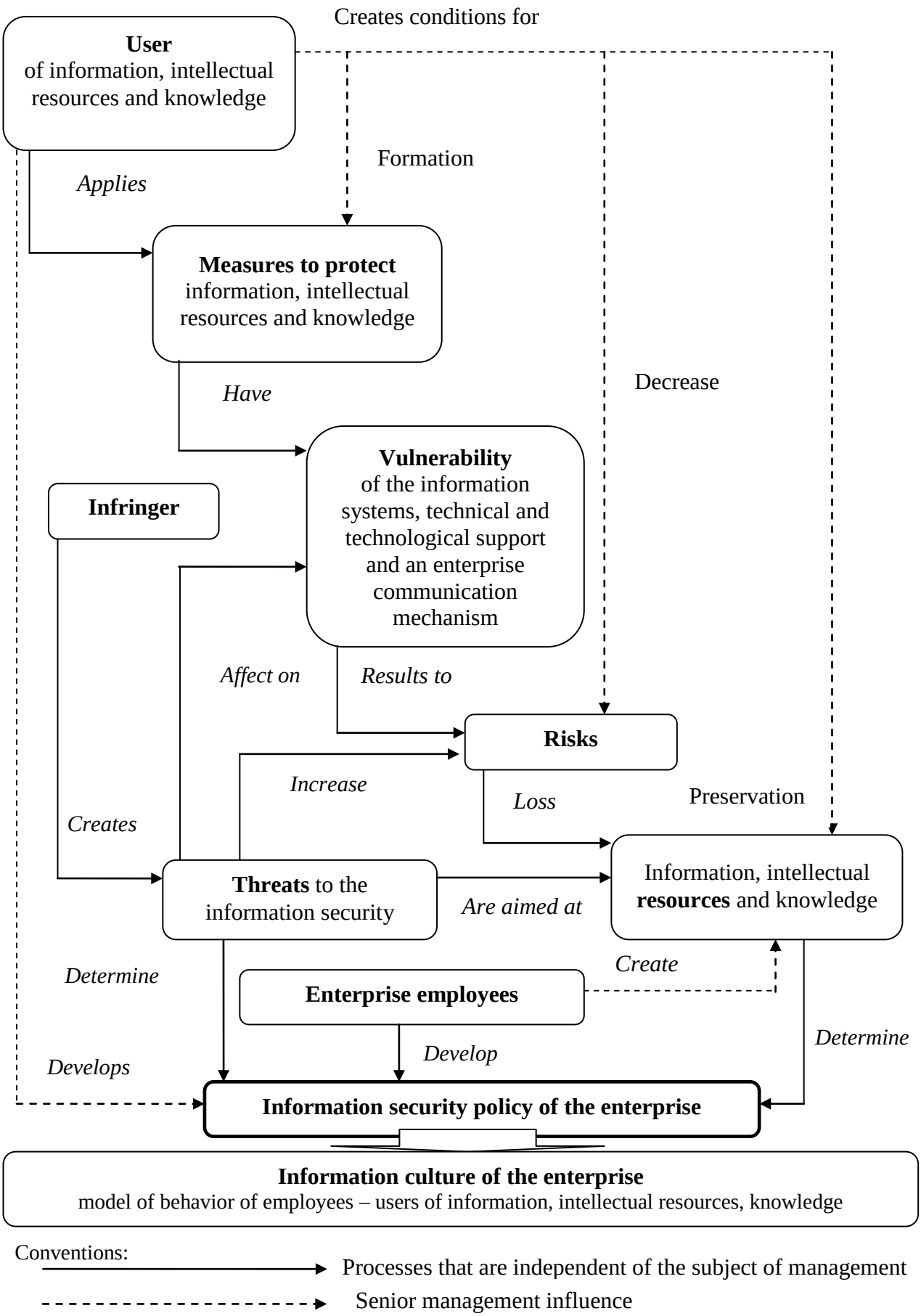

Figure 1. Model of formation of information security policy of an enterprise [developed by the author on the basis of data from: 1; 2; 5; 11]

This model complies with the special regulatory documents on information security GOST R ISO / IEC 15408, the international standard ISO / IEC 15408 “Information Technology – Methods and Means of a Security – Evaluation Criteria for IT Security” and the international standard ISO / IEC17799 “Information Security Management” [1; 2; 5, 11].

The proposed model for the formation of the information security policy of an enterprise is a certain combination of the objective external and internal factors and their influence on the state of information security of an object and on the preservation of material or information resources on the basis of the formation of information relationships. This model, in contrast to existing ones, involves focusing not only on formalized measures to ensure information security, but also on the implementation of the behavior model of the enterprise information system user.

This model, according to the proposed methodology, is constructed as follows: the value of the allocated resources is determined, both from the point of view of the possible financial losses associated with them, and from the point of view of the threat to the reputation of the enterprise, the disorganization of its activities, and the intangible damage from disclosure of confidential information.

The next step is to explain the relationship of resources, to define the threats and to assess the likelihood of their implementation.

Further, based on the established relationships, a system of measures for protecting information, intellectual resources and knowledge should be formed. These measures should be able to reduce the risks to acceptable levels and to ensure a significant socio-economic efficiency. In contrast to the existing information resource protection systems, within the proposed model of information security policy formation, it is advisable to include recommendations on conducting regular inspections of the effectiveness of protection systems (reliability management) and measures to implement the enterprise information culture based on the model of employee behavior with information resources. Ensuring of the increased requirements for information security involves appropriate measures at all stages of the life cycle of information resources (See Figure 2).

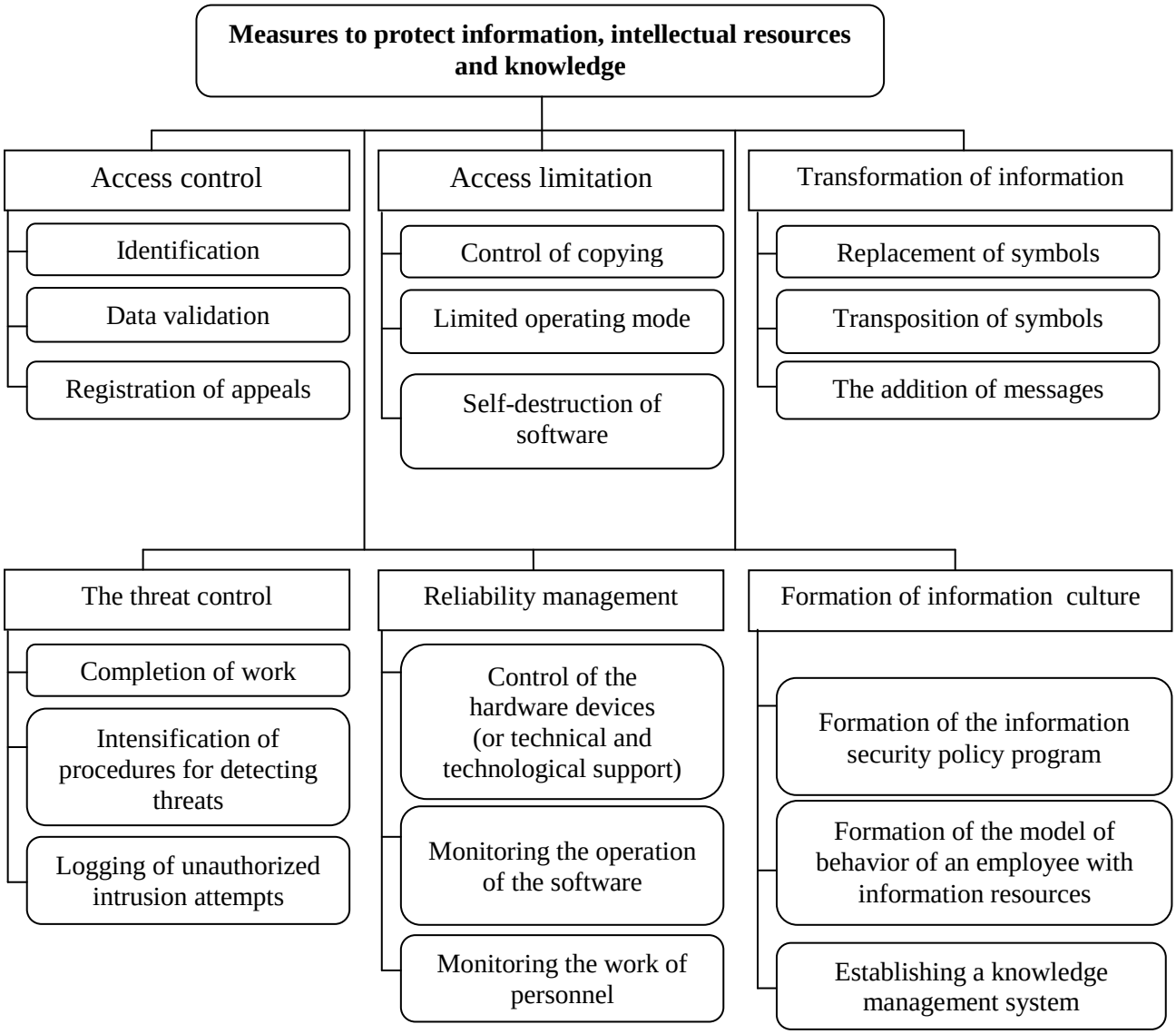

Figure 2. Measures to protect information, intellectual resources and knowledge [developed by the author on the basis of data from: 1; 2; 4; 8]

Planning of these measures is carried out after the completion of the stage of risk analysis and selection of specific activities. The compulsory component of the model of information security policy formation should be a periodic verification of compliance of the existing information security regime, certification of the information system for compliance with the requirements of a certain security standard. An effectively developed information security policy can also serve as a benchmark that allows for the measurement of the degree of competence, as well as the effectiveness of the assignment and work discipline. In fact, the policy must prescribe high standards of information security in advance, therefore the knowledge

and skills of the enterprise personnel must fully comply with these standards. Therefore, the personnel not only must be responsible for the information security of this economic entity, but also for the consequences of various illegal actions.

Foreign and domestic experience in the formation of the information security policy of an enterprise indicates that in order to combat all possible threats related to confidential information, protection of know-how and maintenance of the competitiveness of the business entity, a coherent and purposeful organization of such a counteraction process is needed. In addition, not only employees responsible for a particular line of business should take part in this process, but also highly-qualified specialists in the field of information protection, top manager team of the enterprise and its leading employees. For this purpose it is necessary to develop a concept of the behavior of employees when carrying out various kinds of work with information resources, use of software, technical and technological support and implementation of the communication process.

The purpose of developing the information security policy of a business entity in the field of information security is to determine the effective (from the point of view of the organization) direction of using information, intellectual resources and knowledge of employees, and to develop the procedures that prevent or react to security breaches.

The existence of a scientifically grounded and formalized information security policy is an indispensable condition for the comprehensive protection of a modern enterprise.

References:

1. International Organization for Standardization. 2012. *ISO 17799: Code of Practice for Information Security Management*. [ONLINE] Available at: https://www.iso.org/standard/39612.html. [Accessed 2 January 2018]

2. International Organization for Standardization. 2009. *ISO/IEC 15408-1:2009.* [ONLINE] Available at: https://www.iso.org/standard/50341.html. [Accessed 2 February 2018].

3. Vlasova, L., 2007. Data protection. 1st ed. *Editorial and Publishing Center of Khabarovsk State University of Economics and Law*: Khabarovsk State University of Economics and Law.

4. Guzhov, V., 2007. Development of an information security policy in organizations of the innovation sphere of the economy. 1st ed. *Moscow*: *Twente*.

5. Dyachkov, D.V., (2016). Features of the implementation of information security standards in domestic enterprises. *In conomic development: theory, methodology, management*. Budapest-Prague-Kyiv, 28-30 November. Budapest: Eastern European Center of Fundamental Research. 104-112.

6. Kaminskii, A, (2009). Forming the security policy of information systems. *In international Conference Information Security*. Moldova, 20-21 May. Editorial-Poligraphic Department of ASEM: Editura ASEM. 90-93.

7. Kovalenko, Yu.O., 2010. Ensuring information security of an enterprise. *Economy of industry*, [Online]. 3, 123-129. Available at: http://dspace.nbuv. gov.ua/handle/123456789/24811 [Accessed 1 January 2018].

8. Osadchenko, O., 2008. Information security policy of an enterprise / O. Osadchenko. [Online], 1-4. Available at: http://security.ase.md/ publ/ru/pubru101/15.pdf [Accessed 15 January 2018].

9. Petrenko, S., 2010. *The development of information security policy of an enterprise*. 1st ed. Moscow: Company AiTi.

10. Wikipedia. 2014. *Information Security Policy*. [ONLINE] Available at: https://uk.wikipedia.org/wiki/Політика_інформаційної_безпеки. [Accessed 9 January 2018].

11. Your business. 2016. *Information security standards: State and International*. [ONLINE] Available at: https://tvoi.biz/biznes/informatsionnaya-bezopasnost/prakticheskaya-polza-standartov-info.html. [Accessed 8 January 2018].