UDK 007.51: 330.46

Anatolii Shyian

INFORMATION SECURITY OPTIMIZATION OF AN INNOVATIVE ENTERPRISE BASED ON ACCESS CONTROL

Vinnytsia National Technical University

Abstract: *The development of the economy is carried out through the creation and development of innovative enterprises. It is they who create new technologies, new products, services and knowledge, new technologies of communication, behavior and life of both the individual and society. It must be taken into account that, while working on an innovation, some people should be excluded from admission. The aim of the work is to form requirements for the design of functionality for the development of a computer program that can be effectively used to protect the information of an innovative enterprise based on access control. The developed functionality allows optimizing information security at an innovative enterprise. In particular, it allows you to implement different methods of working with information security incidents.*

Keywords: innovative enterprise; information security; access control; optimization; fragment of document; innovation team.

In recent years, cybersecurity issues have attracted increasing attention from both scientists and practitioners. Both spyware and information security incidents are on the rise. The spread of the number of hybrid wars in the world is an excellent cover for various kinds of information security incidents. The Cyber Security Strategy of Ukraine [1] emphasizes: "The spread of cyber threats to all spheres of life and improving the tools for their implementation necessitates changes in strategies and tactics to combat them. It is important to detect vulnerabilities and cyberattacks as quickly as possible, respond to and disseminate information about them to minimize possible damage." It is also clearly stated that "Ukraine will build a national cybersecurity system based on: … priorities of economic and social development of society". That is, information security management should be aimed at the interests of economic development.

The development of the economy is carried out through the creation and development of innovative enterprises. It is they who create new technologies, new products, services and knowledge, new technologies of communication, behavior and life of both the individual and society.

Let's define, following [2, 3], knowledge (information) as norms of behavior, methods, results of activity, algorithms, and programs of activity of individuals, as well as ways of communicating people in their joint behavior and joint activities. Innovative enterprises can therefore be seen as sources of new knowledge. New knowledge is formalized in the form of documents (a kind of signs, markers) that form a description of knowledge [1, 2].

Thus, innovation is an addition to one or more of the existing documents in society. It is this supplement that is what spreads (socializes) an innovative enterprise into society. It is this addition that the innovative enterprise must keep as the highest secret. As this knowledge is socialized, that is, as we move from an idea to a product, the requirements for the level of secrecy of individual parts (fragments of a document that describes (formalizes) knowledge) or even all knowledge will decrease.

Therefore, the problem arises of managing access to a piece of knowledge that is new for society. There are three significantly different groups of people whose access to information should be regulated.

The first group is the employees of the most innovative enterprise. They have very significant opportunities for obtaining unauthorized access to a secret document that describes new knowledge, or to its individual fragments. The second group is people outside the innovative enterprise. These are competitors, journalists (as people who are looking for new information in society), commercial firms (for example, banks), government agencies (for example, tax authorities), structures of foreign countries, analytical firms, and the like. The third group is potential consumers of new knowledge. They must be prepared to take in the new knowledge correctly, they must know how to use it. Finally, they must be prepared to integrate new knowledge into their own lives.

A very important circumstance is that the access to innovative information of representatives of these three groups will necessarily change over time. In the asymptotic limit of infinite time, the protection of this innovative information must disappear.

Thus, an increasing number of different people get access to individual pieces of innovative information. In addition, it must be taken into account that, while working on an innovation, some people should be excluded from admission. For example, when these people leave the enterprise, or when the invited specialist has finished his work. Of course, some new people need to be given access to some pieces of innovative information.

Finally, access itself should also have many changes. This is, for example, permission / prohibition of modifying innovative information, or copying it to specially specified devices. This is permission/denial to give access to certain employees, or permission/denial of access to several pieces of innovative information. There are also many other situations that need to be taken into account when managing access to innovative information.

There is a fairly large number of different models of access control [4 – 7]. However, each of the models is focused exclusively on well-defined production situations. In addition, they are all stationary. We are forced to consider an initially non-stationary situation. Therefore, it is necessary to develop new approaches to software support for decision-making to ensure information security.

The aim of the work is to form requirements for the design of functionality for the development of a computer program that can be effectively used to protect the information of an innovative enterprise based on access control.

So, new knowledge or innovation is given in the form of a certain document D. This document is formed today, as a rule, in electronic form. The document is formed by a very small group of people, which we will call the "innovation team" (IT). It is these people who have all the information about the innovation.

IT divides the document D into fragments f_i.

$$D = \cup f_i \tag{1}$$

This dividing should take into account that a person who does not belong to the IT, this fragment should be enough for his activity on innovation operations. Some people may have access to more than one of these fragments. The main condition for such a division of document D is the following: a person outside the IT should have only the information that he needs to perform his functional duties.

In the general case, as a result of such a partition, a hierarchical set of fragments f_{ki} is formed, where k specifies the level of the hierarchy, and i specifies a document fragment.

$$D = \cup_k \cup_i f_{ki} \tag{2}$$

Some f_{ki} unions are allowed to contain several fragments from this or lower levels.

$$f_{ki} = \cup'_{l<k} \cup'_i f_{li} \tag{4}$$

In (4), the prime indicates that only some of the f_{ki} are used.

All employees of firm h_s who are involved in the innovation are assigned an access level in the form of such a two-component vector. The access level g is assigned by the IT together with information security specialists.

$$h_s = \left(f_{ki}, g \right) \tag{5}$$

Here g is the level and form of access that can accept the given knowledge (for example, read only, read and append, partially delete, modify, etc.).

The people who have the right to shape the distribution of employee access should also be singled out. They are denoted as h_t, where the index t stands for IT.

$$h_t = \left(\cup f_{ki}, \cup_t g_t \right) \tag{6}$$

When writing (6), it is taken into account that a member of the IT can, firstly, give access to several different fragments of the document D, and, secondly, give different levels and forms of access to this document.

The operation of creating access (1) - (6) is repeated at certain time intervals τr. Note that, as a rule, the document D itself changes as well.

$$D_{\tau r} \to D_{\tau(r+1)} \tag{7}$$

All copies of document D after each change must be archived. Only specified people have access to the archive. However, they do not have the right to delete or change copies of the document until the innovation project is completed.

To complete the information security optimization management of an innovative enterprise based on access control, it is necessary to perform the following during each stage (1) – (6) and during the transition from stage to stage (7). Since the IT and the information security specialist cannot always maintain the required level of communication, the computer program must recognize violations in violation of conditions (5) and (6).

For example, there may be situations that require the intervention of the IT and/or an information security specialist.

Example 1. One of the members of the IT gave access to "read" to a certain fragment of document D to a certain employee of the company. Sometime later, another member of the IT gave the same employee access to "change" the same fragment of document D. However, this person has the right according to (5) access only at the "read" level.

Example 2. An IT member grants an employee a type of access that the IT member is not authorized to grant.

In Examples 1 and 2, the computer program should inform the information security specialist about the presence of violations. And already the specialist makes decisions on how exactly he will respond to this incident.

The developed functionality allows optimizing information security at an innovative enterprise. In particular, it allows you to implement different methods of working with information security incidents.

REFERENCES

1. Decree of the President of Ukraine of August 26, 2021 № 447/2021 "Cyber Security Strategy of Ukraine. Safe cyberspace is the key to Ukraine's successful development." (In Ukrainian).

2. Shiyan, A. A., Nikiforova, L. O. Typology of Institutions – Theory: Classification of Institutions via the Methods for Transmission and Modification of Knowledge. Social Science Research Network (January 4, 2013). http://ssrn.com/abstract=2196300 or http://dx.doi.org/10.2139/ssrn.2196300.

3. Petrov, M. K. Language, Symbol, Culture. Moscow : Nauka, 1991. (In Russian).

4. Devyanin P. N. Security models of computer systems. Moscow : Academy, 2005. 144 p. (In Russian).

5. Grusho A. A., Timonina E. E., Primenneko E. A. Theoretical Foundations of Computer Security. Moscow : Academy, 2009. 272 p. (In Russian).

6. Zegzhda D. P. Information security. Moscow: MSTU named N. E. Bauman, 2010. 236 p. (In Russian).

7. Bogush V. M., Dovydkov O. A., Kryvutsa V. G. Theoretical foundations of secure information technology. К.: ДУІКТ, 2010. 454 с. (In Ukrainian).

Shiyan Anatolii – PhD in Physics, Associate Professor, Department of Management and Information Systems Security, Vinnytsia National Technical University. E-mail: anatoliy.a.shiyan@gmail.com.