2022 IEEE Smart Information Systems and Technologies (SIST)
28-30 April, 2022, Nur-Sultan, Kazakhstan

Comparative analysis of risk assessment during an enterprise information security audit

1st Alimzhanova Zhanna
Department of Information System of Al-Farabi Kazakh Nationl University, Department cybersecurity Almaty academy of the ministry of internal affairs of the republic of Kazakhstan named after M. Esbulatov
Almaty, Kazakhstan
0000-0001-6282-5356

2nd Tleubergen Akzer
Department of Information System of Al-Farabi Kazakh Nationl University
Almaty, Kazakhstan
0000-0002-1178-4491

3rd Salamat Zhunusbayeva
Department of Information System of Al-Farabi Kazakh Nationl University
Almaty, Kazakhstan
0000-0002-1400-354X

4th Nazarbayev Dauren
Department of Information System of Al-Farabi Kazakh Nationl University
Almaty, Kazakhstan
0000-0001-7505-0422

Abstract. **This article discusses a threat and vulnerability analysis model that allows you to fully analyze the requirements related to information security in an organization and document the results of the analysis. The use of this method allows avoiding and preventing unnecessary costs for security measures arising from subjective risk assessment, planning and implementing protection at all stages of the information systems lifecycle, minimizing the time spent by an information security specialist during information system risk assessment procedures by automating this process and reducing the level of errors and professional skills of information security experts. In the initial sections, the common methods of risk analysis and risk assessment software are analyzed and conclusions are drawn based on the results of comparative analysis, calculations are carried out in accordance with the proposed model.**

Keywords: risk assessment; information security; risks; vulnerability; risk management; information security audit.

I. INTRODUCTION

Considering that at the present stage of economic development, the assessment of information risks is one of the main directions of protection against threats, it is necessary to further improve the applied methodological approaches to the assessment of information risks. Therefore, the solution of theoretical and practical problems of assessing information threats is an urgent scientific problem of today. At the same time, such important issues as the economic essence of information assets, changes in their value as a result of destabilizing effects on them, the economic efficiency of using various means and methods of protecting information assets and others remain less studied. Therefore, today it is necessary not only to create new forms and methods of management in the field of information security, but also to form new methodological approaches in the field of assessing the security of information assets.

Relevance of the topic: at present, the organization of the information security regime is becoming an important strategic factor in the development of any company. Due to the increasing role of information and telecommunication systems and technologies in the activities of organizations, the relevance and necessity of applying procedures for assessing and managing risks and risks information systems is constantly increasing.

The purpose of the article: to consider a model of risks and vulnerability analysis based on the analysis of existing methods for assessing information risks.

To achieve this goal, it is necessary to study and analyze existing algorithms and methods about their sufficiency and application in production activities, and study in detail the proposed methodology and assess the risks and threats of information systems.

The object of research of this work is the information system of enterprises with a multi-level structure.

The object of research is a threat and vulnerability analysis model that allow assessing the risks of information security conditions at the object of research. The novelty of the work lies in the fact that the method under study is implemented in the form of software that allows an information security specialist to reduce the time spent on information system risk assessment procedures by automating this process and minimize

errors and professional skills of information security experts that pose a threat to information security.

To date, many foreign companies specializing in solving complex problems of information security have developed and presented their own methods of information risk management. These methods differ, first off all, in the level and perfection of the applied mathematical methods underlying the risk assessment procedures. In this regard, they have various possibilities of adequate consideration of specific factors, which, in turn, determines the accuracy and reliability of the assessment of the resulting risk [1].

COMPARATIVE ANALYSIS OF INFORMATION SECURITY RISK ASSESSMENT METHODS

Despite the increased interest in risks management, most of the techniques currently used are relatively ineffective, since this process is carried out independently in each division in most companies. Centralized control over their actions is often absent, which excludes the possibility of implementing a unified and holistic approach to risk management throughout the organization. To solve the problem of information security risks assessment, the following software packages are used: CRAMM, FRAP, RiskWatch, Microsoft Security Assessment Tool (MSAT), ГРИФ, CORAS and others [2]. All known methods can be classified as follows:

- methods that use risk assessment at a qualitative level (for example, on a scale of "high", "medium", "low"), FRAP belongs to this method;
- quantitative methods (the risk is estimated a numerical value, for example, the size of the expected annual costs), the RiskWatch methodology belongs to this category;
- methods using a mixed assessment (such methods include CRAMM, MSAT).

Let's consider a number of methods for analyzing and assessing information security risks from the point of view of their possible use. Before making a decision on the implementation of a particular information security risk management methodology, it is necessary to make sure that it fully takes into account the business needs of the company, its scale, and also complies with the best international practices and contains a detailed description of the processes and required actions [2].

In order to determine the most appropriate methodology for assessing information security risks for small and medium-sized business, the analysis of the methods discussed above was carried out according to criteria corresponding to the need of organizations, as well their capabilities.

The result of a comparative analysis of the information security risk assessment methodology is presented in Table 1 and their visualization in Figure 1.

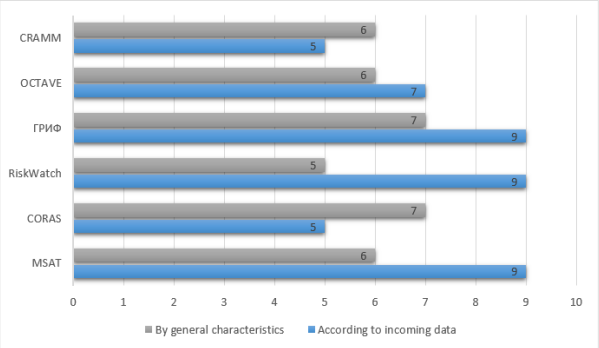

Figure 1. Comparative analysis of information security risk assessment methods

The analysis was performed using a combination of two estimates: the maximum value of the estimate for general characteristics and the minimum value of the estimate for input data.

This choice is due to the fact that for the organization the most priority criterion is the ease of use of the methodology, its evaluation and completeness of the evaluation results, and a large amount of input data for the use of the methodology makes it difficult to apply it [3, 4].

TABLE I. COMPARATIVE ANALYSIS OF INFORMATION SECURITY RISK ASSESSMENT METHODS

Name of the method	**Analysis result**	**Applied methods and standards**
ГРИФ	The methodology uses both qualtiative and quantative risk assessment, determines the conditions under which the risk can be accepted by the company. This methodology is focused on the public sector and is not adapted for use by small and medium-sized bussiness.	Analysis of the information flow model
CRAMM	CRAMM uses an integrated approach to risk assessment, combining methods of quantitive and qualitive analysis. The methods is universal and suitable for both large and small organizations, as well as for the government and commercial sector.	CRAMM, ISO 27002
MSAT	Assessment qualitative risks. The main indicators of the risk profile. Allows you to evaluate the effectiveness of investment in the information security system.	ISO/IEC 27002, FRAP
OCTAVE	The methodology does not provide a quantitative assessment of risks, it easy to use, and is acceptable for organizations with different specifics of their activities. The average amount of input data is used for the analysis.	OCTAVE
RiskWatch	The methods uses quantitative and qualitative risk assessment, is easy to use, very flexible. The analysis of information security risk doed not take into account administrative and organizational factors, and these factors have a significant impact on organizations.	ISO 27002
CORAS	The software is distributed free of charge, does not require significant resources for installation and use. The technique is easy to use and does not reqiure special knowledge. The disadvantage of the methodology is	CORAS

	that the frequency of risk assessment is not provided.	

TABLE II. COMPARISON OF SOFTWARE TOOLS FOR INFORMATION SECURITY RISK MANAGEMENT

Comparison criteria	**CRAMM**	**ГРИФ**	**RiskWatch**	**CORAS**	**MSAT**
Risks					
Using risk categories	+	+	+	+	+
Using the concept of maximum permissible risk	+	+	+	+	+
Risk reduction, preparation of analysis action plan	+	+	+	–	+
Management					
Notification of the manager	+	+	+	+	+
Risk reduction work plan	–	+	+	–	+
Includings seminars, trainings, meetings	–	+	+	–	+
Business risk/operaional risk assessment	–	+	+	+	–
Risk assessment at the organizational level	+	+	–	+	+
Risk assessment at the technical level	+	+	+	+	+
Recommended ways to reduce risks					
Risk avoidance	–	+	+	–	–
Risk reduction	+	+	+	+	+
Risk taking	–	+	–	+	+
Processes					
Tangible assets	+	+	+	+	+
Intangible assets	+	+	+	+	+
Dangers	+	+	+	+	+
Asset value	+	+	+	+	+
Vulnerabilities	+	+	+	+	+
Security measures	+	+	+	–	+
Possible damage	+	+	+	+	+
Probability of threat implementation	+	+	+	+	+
Considered types of risk					
Business risks	–	+	+	+	–
Risks associated with violation of legislative acts	–	+	–	–	+
Risks associated with the use of technologies	–	+	–	+	+
Commercial risk	+	+	+	+	+
Risks associated with third parties	+	+	+	+	+
Employee risk	+	+	–	+	+
Ways to measure risk					
Qualitative assessment	+	+	+	+	+
Quantitative assessment	–	+	+	–	–
Management methods					
Qualitive differentiation of risks	+	+	+	+	+
Quantitative differentiation of risks	+	+	+	+	+
Using analysis independent assessment	–	+	–	+	+
Calculation of return on investment	–	+	–	–	–
Calculation of the optimal balance between different types of security measures					
Preventive measures	–	+	+	–	+
Measures to identify	–	+	+	–	+
Adjustment measures	–	+	+	–	+
Recovery	–	+	+	–	+
Integration og management methods	–	+	–	–	–
Description of the purpose of management methods	–	+	+	+	+
Procedure for taking residual risks	+	+	–	–	+
Residual risk management	–	+	–	–	+
Risk monitoring					
Application of monitoring the effectiveness of information security measured	–	+	+	–	–
Implementation of measures to reduce risks	–	+	+	–	+
Using the process of responding to incidents in the field of information security	–	+	–	–	+
Structural documentation of risk assessment results	–	+	+	–	+

Summarizing the analysis, the methods considered correspond well to the criteria of the “risks” and “processes” (use of risk element) groups, but some of them (CRAMM, CORAS) have disadvantages in accordance with the “monitoring” and “management” sections, as well as the “processes” section. Not all methods (ГРИФ, RiskWatch, MSAT) provide comprehensive recommendations for drawing up a schedule of risk assessment. It is advisable to use the CORAS methodology in cases where it is necessary to perform only a one-time assessment of the risk level in a medium-sized company.

The best CRAMM for risk management based on periodic assessment at the technical level. CRAMM, FRAP, RiskWatch, MSAT have shown the need for highly qualified specialists to use techniques (CRAMM, FRAP, ГРИФ) and the difficulties of application depending on the complexity and duration of the risk assessment process (MSAT) [5]. In addition, it should be noted the high cost of the software product (RiskWatch). It is suitable for use in large companies that manage information security risks based on regular assessment of MSAT and RiskWatch techniques and requite a proper risk mitigation plan [6].

METHODOLOGY OF RISK ASSESSMENT AND INFORMATION SECURITY RISKS

To assess information risk in accordance with the “Threat and vulnerability analysis model”, it is necessary to analyze all threats affecting the information systems and the vulnerabilities that they can implement.

Based on the data entered by the owner of the information systems, it is possible to build a model of current threats and vulnerabilities for the company’s information system. Based on the obtained model, analysis of the probability of information security threats for each resource is carried out and risks are calculated in this regard [7].

There are two modes of operation of the algorithm: (1) one main danger, (2) three main danger.

Information security risk analysis is carried out by building a model of analysis organization’s information systems.

The owner of the information system must first describe the architecture of his network [8]:

- all recourses on which valuable information is stored (server, workstation, mobile computer, etc.);
- recourse significance- the degree of significance of the recourse for the information systems, i.e. the degree to which the recourse affects the

functioning of the information systems in the implementation of information security threats.

- risks affecting resources;
- vulnerabilities in which threats are carried out;
- the probability of the threats being implemented through this vulnerability;
- the importance of implementing the threat through this vulnerability.

To assess the risk, all the risks affecting the information systems and the vulnerabilities with which these threats are carried out analyzed, and, as a result, risks are taken into account [9].

THE PRINCIPLE OF OPERATION OF THE RISK CALCULATION ALGORITHM:

At the first stage, according to the equation (1), the level of danger is calculated based on the significance and probability of the threat being realized through this vulnerability.

The level of threats shows how much this risk affects the resources, taking into account the probability of its implementation [11]:

$$Th = \frac{ER}{100} \cdot \frac{P(V)}{100} \quad (1)$$

ER is the significance of the threat implementation as a percentage, i.e. it shows how much the threat implementation affects the operation of the resource.

It may consist in the importance of implementing a threat on confidentiality, integrity and accessibility (ER_c, ER_i, ER_a) ; PV - the probability that the threat, expressed as a percentage, will be implemented through this vulnerability within a year.

Equation (2) is used to calculate the risk level for all vulnerabilities with which this threat can be carried out on the resource:

$$CTh = 1 - \prod_{i=1}^{n} (1 - Th_i) \quad (2)$$

Th is the vulnerability risk level. The risk level values for all vulnerabilities are taken in range from 0 to 1.

The total risk level for the resource $CThR$ (taking into account all risks affecting the resource) is calculated according to the equation (3):

$$CThR = 1 - \prod_{i=1}^{n} (1 - CTh_i) \quad (3)$$

CTh is the risk level from all vulnerabilities. The value of the general level of risks is taken in the range from 0 to 1.

Resource risk is calculated according to equation (4):

$$R = CThR \cdot D \quad (4)$$

D is the value of the resource in monetary terms or as a percentage; $CThR$ the overall risk level of the resource. The unit of measurement (% or type of money and currency) is set in the project settings. When transferring risks at levels, the number of levels and the assessment of levels are given on the project settings level sheet. The data is presented in Table 3.

TABLE III. UNITS OF MEASUREMENT LEVELS

Name of level	Level assessment (%)
1	33,33
2	66,66
3	100

The significance of the resource in the event of a threat to availability (refusal to provide a service):

$$D_y = D_h \cdot T_{\max} \quad (5)$$

D_y is the significance of the resource in terms of access risk per year; D_h - the importance of a resource on the risk of access to the clock; $T_{\max}$ - maximum downtime of resources per year (very important work time for the organization).

The risk value for each of the resource in the mode with three main threats and total risk value for the three risks are determined in monetary terms or by level by the following expression:

$$R_a = CThR_a \cdot D_a;\ R_c = CThR_c \cdot D_c;\ R_i = CThR_i \cdot D_i; \quad (6)$$

$$R_{\sum} = \left(1 - \left(\left(1 - \frac{R_c}{100}\right) \cdot \left(1 - \frac{R_i}{100}\right) \cdot \left(1 - \frac{R_a}{100}\right)\right)\right) \cdot 100 \quad (7)$$

We consider the risk of the information systems in monetary terms or for the mode of operation at the levels and for the mode of operation with three risks.

For the mode of operation with one main product in monetary terms or at levels:

$$CR = \sum_{i=1}^{n} R_i, \quad CR = \left(1 - \prod_{i=1}^{n} \left(1 - \frac{R_i}{100}\right)\right) \cdot 100 \quad (8)$$

For the mode of operation for three risks in monetary terms or at the levels:

$$CR_{a,c,i} = \sum_{i=1}^{n} R_i;$$

$$CR_{a,i,c} = \left(1 - \prod_{j=1}^{n} \left(1 - \frac{R_i}{100}\right)\right) \cdot 100;$$

$$CR_{\sum} = CR_c + CR_i + CR_a; \quad (9)$$

$$CR_{\sum} = \left(1 - \left(\left(1 - \frac{CR_c}{100}\right) \cdot \left(1 - \frac{CR_i}{100}\right) \cdot \left(1 - \frac{CR_a}{100}\right)\right)\right) \cdot 100 \quad (10)$$

The user can take countermeasures. To calculate the effectiveness off the introduced countermeasures, it is necessary to consistently follow the algorithm taking into account the specified countermeasures. That is, as a result the user receives two risk value before the adoption of countermeasures R_{old} and the risk value after the

adoption of countermeasures R_{new}. The effectiveness of the implementation of countermeasures is calculated by the equation:

$$E = \frac{R_{old} - R_{new}}{R_{old}} \quad (11)$$

Based on the application of this algorithms, the probability of threat realization and the significance of threat realization through vulnerability are obtained [10].

II. CONCLUSION

The article discusses the "Threat and vulnerability analysis model" related to information security. To use of this method allows avoiding unnecessary costs for security measures arising from subjective risk assessment, planning and implementing protection at all stages of the life cycle of information systems, as well as ensuring the execution of work in the shortest possible time.

Currently, the existing methods and software tools for assessing risks and threats are fully described, as a result of the analysis of advantages and disadvantages, conclusions are drawn indicating optimal solutions. Based on this conclusion, it is planned to create a software application in the future, which will be complied on the basis of the model specified in this paper.

REFERENCES

[1] S. Taubenberger, J. Jürjens, Y. Yu, and B. Nuseibeh, "Resolving vulnerability identification errors using security requirements on business process models," Information Management & Computer Security, vol. 21 No. 3, pp. 202-223, 2013.

[2] P. Shamala, R. Ahmad, A.H. Zolait, and S. bin Sahib, "Collective information structure model for Information Security Risk Assessment (ISRA)," Journal of Systems and Information Technology, vol. 17 No. 2, pp. 193-219, 2015.

[3] YU. O. Gubareva "CRAMM methodology used for risk analysis in the field of information security" (Методика CRAMM применяемая для анализа рисков в сфере информационной безопасности), Tezisy dokladov XIX Rossijskoj nauchnoj konferencii professorsko-prepodavatel'skogo sostava, nauchnyh sotrudnikov i aspirantov, 51-64, 2017. (In Russian)

[4] P. Shedden, R. Scheepers, W. Smith, and A. Ahmad, "Incorporating a knowledge perspective into security risk assessments," VINE, vol. 41 No. 2, pp. 152-166, 2011.

[5] S, V. Razumnikov "Analysis of the possibility of using OCTAVE, RISKWATCH, CRAMM methods to assess IT risks for cloud services" (Анализ возможности применения методов OCTAVE, RISKWATCH, CRAMM для оценки рисков ИТ для облачных сервисов), Molodoj uchenyj, 247-256, 2018. (In Russian)

[6] P. V. Pletnyov, V. M. Belov, "Comparative analysis of existing methods for determining information security risks" (Сравнительный анализ существующих методов определения рисков информационной безопасности), Polzunovskij vestnik, №3/1, 221-223, 2015.

[7] S. C. Misra, V. Kumar, and U. Kumar, "A strategic modeling technique for information security risk assessment," Information Management & Computer Security, vol. 15 No. 1, pp. 64-77, 2007.

[8] O. YU. Gubareva "Assessment of information security risks in telecommunication networks" (Оценка рисков информационной безопасности в телекоммуникационных сетях), Vestnik Volzhskogo universiteta imeni Tatishcheva V.N. Seriya Informatika, №2, 76-81, 2014. (In Russian)

[9] E. K. Baranova "Methods and software for risk assessment in the field of information security" (Методики и программное обеспечение для оценки рисков в сфере информационной безопасности), Upravlenie riskom, № 1 (49), 15-26, 2015. (In Russian)

[10] S. Fenz, J. Heurix, T. Neubauer, and F. Pechstein, "Current challenges in information security risk management," Information Management & Computer Security, vol. 22 No. 5, pp. 410-430, 2014.

[11] V. V. Pugin, YU. O. "RISK WATCH methodology used for risk analysis in the field of information security" (Методика RISK WATCH применяемая для анализа рисков в сфере информационной безопасности), Tezisy dokladov XIX Rossijskoj nauchnoj konferencii professorsko-prepodavatel'skogo sostava, nauchnyh sotrudnikov i aspirantov, 42-44, 2017. (In Russian)