DOI: https://doi.org/10.5281/zenodo.11651059

ANALYSIS OF RISK ASSESSMENT METHODS

Kholimtaeva I.U
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
Tashkent, Uzbekistan
darslar@gmail.com

Shamshieva B.M
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
Tashkent, Uzbekistan
nuiddinjabbarov2606@gmail.com

Abstract: *Information risks are related to the creation, processing, transmission, storage and use of information using electronic carriers and other means of communication. Prevention of information risks allows to ensure data integrity, confidentiality.*

Risk analysis consists of identifying existing risks and assessing their size (quality or quantity). The risk analysis process can be divided into several sequential steps:

• Identify the main IT resources;

• Determining the importance of certain resources for the organization;

• Identify existing security threats and vulnerabilities that allow threats to be implemented;

• Identification of risks associated with the implementation of a security threat.

Keywords: *Information, risk, low, high, assessment method, medium, PHA, SWIFT, RCA, RHA.*

INTRODUCTION

In building an organizations IS security system, the organizations IS control and audit processes are important for managing IS risk assessment processes, implementing and applying protective measures, training employees on information security, and other important processes. The timeliness, accuracy and completeness of the IS assessment obtained as a result of IS control and inspection allows to identify the weaknesses of the organizations IS provision system, identify unassessed risks, determine corrective and warning measures aimed at improving the organizations IS provision processes.

MATERIAL AND METHODS

There are different methods of risk assessment: economic, mathematical-statistical, expert assessment method, combined (in which all three methods, mathematical-statistical, expert assessment or expert assessment method and economic methods are combined).

However, there are two main approaches to risk assessment:

- The qualitative approach allows to determine and identify possible types of risks inherent in the information object, as well as to determine and describe the causes and factors affecting the level of this type of risk. In addition, the qualitative analysis includes the description of the possible damage caused by the occurrence of risks, its value and measures to reduce or prevent the risk. When using a qualitative approach, it is not necessary to determine the exact financial indicators of the value of assets, expected losses and the cost of management and control tools. Instead, relative costs are calculated.

- Quantitative approach to risk assessment includes numerical determination of the value of individual risks and integrated assessment of risk in general. Quantitative analysis is based on probability theory, mathematical statistics, operations research theory.

- Common methods of risk assessment can be considered. Checklists are a simple form of hazard identification that provide the user with a list of sources of uncertainty to consider. Users use previously developed list, codes (set of rules) and standards.

- Preliminary hazard analysis (PHA) is a simple inductive analysis method, the purpose of which is to identify risks, dangerous situations and events that can damage the organization's operations, equipment or systems.

- Structured Interviewing and Brainstorming - A way to get a set of ideas and ratings. Brainstorming can be encouraged by using one-on-one or one-on-one discussion techniques.

- The Delphi method is a method for obtaining expert opinion to identify sources and impacts of hazards, determine probabilities and consequences, and assist in overall risk assessment. This method of summarizing the opinions of experts allows independent analysis and voting of experts.

- "What if?" scenario analysis using the method (SWIFT) - A system that helps a group of experts identify a risk. Usually used in small gatherings. Used in conjunction with risk analysis and assessment methods.

- Human Factors Analysis (HRA) is a method of studying the impact of human factors on a system and evaluating human errors that affect system performance.

- Root Cause Analysis (RCA) is a method of analyzing losses that have occurred to determine their causes and find ways to improve a system or process to prevent similar losses in the future. The review process should examine management practices in place at the time of the loss and opportunities for management improvement.

- Scenario analysis - A method of studying and determining possible scenarios of the development of events by expressing or extrapolating known hazardous events and risk, each of these scenarios may occur. The method can be used formally or informally, and the analysis can be qualitative or quantitative.

- Toxicological risk assessment is a method of identifying and analyzing hazards and their possible pathways, providing information on the extent and harm of environmental exposure and is useful in assessing the likelihood of such harm.

- Business impact analysis (BIA) - The method allows you to analyze the risk of disruption (destruction) of the main activity of the organization and determine the opportunities for managing these disruptions (destruction).

- Fault tree analysis (FTA) - in which a system failure (main event) is identified, and then the paths of its occurrence are determined, which are graphically depicted in the form of a logical tree diagram. A fault tree explores ways to reduce or eliminate possible causes/sources of a failure.

- Event Tree Analysis (ETA) - A method that uses inductive reasoning to estimate the probability of events occurring and transitions to other events.

- Cause and effect analysis is a technique that combines fault tree and event tree techniques to account for latency. Within the framework of the method, the causes and consequences of the incident can be investigated.

- Causal Analysis – An impact can have multiple influencing factors that can be grouped into different categories. Influence factors are often identified during brainstorming and displayed as a tree structure or herringbone.

- Hazard analysis and critical control points (HACCP) - a system of preventive actions aimed at ensuring product quality, reliability and process safety based on the application of observation and measurement of specific characteristics that must be within specified limits (critical control points).

- Level of Protection Analysis (LOPA) - The method allows you to evaluate the control elements and their effectiveness. (The method is called barrier analysis.).

- Markov Analysis - Markov analysis is sometimes called state analysis and is commonly used to analyze complex renewable systems that may exist in various states, including a degraded state. Monte Carlo Simulation - Monte Carlo simulation is used to determine system changes as a result of changes in system inputs, given the distribution of inputs and their relationship to outputs. Analysis can be applied to a model that identifies the relationship between input and output data. Input data can be described as random variables with associated distributions and inherent uncertainty. Triangular or beta distributions are commonly used to estimate risk.

- Baesian Analysis and Baesian Networks - A statistical procedure that uses a prior distribution of data to estimate the probability of outcomes. The accuracy of the results of Bayesian analysis depends on the correctness of the prior distribution. A Bayesian network models causal relationships based on the analysis of probabilistic relationships between inputs and outputs.

- For the comparative assessment of the application of the methods, two aspects of the effect are given - the main factors, features and characteristics of the methods, as well as the possibility and efficiency of their use for different stages of evaluation. To further rank the methods on each factor, each method was assigned a factor level: high, medium, or low.

Table 1.

Comparative table of risk assessment methods by criteria

Name	Factors influencing the choice of risk assessment methods					Features of the application of the method at the stages of risk assessment			
	Necessary resources and opportunities	Uncertainty	The difficulty of the method	Quantitative output	Risk identification	Analysis of risk consequences	Probability of values	Risk level	Comparative assessment of risk
Watchlists	Low	Low	Low	No	Yes	No	No	No	No
PHA	Low	Low	Medium	No	Yes	No	No	No	No
Structured interviewing and brainstorming	Low	Low	Low	No	Yes	No	No	No	No
Delphi method	Medium	Medium	Medium	No	Yes	No	No	No	No
SWIFT	Medium	Medium	Various	No	Yes	Yes	Yes	Yes	Yes
HRA	Medium	Medium	Medium	Yes	Yes	Yes	Yes	Yes	It is possible
PCA	Medium	Low	Medium	No	No	Yes	Yes	Yes	Yes
Scenario analysis	Medium	High	Medium	No	Yes	Yes	It is possible	It is possible	It is possible
Toxicological risk	High	High	Medium	Yes	Yes	Yes	Yes	Yes	Yes
BIA	Medium	Medium	Medium	No	It is possible	Yes	It is possible	It is possible	It is possible
FTA	High	High	Medium	Yes	It is possible	No	Yes	It is possible	It is possible
ETA	Medium	Medium	Medium	Yes	It is possible	Yes	It is possible	It is possible	No
Causal Analysis	High	Medium	High	Yes	It is possible	Yes	Yes	It is possible	It is possible
Hazard analysis and critical control points	Low	Low	Medium	No	Yes	Yes	No	No	No
FMEC and FMECA	Medium	Medium	Medium	Yes	Yes	Yes	Yes	Yes	Yes
Reliability oriented maintenance	Medium	Medium	Medium	Yes	Yes	Yes	Yes	Yes	Yes
Analysis of latent defects	Medium	Medium	Medium	No	It is possible	No	No	No	No
HAZOP	Medium	High	High	No	Yes	Yes	It is possible	It is possible	It is possible
HACCP	Medium	Medium	Medium	No	Yes	Yes	No	No	Yes
LOPA	Medium	Medium	Medium	Yes	It is possible	Yes	It is possible	It is possible	No
Analysis of the neck	Medium	High	High	Yes	No	It is possible	Yes	Yes	It is possible
Markov analysis	High	Low	High	Yes	It is possible	Yes	No	No	No
Monte Carlo simulation	High	Low	High	Yes	No	No	No	No	Yes
Baesian analysis and Baesian networks	High	Low	High	Yes	No	Yes	No	No	Yes

CONCLUSION.

In addition, the second aspect of influence is the application of the method at a certain stage of risk assessment, for example, to assess the condition of dangerous objects.

Accordingly, the classification of methods is related to the stages of the risk assessment process:

- risk identification;
- analysis of the consequences of risk implementation;
- qualitative, mixed or quantitative assessment of possible risk indicators;
- assessment of the effectiveness of existing management tools;
- quantitative assessment of the level of risk;
- comparative risk assessment.

For each stage of the risk assessment process, the application of the risk assessment method is determined on a scale: strictly applied, applied and not applied (Table 2). 1 – 2 – analysis of the tables and taking into account the experts' score showed that the most effective methods are FMEA and FMECA, reliability-oriented maintenance, HRA, ETA, LOPA, SWIFT.

REFERENCES

1. P. Shamala, R. Ahmad, A. Zolait and M. Sedek, "Integrating information quality dimensions into information security risk management (ISRM)", Journal of Information Security and Applications, vol. 36, pp. 1-10, 2017. Available: 10.1016/j.jisa.2017.07.004.
2. A. Gupta, "Strategic Dimensions of Information Security Risk Management", Journal of Business Management and Information Systems, vol. 6, no. 2, pp. 1-9, 2019. Available: 10.48001/jbmis.2019.0602001.
3. Yevseiev, Serhii & Shmatko, Oleksandr & Romashchenko, Nataliia. (2019). Algorithm of information security risk assessment based on fuzzy-multiple approach. Advanced Information Systems. 3. 73-79. 10.20998/2522-9052.2019.2.13.
4. Wang Meng*, Zhou Shiyuan and Dong Zhankui. A Support Subset Algorithm and Its Application to Information Security Risk Assessment. Recent Patents on Engineering. Volume 11, Issue 3, 2017. Page: [188 - 193]. DOI: 10.2174/1872212111666170221164622.
5. Abhishek Sharma, Umesh Kumar Singh. Modelling of Smart Risk Assessment Approach for Cloud Computing Environment using AI & supervised machine-learning algorithms. Global Transitions Proceedings. 2022. ISSN 2666-285X, https://doi.org/10.1016/j.gltp.2022.03.030.

6. Olusola Akinrolabu, Jason R.C. Nurse, Andrew Martin, Steve New. Cyber risk assessment in cloud provider environments: Current models and future needs. Computers & Security. Volume 87. 2019. 101600. ISSN 0167-4048. https://doi.org/10.1016/j.cose.2019.101600.

7. Q. Hong et al., "An information security risk assessment algorithm based on risk propagation in energy internet," 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2), 2017, pp. 1-6, doi: 10.1109/EI2.2017.8245703.

8. Shameli-Sendi, A., Aghababaei-Barzegar, R. & Cheriet, M., Taxonomy of information security risk assessment (isra). Computers & Security, 57, pp. 14–30, 2016.http://dx.doi.org/10.1016/j.cose.2015.11.001.

9. "Information Security Risk Assessment- 7-Step Guide - CISO Portal", CISO Portal, 2022. [Online]. Available: https://www.ciso-portal.com/information-security-risk-assessment-7-step-guide/. [Accessed: 07- Jun- 2022].

10. "Performing an Information Security and Privacy Risk Assessment| Industry News | ISACA", ISACA, 2022. [Online]. Available: https://www.isaca.org/resources/news-and-trends/industry-news/2022/performing-an-information-security-and-privacy-risk-assessment. [Accessed: 07- Jun- 2022].