UDC 621.396.2

Zh.V. Kudrytska, Cand. Sci. (Econ.)
(National Aviation University, Ukraine)
O.I. Klimova, Cand. Sci. (Econ.)
(Donetsk State University of Management, Ukraine)
O.V. Aparova, Dr. Sci. (Econ.)
(State University of Telecommunications, Ukraine)

Evaluation of State and Information Security Management

The report examines the methods of assessing the level of information security of subjects and the principles of the system approach to information security, the main indicators of information security assessment, methods for assessing information security risks and the main elements of technology management of the information security regime.

The globalization of world economic and political processes requires the maintenance of a high level of information security and preservation of information resources of economic, political and social relations. This need arises as a result of intensive use of the achievements of modern information technologies.

On the other hand, in order to provide an adequate level of information security, it is necessary to determine the state of information security of an enterprise, as well as indicators that characterize this state, and their meanings. In the conditions of uncertainty which now features all spheres of activity, the implementation of this task faces certain difficulties. Therefore, in order to ensure the proper state of information security, a systematic approach is needed, which includes a set of interrelated measures, such as the use of special technologies and software tools, organizational measures, regulatory, etc.

The main objective of any information security system is to create conditions for the operation of an object, to prevent threats to its security, to protect its legitimate interests, to prevent theft of funds, disclosure, loss, leakage, distortion, and destruction of official information at the level of all its subsystems.

While ensuring the information security regime, a very important place assigned to the task of analyzing and managing the company's information dangers. Typically, the process of performing tasks includes the following steps: the formulation of security policy; defining the scope of the system of information security management and the specification of the objectives of its creation; evaluation of existing hazards; selection of countermeasures that provide the necessary regime of information security; identifying and managing risks; checking system information security management.

The most widely used indicators of the level of information security are the coefficients of completeness of information, the accuracy of information, inconsistency of information. An assessment of the level of information security is usually determined on the basis of three mentioned coefficients. In this case, the level of safety is high, if the product is greater than or equal to 0.7, the level of safety is average, if it is within [0.3; 0.7], the safety level is low if its value is less

than 0.3.

The most common methods for assessing the risks of information security are the following:

1) OCTAVE risk assessment methodology (Software Engineering Institute, USA);

2) FRAP group process of risk analysis (for conducting a qualitative risk assessment);

3) CRAMM method of analysis and risk management of the Central Agency for Computers and Telecommunications (CCTA), UK.

The OCTAVE methodology provides for the process of analyzing information security risks only by employees of an enterprise without involving external consultants because such employees better understand the needs of the enterprise and its inherent risks.

This methodology is used to develop a profile of threats, identify vulnerabilities in information security and develop a security strategy. For each source of threats, a variant tree is built, which clearly shows the appearance of the threat and the ways to eliminate it. In assessing the risks to information security, a scale of three positions formed: high, medium and low level of risk, and possible financial loss calculated. The main advantage of this method is that it is available and free of charge.

The FRAP methodology constructed in such a way that any person with group work skills can successfully analyze information security risks. According to this method, it is necessary to perform the following: brainstorming session to identify all threats to the company's information security; identification of the probability and vulnerability for each threat on the scale of large/medium/low; drawing up a report on the results of the possible impact of each of the threats. The advantage of this technique is the rapidity and ease of decision-making.

The CRAMM method combines quantitative and qualitative risk assessment techniques. The method is universal. CRAMM software versions are targeted at different types of businesses and differ in their knowledge bases. For commercial enterprises, there is a commercial profile, and for the government - a government profile. The government profile allows conducting the audit to meet the requirements of the ITSEC standard.

The CRAMM method allows economically justifying the costs of an enterprise to ensure information security and business continuity. It is divided into three segments: identification and valuation of assets, analysis of threats and vulnerabilities, selection of countermeasures. This method, despite its considerable versatility and functionality, has such disadvantages as the need for special training for users and the significant cost of the license.

It is advisable to use the OCTAVE technique for small businesses, FRAP - for medium, and CRAMM - for large.

Information security plays an essential role in ensuring the vital interests of any country. The purpose of ensuring information security in Ukraine is to create an extensive and protected information space, protect Ukraine's national interests in the formation of world information networks, protect the state's economic potential from illegal use of information resources, and realization of the rights of citizens,

institutions and the state to receive, disseminate and use information.

An important role is played by the development of the risk management strategy. Such a strategy may include traditional approaches to information risk management: risk reduction; risk aversion; change in the nature of risk; taking the risk.

Various models and methods for evaluating threats are important for effective information security. The use of this or that method depends both on the level of development of a particular civilization, and on the context of the assessment, the availability of comprehensive data on the factors of the threat, the algorithm for calculating the probability of occurrence and the size of the negative consequences. The significance of each method should be determined in the light of the specific risks faced by the subject. Commonly accepted methods of providing information security include the following: the creation of a document defining a policy of information security; distribution of responsibility for information security; training in the field of information security; incident reporting; support for business continuity. These methods can be used in most organizations and in most environments.

Also, an important method of providing information security is the method of critical scenarios. In these scenarios, situations analyzed where an imaginary opponent paralyzes the control system and accordingly reduces the ability to maintain control within the optimal parameters.

The technology of information security management in the full version includes the following elements: documenting the information system of the organization from the standpoint of information security; categorization of information resources from the position of management of the organization; determining the possible impact of various security events on information technology; risk analysis; technology of risk management at all stages of the life cycle; audit in the field of information security.

Risks usually assessed according to several criteria (not only cost). It is important to take into account that there will be the risks which remain always. The choice of certain residual risk values should also be considered in the course of their assessment.

At the risk analysis stage, quantitative methods are used to assess the residual risk parameters and the effectiveness of different options for countermeasures in risk management.

In the future, different variants of optimization tasks in the field of providing information security regime considered and solved. Such tasks can be represented by the following:

1) selection of the information security subsystem optimized according to the “cost-effectiveness” criterion at a given level of residual risks;

2) selection of the information security subsystem option, which minimizes residual risks at a fixed cost of the security subsystem;

3) selection of the architecture of the information security subsystem with the minimum cost of ownership during the life cycle at the established level of residual risks.

Conclusions. Thus, the considered technology will allow raising the

essence of managerial decisions in a qualitative way, ensuring the effective use of information resources and reducing the costs of providing information security. The next step in managing the level of information security can be the development of an automated system for monitoring the state of information security. Such a system could accumulate information about the state of information security, calculate the values of indicators and provide recommendations for managing the state of information security of the enterprise.

References

1. Безбожний В.Л. Передумови забезпечення соціально-економічної безпеки великих промислових підприємств [Текст] / В.Л. Безбожний // Управління проектами та розвиток виробництва: Зб.наук.пр. – Луганськ: вид-во СНУ ім. В. Даля, 2013. – №1(45). С. 10-15.

2. Россошанская О.В. Метод оценки экономической безопасности инновационных проектно-ориентированых предприятий с позиции метрики внутренней среды деятельности [Текст] / О.В. Россошанская // Управління проектами та розвиток виробництва: Зб.наук.пр. – Луганськ: вид-во СНУ ім. В. Даля, 2013 – No 1(45). -С. 33-44.

3. Рач В.А. «Небезпека/ризик/криза» як тріадна сутність процесів розвитку в сучасній економіці [Текст] / В.А. Рач // Управління проектами та розвиток виробництва: Зб.наук.пр. – Луганськ: вид-во СНУ ім. В. Даля, 2013. – № 1 (45). – С. 155-160.

4. Christopher J. Alberts. Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0 / Christopher J. Alberts, Sandra G. Behrens, Sandra G. Behrens, Sandra G. Behrens. – Pitsburg : Carnegie Mellon University, 1999. – 72 p.

5. Thomas R. Peltier. Facilitated Risk Analysis Process (FRAP) [Electronic Resource] / Thomas R. Peltier. – 2000. – Mode of access: www.ittoday.info/AIMS/DSM/85-01-21.pdf.

6. Hank Marquis. 10 Steps to do it yourself CRAMM [Electronic Resource] / Hank Marquis. – 2006. – Mode of access: http://www.itsmsolutions.com/newsletters/DITYvol2iss8.htm.

7. ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements.

8. ISO GUIDE 72:2001, Guidelines for the justification and development of management system standards.

9. ISO/IEC 27003, Information technology – Security techniques – Information security management system implementation guidance.

10. Technical Report ISO/IEC TR 18044, Information technology – Security techniques – Information security incident management.