Modeling the risk level of information security at enterprise

https://doi.org/10.31713/MCIT.2020.23

I. Karpovych
Department of Computer Technology and Economic Cybernetics
National University of Water and Environmental Engineering
Rivne, Ukraine
karpivan@ukr.net

O. Hladka
Department of Computer Technology and Economic Cybernetics
National University of Water and Environmental Engineering
Rivne, Ukraine
o.m.hladka@nuwm.edu.ua

Ju. Nakonechna
3nd year student
National University of Water and Environmental Engineering
Rivne, Ukraine

Abstract—**The paper is devoted to the study of cybersecurity of information resources at an enterprise. We consider some of the methods that allow you to analyze information security risks and evaluate the optimal costs for an enterprise to protect information. Addressing the cybersecurity problem of information resources requires the preparation and adoption of organizational and technical measures, the development of which is based on the approaches proposed.**

Keywords—risk; informational security; threats; minimizing risks; cybersecurity

I. Introduction

In the context of accelerated dynamics of development of informatization of society, there is an annual tendency of growth of cyber threats to information resources, so their protection is one of the important problems. This task requires the preparation and adoption of organizational and technical measures to ensure cybersecurity of information resources. This paper examines the basic approaches that allow you to conduct risk analysis and estimate the optimal cost of information security.

The concept of risk is known to result from the close interaction of concepts such as asset, vulnerability, threat and loss. Assets are key components of infrastructure and important information that is processed in the information system. The ISO / IEC 27000 standard [1], which describes in detail the procedures of an information security management system, allows us to conditionally divide the assets of the organization into main and ancillary. The main assets include business processes – a set of activities that results in the creation of a product or service of interest to the consumer. The main asset is also information – information that is subject to ownership, subject to protection against breach of confidentiality, integrity and accessibility in accordance with the requirements of legal documents and requirements of the owner of the information, regardless of the form of submission, in particular, information resources (databases and files, system documentation, research and documentation, contracts and agreements, etc.). Ancillary assets include, first and foremost, a hardware and software complex – a set of hardware and software intended to perform interdependent limited-information-processing operational functions, which includes active data processing equipment, fixed equipment, peripherals, operating systems, and application software. The same category includes data carriers; a set of telecommunication devices used to connect several physically remote segments of an information system; employees of the company, their qualifications and experience, as well as intangible resources (reputation and image of the company).

Vulnerability is a weak spot in information security, caused by errors or imperfect procedures, projects, implementation that the threat can overcome. In other words, vulnerabilities are any factors that make a successful implementation of threats possible. Practice shows that vulnerabilities are the main cause of attacks. A threat is considered to be a potential opportunity to cause damage in a known manner in advance. Information security threats can beeen realised by exploiting system vulnerabilities. Security weaknesses can be used by one or more threats, which can cause unwanted incidents that can cause components of the information system to malfunction. The presence of weaknesses in the protection of the information system may be due to various factors, ranging from mere negligence of employees and ending with deliberate actions of the attackers. Losses are the costs of restoring the system after a possible breach of information security.

Risk is the probability that certain undesirable events will occur that adversely affect the achievement of the goals of a particular business process. In particular, the functioning of the

enterprise in the IT industry is related to innovative processes, development and production of new products, works, services. Innovative activity, the pursuit of competitive advantage, compels the company to introduce the latest achievements of science, new products and technology, a new system of labor and production management in order to maintain leading market positions, which is combined with numerous risks that have a significant impact on the company's business results. In this regard, timely, prompt and correct assessment of the risks of reduction or complete loss of information security is today a pressing problem in the activities of any organization.

The development of enterprise information infrastructure entails an uncontrolled increase in the number of information threats and vulnerabilities of information resources. Current research has identified the following types of sources of threats that affect information security: natural; technogenic; human intentional and human unintentional.

The following types of activity risks are characteristic of the innovative type of enterprises to which the companies of the IT branch belong: organizational (low qualification of project developers, delay of execution of stages of its realization); scientific and technical (deterioration of technological equipment, lack of capacity reserves or typical design decisions); financial and economic (marketing, project financing risk, inflation, interest rate, tax and operational risks).

In modern conditions, every enterprise that cares about the security of its information resources is asked the question about the organization of information security system, which would guarantee the security of the functioning of telecommunication equipment and circulating information in the enterprise information system. The effectiveness of information security depends on the approach to its organization and the correct choice of methods for calculating information security risks. There are many risk assessment and treatment techniques that can be applied to any information system, regardless of the level of confidentiality of the information available. However, in order to build a quality information security system using such techniques, however, a considerable amount of information about potential attacks, as well as attempts to implement them, is required, which is subject to programmatic analysis to identify the most pressing threats to information security.

II. METHODS OF RISK ANALYSIS AND ASSESSMENT OF OPTIMAL COST

Information security, determining the level of security of the business environment, becomes an important aspect of overall economic security in the activities of a modern company. Information security is a special type of activity to prevent information leakage, unauthorized changes to its flows and other factors that adversely affect the stable operation of the organization and related economic partners (customers, equipment suppliers, investors, etc.).

The process of information security risk calculation is relevant at all stages of the information security system and is interesting for the information owner, first of all, in terms of economic losses. The choice of the method of information security risk assessment is in most cases based on the following factors: time, financial, information resources; the degree of uncertainty of information security risk assessment; the presence or absence of the ability to quantify inputs, where inputs may include conclusions, decisions, lists, and recommendations, depending on the method and stage of information security risk assessment. At the same time, the risk assessment process should establish risk acceptability criteria and criteria for information security risk assessment, as well as guarantees that the risk analysis will provide reliable and consistent arrays relevant to the given system of risks.

We must identify information security risks that target information resource properties such as confidentiality, integrity, and accessibility. It is necessary to carry out identification of the owner of the risk, where the owner is understood to be an individual, legal entity or unit responsible for risk management and having the necessary powers for this, in this case, we can refer to managers, information security specialists, information security departments, etc. In the process of information security risk analysis, the potential loss in the event of a risk is assessed, the probability of risk realization is assessed and the magnitude of the risks is determined. During the assessment of information security risks, a comparison of the risks with the established criteria should be made, as well as a vector of priority directions for their processing.

Analyzing and assessing risks in the problem of information security management is one of the most difficult and topical tasks for today. The difficulty is that there are no generally accepted approaches and techniques for risk assessment. Risk factors (threat, vulnerability, damage) are analyzed using heuristic methods that contain a subjective component.

Risk analysis involves a procedure for identifying risk factors, assessing their significance and methods for reducing of risk or reducing the associated adverse effects. The current tasks of analysis and assessment of information security risks make it possible to determine the required level of information security, as well as to develop recommendations for improving the system of protection and minimization of risks.

Risk analysis is divided into two types: qualitative and quantitative. Qualitative analysis allows to identify factors, areas and types of risks. Quantitative risk analysis makes it possible to numerically determine the size of individual risks and the overall size of the risk as a whole. The overall results of a qualitative risk analysis may, in turn, be input to quantitative analysis. However, quantitative risk analysis requires reliable input data (the collection of statistical information is complicated by stiff competition in the business environment) and a well-defined scale for the parameter estimation. The conceptual bases of qualitative and quantitative risk analysis, the system of indicators of its evaluation, basic approaches to modeling, management and methods of risk reduction are analyzed in detail in the monograph [2].

Based on quantitative analysis, we consider risk R as a complex value that depends on such factors as threats, vulnerabilities and losses [3]:

$$R = \lambda P_T P_V(z), \quad (1)$$

where λ is the amount of damages caused by the breach of security of information assets; P_T is the probability of a threat; $P_V(z)$ is a function that describes the probability of realization of the threat to an information asset depending on the cost of z to provide security measures.

Thus, the magnitude of the losses depends on both the information to be protected and the predetermined probability of a threat. The probability of a threat being realized can be significantly reduced by investing in an asset's information security.

The task of risk management of the company is to reduce the impact of undesirable factors on the life of the organization to get the results of work as close as possible to the desired ones that meet the set goals. Risk management is a set of methods of analysis and neutralization of risk factors, integrated into the system of planning, monitoring and effective corrective actions for their reduction [4, 5]. This set of measures includes identification, risk analysis and decision making aimed at reducing the probability and extent of their impact on the company's performance.

As information security studies have shown, all information security risks must be consistent with the risks of the organization as a whole. Thus, the task of integrating the information risk management system with the company-wide management system arose. Quantitative calculation methods make it possible to financially justify investments in information security and to find out the cost-effectiveness of these costs. However, the issue of optimizing information security investments and identifying those areas of the system for which increase security costs most significantly reduce the risk to the system as a whole remains unexplored remains unexplored.

Considering the significant variety of threats, the development of techniques and algorithms for assessing the risk of reduction or complete loss of information security is a very time-consuming and important task for any information system. First of all, it is necessary to build flexible integrated models of the information system, taking into account software, hardware resources, internal and external threats and vulnerabilities, which can be customized according to the peculiarities of a particular organization. In addition, given the large number of risk factors involved, a mathematical model of information security assessment should allow the development of effective numerical information processing algorithms.

In order to assess information security risks, it is important to identify and analyze the main factors through which threats affecting the information system in the sense of failure or impairment are realized. A significant number of information security risk assessment methods include the risk assessment method, which is based on building a model of threats and vulnerabilities.

This methodology is based on the use of expert and statistical information on threats and vulnerabilities. To evaluate risks in an organization's information system, security of each valuable resource is determined by assessing the probability of implementation of threats affecting a specific resource of the organization (eg, the probability of failure in the information security system due to low staff skills, lack or aging of software or hardware security, etc.), and the vulnerabilities through which these threats can be addressed. This probability assessment allows you to rank threats and vulnerabilities by degree of risk.

Since information security risks are closely linked to the use of modern information technologies, which determine the effectiveness of the organization in its innovative aspect, they can be attributed to a variety of innovation risks. When defining innovation risk as the probability of losses due to a misplaced or unfulfilled strategic goal [6], it is expedient to use such an indicator as the level of costs (in material or cost terms) for restoring the system performance in characterizing the risks of system failure.

Based on the expert data on risks, vulnerabilities and costs for each of the resources, it is possible to build a model relevant for the information system of the organization, and to analyze the functioning of the information system in terms of minimizing the risks of failure or reducing the efficiency of the system and, consequently, maximizing its effectiveness by the criterion information security. In the first stage of solving this problem, we find the most important for the organization the areas of activity, which determine (in terms of its management) the level of information security. In the second stage, the importance of each threat is calculated for the selected areas of activity based on the expert assessment of the probability of realization of information security threats, as well as the level of cost in terms of restoration of the system capacity is estimated. The total risk of system failure is calculated as the sum of the risks in each area.

The result of the solution of the described problem will be the allocation of financial resources in the selected areas of activity of the organization, which minimizes the risks of failure of the system by the criterion of information security.

With a significant number of information security threats, optimization methods can be used to numerically assess risks. Consider a mathematical model for minimizing information security risks.

Let in the technical or socio-economic system we know the dependence $r_i = f(x_i)$, where r_i are the risks of failure of the system, x_i are the cost of their avoid (exclude, reduce) in the i-th ($i = 1, \ldots, n$) direction of providing information security (hardware, software failure, system failure due to understaffing of employees, managers, etc.). To minimize information security risks, we will use an indicator such as the

level of costs (in material or cost terms) to restore the system's performance in the event of its failure in one or more areas.

We define the following values: $R = \sum_{i=1}^{n} r_i$ is total risk of system failure; Z is the maximum cost of reducing (eliminating) the allocated risks. Let the cost functions be linear functions of x_i , that is, $f(x_i) = a_i - b_i x_i$, ($i = 1, \ldots, n$). The coefficients a_i can be interpreted as costs that the system may incur in the absence of costs to prevent risks or, otherwise, the maximum costs of organizing a crisis-free system operation in the i-th direction of guaranteeing security, and the coefficients b_i as the weighting coefficients reflecting the relative importance of i i-th direction of guaranteeing safety [7].

Considering $R \to \min$ as a function of purpose, one can formulate the following mathematical programming problem:

$$\begin{aligned} &\sum_{i=1}^{n} b_i x_i \to \max, \\ &\sum_{i=1}^{n} x_i \le Z, \\ &x_i \ge 0 \quad . \end{aligned} \qquad , \qquad (2)$$

Model (2) is a multi-parameter linear programming problem. Given the boundedness of all the variables of the problem and the non rigidity of the constraints, it can be argued that the acceptable set of solutions is non-empty and the problem can be solved using the simplex method (see, for example, [8]), which with the help of modern computer technology will allow to consider practically unlimited number n of information security threats.

The practical application of model (2) can be divided into two steps. The first is the assessment of the pressure of each of the significant groups of negative influence on the position of the enterprise; the second is the choice of an appropriate protective action strategy.

In real terms, the number of risk groups that pose a real threat to the information security of a company is relatively small. In particular, according to theoretical studies [9], the risk of threats to information security of the enterprise is caused by the action of five major competitive forces: the risk of occurrence of goods-substitutes, intra-industry threats of competition, the emergence of new competitors, the threat (risk) of loss of customers, the threat (risk) vendor. The main indicators that determine the effect of these factors are: demand conditions, production conditions, the nature of the company strategy, the presence of concurrent or related industries.

This theory makes it possible to evaluate the competitive position in the market and on this basis to develop such a variant of the long-term strategy of the firm, which will maximally ensure its protection and at the same time will help to create additional competitive advantages. The analysis performed in [10] made it possible to identify risk groups with a high probability of occurrence and to assess the level of major risks of the company.

CONCLUSIONS

An analysis of existing approaches to the problem of risk management of complex systems shows that this problem area is not yet well formalized and studied. To reduce the degree of uncertainty in the choice of possible options for solving risk management problems, we use a different mathematical apparatus: methods of subjective probability, fuzzy sets, neural networks, etc.

Today, small and medium-sized enterprises are part of the economy most susceptible to technological, informational and business innovation. Meanwhile, many small and medium-sized enterprises, while in the information environment, ignore all kinds of threats to their information system, thereby putting themselves at risk of financial loss. Reducing (minimizing) the risk inherent in the company's activities contributes to enhancing its competitiveness.

REFERENCES

[1] ISO/IEC 27000:2009. Information technology — Security techniques — Information security management systems — Overview and vocabulary.

[2] V. V. Vitlinsky, and G. I. Velikoivanenko, “Riskology in Economics and Entrepreneurship”: Monograph, K.: KNEU, 2004. 480 p.

[3] V. Y. Korolev, V. E. Bening, and S. Y. Shorgin, “Mathematical foundations of risk theory”, Moscow: FIZMATLIT, 2011, 620 p.

[4] T. Lister, and T. Demarco, “Waltzing with the bears. Risk management in software development projects”, Moscow: Company p. m. Office, 2005, 196 p.

[5] A Guide to the Project Management Body of Knowledge. (PMBOK Guide), Fifth edition, Project Management Institute, 2013, URL: http://dinus.ac.id/repository/docs/ajar/PMBOKGuide_5th_Ed.pdf

[6] N. D. Ilyenkova, “Problems of Innovation Risk Analysis”, in Investments and Innovations, № 5, 2011, pp. 90–92.

[7] A. V. Medvedev, “Mathematical model of estimation of investment attractiveness of the region”, in Modern science-intensive technologies, № 8–2, 2013, pp. 357–361.

[8] S. I. Nakonechny, and S. S. Savina, “Mathematical Programming”,: Textbook, K.: KNEU, 2003, 452 p.

[9] M. Porter, “Competitive advantage. How to achieve a high result and ensure its sustainability”, Moscow: Alpina Publishers, 2008, 720 p.

[10] I. A. Nechaieva, and Ye. A. D′ordiy, “Management of enterprise risks in the IT services sector as a tool to increase its competitiveness”, in An efficient economy, № 12, 2018, URL: http://www.economy.nayka.com.ua/?op=1&z=6797 (accessed: 01/23/2020). DOI: 10.32702 / 2307-2105-2018.12.120.