

THE MAIN APPROACHES TO EVALUATING THE EFFECTIVENESS OF APPLYING THE RISK ANALYSIS AND MANAGEMENT METHODOLOGY AT ENERGY COMPANY

DOI: 10.36724/2072-8735-2022-16-9-46-55

Manuscript received 26 July 2022;
Accepted 28 August 2022

Rahmani Jahed,
Moscow Technical University of Communication
and Informatics, Moscow, Russia,
jahed@mail.ru

Keywords: risk, performance evaluation,
risk management, analysis, probability, costs,
energy company of Iran

At present, it is difficult to imagine the provision of any global services without the introduction of information and communication technologies. The energy company of the Islamic Republic of Iran is territorially distributed, and without a corporate information and telecommunications network, it would cease to exist. In a geographically distributed company on 1,648,195 sq.km, there are several hundred access points and several thousand users of the corporate information and telecommunications network and, therefore, it is very important to understand the possible risks, their assessment and management. In such large geographically distributed corporate information and telecommunications networks with high load, for the use of big data, you need to have a complete picture of risks in order to develop risk models. Without a picture of possible risks, it is impossible to build scenarios for various negative and emergency situations. If we consider the probability of a negative event occurring in the corporate information and telecommunications network as a risk, then its definition, analysis and taking measures to minimize the negative consequences is called risk management. One of the main properties of the risks of a corporate information and telecommunications network is their uncertainty. A geographically distributed corporate network is highly exposed to external factors that can directly affect the quality of its functioning. The occurrence of such situations is difficult to predict.

Information about author:

Rahmani Jahed, Senior Lecturer of the Department "Networks Information Technologies and Services" Moscow Technical University of Communication and Informatics (MTUCI), Moscow, Russia

Для цитирования:

Рахмани Джахед. Основные подходы к оценке эффективности применения методологии анализа и управления рисками в энергетической компании // Т-Comm: Телекоммуникации и транспорт. 2022. Том 16. №9. С. 46-55.

For citation:

Рахмани Джахед (2022). Основные подходы к оценке эффективности применения методологии анализа и управления рисками в энергетической компании. *T-Comm*, vol. 16, no.9, pp. 46-55. (in Russian)

Introduction

The first works in which the problems of the emergence of economic risks were considered and which laid the foundation for the neoclassical theory of risk date back to the 1930s [1].

Risk is defined in a number of studies as the probability of loss or loss of benefits, uncertainty in obtaining the corresponding income [2].

Also, the risk is considered as a probability (threat) to lose part of one's resources, a shortfall in profits or the appearance of additional costs as a result of certain production and financial activities, probability of leakage of confidential information (including personal data), reputational losses [3-5].

There are also other interpretations of risk:

– risk – the uncertainty associated with the value of investments at the end of the period [6];

– risk – the possible danger of losses that arises under the influence of the specifics of certain natural phenomena and activities [1];

– risk defines an event that may or may not take place [7];

– risk is a threat, the danger of a loss, the danger of a potentially possible, probable loss of resources or a shortfall in income in comparison with an option designed for the rational use of resources in this type of activity [8];

– risk – the probability of an error or success of a choice in a situation with several alternatives [2];

– risk is a situational characteristic of activity, which consists of the uncertainty of the result in the possible adverse consequences in case of failure [9].

Thus, when determining risks, various bases are used, such as action, uncertainty, reliability, characteristic, but, in general, they all indicate a loss in the value of the object with which the risk is associated.

Risk classification

There is a basic classification of economic risks depending on the area in which the risks arise. The following types of financial risks for an enterprise are most often distinguished [6]: 1) price risk; 2) credit risk; 3) interest rate risk; 4) currency risk; 5) liquidity risk; 6) operational risk.

Price risk arises when the future price deviates from its expected value, and the deviation can be observed both for the worse and for the better. Thus, any deviation from the expected value is considered a manifestation of price risk. It should be noted that in the monograph the author [3] limits the definition of price risk only to situations with an unfavorable outcome, that is, we are talking about the risk of incurring losses.

Credit risk is the risk that arises when a debtor or counterparty fails to fulfill its obligations under an agreement in part or in full. Depending on the carriers of credit risk, there are:

– direct credit risk – direct and indirect lending agreements;

– settlement credit risk - agreements for the purchase / sale of assets without prepayment by the counterparty and settlement guarantees from third parties.

Figure 1 shows the features of business risk classification [1].

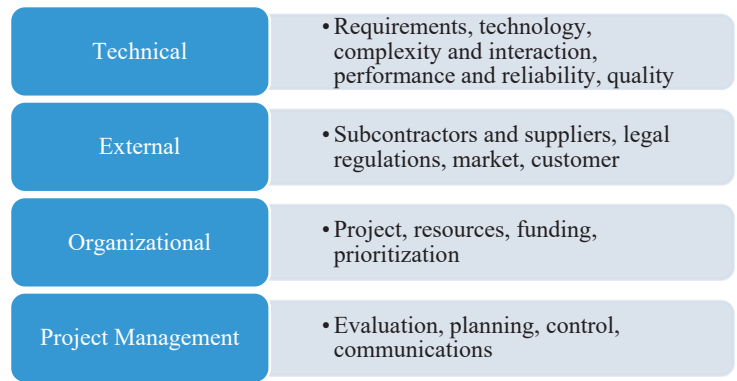


Figure 1. Classification of business risks

Business risks include risks arising both inside and outside the company, as well as commercial and scientific risks. Perhaps most importantly, adverse effects can include an organization's failure to optimize its assets (both tangible and intangible), which can result in the loss of the company's competitive advantage. Simply put, sound risk management can enable a company to make rational decisions in the face of powerful and dynamic forces shaping the global business environment [10].

The classification of risks associated with the introduction of modern information and communication technologies, cloud architecture and services, digital transformation at enterprises is given in [11-15].

In order to study the relationship between risk and uncertainty more thoroughly, it is necessary to consider the use of the terms risk and uncertainty from two points of view: description of the situation of risk/uncertainty; a description of the particular element of risk/uncertainty.

There are several main risk functions that have a positive impact on business development:

1. The analytical function of risk is expressed, respectively, in the analysis of the factors and conditions of the organization's activities. It contributes to the development of alternative solutions in a risky situation and allows you to choose the most correct course of action based on the calculations and analysis carried out. For example, the calculation of the possible damage and the probability of the realization of the risk refers to this function.

2. The regulatory function consists in the fact that the presence of a risk makes it necessary to make decisions taking into account its possible occurrence, that is, it is necessary to avoid or minimize risks throughout the entire activity. In essence, this means that the risk affects the decisions made by management, which means that we can talk about the application of a risk-based approach.

3. The protective function of risk is manifested in the fact that, in order to avoid damage and make a profit, the entrepreneur works in good faith, following the law and common sense. Thus, he protects himself from any sanctions both from the state and from other market participants, including his partners.

4. The innovative function of risk is manifested in the fact that the condition for the entrepreneur to search for non-traditional solutions and problems facing him is the possibility of risk and its negative consequences. This function indicates that the risk contributes to the use of new materials, technologies, raw materials and equipment, as well as the introduction of innovations in the production process in order to reduce costs and increase production volumes (services, works). It is the innovative function of risk

that stimulates entrepreneurs to improve the planning of activities, the production process and its management [6].

Risk assessment

Risk assessment is carried out using two main methods: qualitative and quantitative.

Qualitative risk analysis consists in assessing the factors influencing its magnitude using expert assessments. The accuracy of such estimates is reduced due to their subjectivity. Increasing the reliability of the results obtained is possible through the use of quantitative assessment methods. Quantitative analysis allows you to formalize the level of risk and express it in absolute and relative terms.

Quantitative risk assessment has a probabilistic (forecast) character, the calculation is based on statistical methods that rely on the size of losses in the past, and the value depends on the level of the accepted confidence level.

The degree of risk can be assessed in various ways, from complex probabilistic analysis to purely intuitive assumptions. Each of the methods is not without drawbacks, so in practice it is necessary to use combinations of different methods and combine formally economic and expert procedures. The choice of risk assessment method should be based on the available information and the desired end result.

The most common methods for assessing and analyzing risks and their comparative characteristics are proposed in Table 1.

Qualitative analysis is supplemented by quantitative risk assessment. Quantitative risk analysis - a numerical determination

of the magnitude of individual types of risks, as well as the total risk of the entire selected area of business activity.

Now managers usually rely on intuition, authority or experience of predecessors. Only a small percentage of managers are able to assess risk using economic and mathematical methods.

The most common and universal methods are cost feasibility, expert assessments, statistical, analytical and a number of others.

In world practice, the implementation of risk management is considered on the basis of a number of standards.

1. COSO proposes a study of existing risk assessment practices that are most useful in terms of the effectiveness of managerial decision-making. According to COSO ERM [6], the goal of risk management is to focus management on the largest threats and opportunities with the development of appropriate measures for these challenges.

The assessment algorithm includes the following steps: risk identification; development of evaluation criteria; risk assessment; assessment of the mutual influence of risks; risk prioritization; risk response.

Stage 1. The results of risk identification can be presented in the form of a list (list) of risks and opportunities, in particular, by groups (financial, operational, strategic), by subgroups (market, credit, liquidity risks), for business units or corporate functions and financial projects. It is the understanding of the nature of enterprise risks that forms the basis for building a risk portfolio at this stage. Each risk can affect management at the business unit level or functionally. The list of risks should be built in accordance with the priorities of key managers and the goals on which the attention of board members is focused.

Comparative characteristics of risk assessment and analysis methods

Table 1

Risk Assessment Method	Advantages	Disadvantages
Rating method of risk assessment	No need to analyze large datasets. Ranking of the received result on a certain scale is provided. Risk assessment can be carried out by a qualified economist, since the method uses elementary financial calculations	The problem of choosing a standard for comparison, the need for its differentiation for different areas of activity, which limits the conclusions about the level of risk and makes it impossible to develop universal recommendations
Expert assessment method	Allows you to detect the most significant risks and the average probability of their occurrence. Possibility of using this method in conditions of lack of information	Difficulty of application with a small number of evaluation indicators. Dependence on professionalism, experience, intuition of an expert. Subjectivism
Monte Carlo Method	The results show not only possible events, but also the probability of their occurrence. The data obtained allows you to create graphs of various consequences, as well as the likelihood of their occurrence. Allows you to see which inputs have the most impact on the final result	For estimates and conclusions, probabilistic characteristics are used, which is not convenient for direct practical application. Low accuracy of calculations (5-10%)
Decision Tree Method	Allows you to correlate subjective and objective assessments of possible actions, visibility	Labour intensive. It takes into account only those actions that the entrepreneur must intend to carry out, and does not take into account the influence of external factors on the activities of the enterprise
Statistical Method	Probabilistic risk assessment is mathematically sufficiently developed	The accuracy of calculations largely depends on the initial information, therefore, relying only on mathematical calculations in entrepreneurial activity is not always enough
Analytical Calculation	Allows you to model risky processes with high accuracy. It is used in case of instability of the operating conditions of the enterprise	Requires cumbersome calculations, development of economic and mathematical models for each level of risk

Stage 2. The development of evaluation priorities is the formation of a common set of criteria for application in the context of the work of business units, functions and capital investment projects. A typical assessment is to establish the credibility and extent of the impact. Many practitioners note the feasibility of risk assessment based on such additional dimensions as sensitivity and speed of response to changes.

Stage 3. Risk assessment consists of assigning a value to each risk and opportunity using certain criteria. Two stages - qualitative and quantitative consistently complement each other [16].

Stage 4. Assessing the interaction between risks. Risks do not exist in isolation from each other. Businesses must take into account the mutual influence of these risks and implement management of this influence. Even minor risks resulting from this interaction can cause significant harm or create a huge opportunity. As a result, enterprises tend to take an integrated or holistic view of risks using techniques such as the mutual influence matrix, aggregated probability distribution.

Stage 5 Risk prioritization is the process of prioritizing risk management by comparing the actual level of risk with the planned level and against a risk tolerance line. Risk is considered not only in terms of financial significance and credibility, but also in terms of subjective criteria of impact on safety and reputation.

Stage 6 Risk response. According to the results of the risk assessment, options for influencing them (acceptance, reduction, distribution, avoidance) are considered, a cost-benefit analysis is performed, a response strategy is formed and a plan is developed.

When developing evaluation criteria, we note that the traditional approach in the form of determining the reliability and significance is not perfect. It is common knowledge that low-probability events occur too often, and many high-probability events never occur. That is, these two criteria are not enough. It becomes useful to answer the question of how quickly the risk arises and how quickly it is necessary to respond or cover this risk, or how long one can remain tolerant. This is the answer that can be given by measuring the rate of occurrence of risk and its sensitivity. This information gives an understanding of the need for abrupt adaptation or the possibility of waiting.

The development of assessment scales is also important. Without setting a standard or norms, it is impossible to compare and identify the cumulative impact of risks on an organization. Most specialized scales for this purpose concern reliability and significance. They represent the ranking and fixation of measurements for further clear interpretation and use. The more detailed the scale is, the clearer the interpretation will be for users. The main purpose of compiling scales is to find a reasonable balance between convenience and completeness. Each organization has its own level of capitalization, size, industry specifics and culture, so the scales must be individualized [8].

2. Standard developed by the Federation of European Risk Management Associations "FERMA – Federation of European Risk Management Association" in conjunction with the "Risk Management Institute of Great Britain", "Risk Management and Insurance Association" and "National Forum of Risk Management in the Public Sector" and adopted in 2002. When developing this standard, a significant contribution was made by organizations that deal with risk management issues at a professional level [16].

This document contains basic definitions, explains internal and external risk factors, risk management processes, methodology and technology for risk assessment and analysis, general responsibilities of a risk manager. According to the FERMA standard, the duties of a risk specialist include: developing a risk management program; support for its implementation; coordination of cooperation between departments of the organization; creation of programs to reduce costs and activities to support the continuity of business processes. In the FERMA standard, developed by the European Federation of Risk Managers' Associations, risk management is a central part of the strategic management of an organization. This is a process by which an organization systematically analyzes the risks of each type of activity in order to maximize the effectiveness of each step and, accordingly, of the entire activity as a whole. Risk management must be incorporated into the general culture of the organization, accepted and approved by the management, and then communicated to each employee of the organization as a general development program with the setting of specific tasks on the ground.

3. One of the few legally approved standards in the field of risk management is the Sarbanes-Oxley Act. But even this law does not guarantee the success of actions and procedures. Companies need their own standard, which helps to draw up regulations and instructions that define: the principles of interaction between the structural divisions of the company in the field of risk management; clear distribution of functions, powers and responsibilities between the company's divisions in the field of risk management; control system and powers of controlling structural divisions; norms and requirements for operations that carry risk. The Sarbanes-Oxley Act is part of the US securities law [17].

One of the main goals of this law is to restore public confidence in corporate reporting. This law is aimed at reforming accounting, corporate governance and financial reporting in public joint stock companies. Its implementation is aimed at ensuring that shareholders, management, directors, regulators, creditors, investors and the market as a whole are confident in the reliability of published financial statements [17].

So, the analysis of the most well-known and widely used international standards, and practices, and risk management norms made it possible to identify the main differences in the structure of the elements of the risk management process. The main difference between the standards developed on a functional basis is that they are oriented, first of all, to the industry vision of the problems associated with risks, and do not detail the methodology, tools and risk management processes.

The advantages and disadvantages of risk management practices in an organization are presented in Table 2.

Thus, as part of the organization's risk management, various methods are used to minimize a risk event that help reduce the negative impact on the organization, the main of which are risk acceptance methods, risk transfer methods and risk avoidance. The choice of financial risk management methods depends on the specific organization, as well as on the type of its activity, development, chosen financial strategy and opportunities. However, it is worth remembering that these methods must be economically justified, and recommendations and measures should be aimed at minimizing financial risk and predetermining its occurrence [3]. Also, methods and approaches to risk assessment and management are discussed in [18-21].

Table 2

Advantages and disadvantages of risk management methods in an organization

Method of Financial Risk Management	Advantages	Disadvantages
Self-Insurance	Allows you to quickly recover the financial losses incurred by the organization	Freezes a fairly significant amount of financial resources, which reduces the efficiency of using equity and increases dependence on external sources of financing
Diversification	Allows you to minimize complex, portfolio financial risks of a non-systematic group	Does not give the desired effect in neutralizing the vast majority of systematic risks
Limitation	Doesn't cost much	Applicable only to risks that have gone beyond the acceptable level
Distribution of risk among participants	Allows you to shift part of the financial risks to partners	Applicable only if there are a sufficient number of partners
Risk avoidance	Allows you to completely eliminate a specific type of financial risk	Deprives the organization of additional sources of profit generation
Insurance	Applicable to any type of financial risk	Requires certain costs in the form of payment of remuneration to insurance companies
Hedging	Eliminates uncertainty and improves stability	Deprives the organization of probable bonus profit

To organize the interaction of the elements of the company's risk management system, it is necessary to have special accounting forms - a passport and a risk card, which allow you to track all changes in time. Approaches to understanding the essence of risk according to [7]: relationship between risk and hazard (risk refers to the possibility of an unfavorable event occurring); risk is understood as an activity performed in the hope of a successful outcome; risk is seen as a unity of circumstances.

To maintain financial stability and market position, companies need to adapt risk management in a crisis and provide businesses with effective tools for making decisions based on potential risks. It is important for company management to understand which risks may pose the greatest threat in the medium term, to which they need to prepare to respond now.

In order to make quick, but at the same time balanced decisions, it is necessary in commercial structures to take clear and effective measures [10] (Fig. 2).

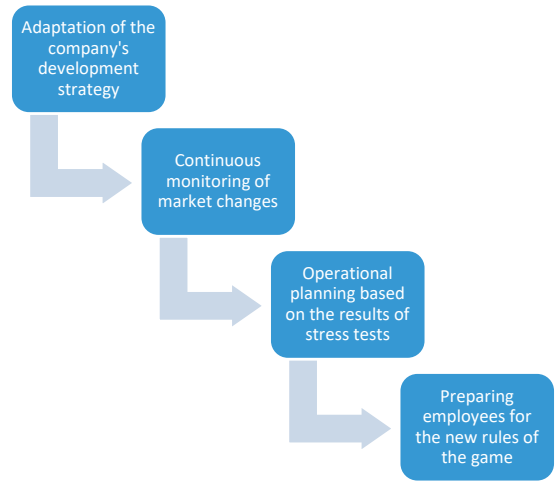


Figure 2. Measures aimed at adapting the company's risk management in conditions of high uncertainty

It should be noted that risk monitoring only makes it possible to register, accumulate and, if necessary, provide management personnel with information about various adverse facts, conditions and circumstances in a timely manner.

The choice of risk management method should be based on the content and specific features of the risk operation. For example, you can insure mainly statistical risks, but this method is not applicable for most financial risks. Liability and asset management is primarily applicable to the management of interest and financial risks, which is associated with changes in the company's balance sheet, which is not always acceptable.

In the modern world economy, the status of the leading trend is acquiring the process of globalization. There is an increase in international competition, an increase in the volume of international trade and capital movements, the development of information technology, the emergence of new financial instruments. All this entails an increase in risk and uncertainty.

Analysis and risk management in the Islamic Republic of Iran Energy Company

As for the Islamic Republic of Iran (IRI), in the era of the development and progress of science in various fields, almost all areas of activity are increasingly digitalized and automated, communication networks are being built to transmit data, both commercially and strategically significant [22]. As the problems of infrastructure, networks and users expand, more and more questions will be raised regarding the risks in data networks [23].

The main task is to achieve a balance between the best risk indicators and the optimal state of the geographically distributed information and communication network. Finding such a balance occurs in the process of complex iterations. Such a process is called risk management and solves the following tasks: choosing a management method, determining the type of risk, risk analysis, assessing the impact on the system, creating a scenario that is optimal for the system, monitoring the execution of the scenario and evaluating its effectiveness.

The purpose of these actions is to determine the likely risks, their qualitative and quantitative assessment. Here are the main risks that can occur and damage the company's information and communication network:

1. A hardware or software failure causing a violation of the integrity of the information and communication system, due to which the network performance suffers (technological risk).

2. Unauthorized access and penetration into the information and communication network and disruption of the system due to the hiring of non-staff specialists (information security risk). Since the beginning of the sanctions against Iran, the trends in the growth of technological progress have slowed down very much. There are not always enough full-time specialists of a narrow focus.

3. Risk of system disruption due to non-compliance with regulations and federal laws (political risk).

4. Risk of system failure due to human error (human factor risk).

5. The risk of disruption of the information and communication network due to external failures of infrastructure networks (infrastructure risks) [24-26].

6. The risk of loss of communication between remote small objects with the information and communication network due to the instability of communication in 2G and 3G networks. A number of remote small objects and stations, due to their small size relative to the general network, as well as their remoteness in hard-to-reach geographical areas, use the mobile network for data transmission.

7. Risk of data leakage due to the participation of foreign companies in the reconstruction of infrastructure data networks.

8. The risk of a collapse of the payment system. After sanctions were imposed on Iran, access to the swift payment system was closed. After that, the Iranian National Bank introduced its own payment system. Because of its imperfection, there is always the risk of its collapse.

9. Risks of communication loss in seismically active areas, also in areas with frequent dust storms. Due to these natural phenomena on the territory of Iran, there is a high risk of loss of radio communications or even destruction of equipment and communication channels due to equipment failure.

10. Risk of martial law. For the past four decades, Iran has been constantly under pressure from the United States and its allies. There have been repeated threats of martial law.

11. Risk of life threatening due to non-compliance with safety regulations.

12. Big data risks [27].

In the IRI energy company, there are many subsystems that are part of the corporate information and communication network, each of which has its own specific risks. For example, consider several basic subsystems.

Compilation and output of accurate, up-to-date statistical reports to relevant organizations is one of the most important operational needs of the electric power industry. Given that industrial energy is a strategic, vital and infrastructural industry, its reports are of great importance. Therefore, the power system reporting system can design and generate various reports. These reports can be a generalized parametric report with several and different parameters, or arbitrary reports created based on the proposed model.

Global risks in such a subsystem are obvious. The main risk is a violation of the completeness of the data. Due to outdated

equipment at a remote small control station, a number of errors associated with the operation of the equipment are not recorded. Poor system performance cannot keep up with all incoming error messages. Without fully registering all errors, there is no complete picture of what is happening at a given station. Without having a complete picture, it is impossible to make accurate decisions in managing and solving tasks.

Just as important is the risk of controlling access to information collection and reporting. The system of a fairly wide spectrum of action affects almost all the resources of the Iranian energy company. The different level of access is to protect high-level corporate sensitive data from ordinary operators.

Risks in an EPBS information system, like any information system, should be assessed for their relevance.

The electric power industry and its development play an indisputable role in the process of national infrastructure development, and therefore its long-term planning is of particular importance. One of the most important tools for planning and controlling the development of the electric power industry is the calculation of the level of production and consumption that will be maintained in the coming years, usually for ten or twenty years. The production system and energy balance system of the country is based on the above and is able to calculate the balance of production and consumption in four seasons for conditions of minimum, maximum and average load. In this system, calculations can be made based on rated power, practical power, or units. The calculation of this system can be done at the level of provinces, regional power supply, dispatcher level or the whole country, and various parameters such as the method of public or non-public funding, the accuracy of putting power units into the circuit, the availability factor, fixed storage, etc. can be used in calculation process.

Consider a number of technological risks that can directly affect the quality of information: the risk of data leakage, the risk of data loss, the risk of reducing the relevance of data, the risk of losing access, the risk of data completeness violation.

The causes of these risks and their possible damage are presented in Table 3.

Table 3

Causes of technological risks and their possible damage

Risk	Causes	Possible Damage
Risk of data leakage	Software failure, human error, hardware failure, use of unverified hardware	Commercial damage, financial costs of restoration
Risk of data loss	Software failure, human error, hardware failure, extreme weather events	Commercial damage, financial costs of restoration, company costs
Risks of decreasing the relevance of data	Insufficient processing power	Increased system response time, decreased data processing speed, commercial damage, financial costs of restoration, company costs
Risks of losing access	Software failure, human error, hardware failure	Loss of control over a system or node, business damage, financial cost of recovery, company costs
Risks of violation of completeness of data	Software failure, human error, hardware failure	Commercial damage, financial costs of restoration, costs

Qualitative and quantitative risk assessment methods can be used to assess risk. Each of which has its own characteristics. For example, for the quantitative method, statistical data on the risks that have occurred in the past are needed, and based on these data, a calculation is entered. And for quality, the basis is the assessment of specialists when testing and using the system, analyzing possible risks. The resulting numerical estimates of the impact of possible risks on the information and communication network can also be quantitative.

To quantitatively calculate the risk R for each of the found threats to the information and communication network, it is necessary to obtain by summing the product of the costs of the system S_i as a result of a detrimental situation on the information and communication network by the probability of realizing these situations P_i .

$$R = \sum_{i=1}^n S_i P_i, \text{ where } n - \text{number of critical situations.}$$

If there are no statistical data for risk assessment by a quantitative method, then the assessment is carried out by an expert method.

The following quantities are required for risk assessment: the probability of a threat; the likelihood of vulnerability; cost of loss.

Conclusion

Under the risk in the conditions of modern threats, it is proposed to understand the degree, the probability of deviation from the desired result as a system of indicators that deviate the actual result from the planned one and significantly affect the activities of a business entity both from the inside and from the outside.

In such large geographically distributed corporate information and communication networks with a high load, such as the IRI energy production company, in order to use big data, you need to have a complete picture of risks in order to develop risk management models.

One of the main properties of the risks of a corporate information and communication network is uncertainty. A geographically distributed corporate network is subject to external factors. The main task is to achieve a balance between the best risk indicators and the optimal state of the geographically distributed information and communication network.

At present, the integrated information system of the IRI energy company is used by many companies and organizations that are part of the energy company, including head offices such as the Ministry of Energy, Tavanir Management Company, Iranian Electricity Network Management Company, Thermal Energy Company, as well as all regional divisions and power plants in the whole country.

In a global system that links the entire corporate information and communication network of a company, the risks of intrusion from outside are not excluded. The risk may come from non-staff employees, as well as from imported foreign equipment. There are also human factor risks in data processing and management.

References

1. T. I. Gontarenko, N. V. Vashchenko (2020). Risk assessment of the QMS and certification procedures for the QMS of enterprises in the oil and gas industry. *II All-Russian Scientific and Technical Conference*

"Domestic and Foreign Experience in Quality Assurance in Mechanical Engineering", pp. 225-227.

2. V.A. Aksenova (2018). Risk Management in Organization Management. *Alley of Science*. Vol. 5. No. 4 (20), pp. 354-358.

3. E.I. Bashkintseva (2020). Risk assessment in the activities of the certification body. *Education and science in Russia and abroad*. No. 5 (69), pp. 254-258.

4. V.A. Dokuchaev, A.A. Kalfa, V.V. Maklachkova (2020). Architecture of Data Centers. Moscow: Hot Line-Telecom. 240 p. ISBN 978-5-9912-0849-9.

5. V.A. Dokuchaev (2020). Digital transformation: New drivers and new risks. *2020 International Conference on Engineering Management of Communication and Technology, EMCTECH 2020 - Proceedings*, Vienna, October 20-22. Vienna, 2020. P. 9261544. DOI 10.1109/EMCTECH49634.2020.9261544.

6. D.P. Baiderina, I.G. Shepelev (2019). Evaluation and management of investment portfolio. *Management of investments and innovations*. No. 2, pp. 23-29.

7. V.N. Bogatnikov, S.R. Bakasov, G.N. Sanaeva (2019). Management of the state of industrial technologies based on the risk criterion. *Software products and systems*. No. 4, pp. 725-734.

8. B.V. Bondarev, E.A. Tyukanko (2019). Improving the methods of optimal management of investment portfolios subject to risk limitation. *Bulletin of the Donetsk National University*. No. 4, pp. 13-22.

9. Ya.A. Vasilyeva (2020). Risk management: classification and methods of management. *Society: politics, economics, law*. No. 12 (89), pp. 106-110.

10. T.S. Artamonova, E.A. Sotskova (2019). Risk assessment of non-bank credit institutions. *Young scientists to the development of the national technological initiative (search)*. No. 1-1, pp. 265-266.

11. A.P. Simonov, V.A. Dokuchaev (2021). Risk analysis of cloud computing. *Promising technologies in the media: materials of the 14th international scientific and technical conference*, Vladimir, October 06-07. Vladimir: Vladimir State University named after Alexander Grigorievich and Nikolai Grigorievich Stoletov, pp. 344-347.

12. D.A. Petukhov, V.A. Dokuchaev (2021). Analysis of the quality indicators of cloud services in the world market. *REDS: Telecommunication devices and systems*. Vol. 11. No. 1, pp. 30-35.

13. V.V. Maklachkova, V.A. Dokuchaev, V.Y. Statev (2020). Risks identification in the exploitation of a geographically distributed cloud infrastructure for storing personal data. *2020 International Conference on Engineering Management of Communication and Technology, EMCTECH 2020 - Proceedings*, Vienna, October 20-22, p. 9261541. DOI 10.1109/EMCTECH49634.2020.9261541.

14. V.A. Dokuchaev, V.V. Maklachkova, V.Yu. Statev (2020). Classification of personal data security threats in information systems. *T-Comm*. Vol. 14. No 1, pp. 56-60. DOI 10.36724/2072-8735-2020-14-1-56-60.

15. V.A. Dokuchaev, E.V. Gorban, V.V. Maklachkova (2019). The System of Indicators for Risk Assessment in High-Loaded Infocommunication Systems. *2019 Systems of Signals Generating and Processing in the Field of on Board Communications, SOSG 2019*, Moscow, 20-21 March. P. 8706726. DOI 10.1109/SOSG.2019.8706726.

16. P.S. Zhernavkov (2019). Formalization of the process of organization of certification in railway transport. *Economics of railways*. No. 11, pp. 59-64.

17. O.G. Lapteva, N.V. Kiseleva (2021). Automation of the risk management process at oil and gas industry enterprises: analysis of automated risk management systems. *Bulletin of science and education*. No. 5-1 (108), pp. 5-13.

18. V.A. Dokuchaev, V.V. Maklachkova, S.V. Pavlov, S.S. Mytenkov (2021). Comparison of the Spectral and Hierarchy Analysis Methods Applicability for Technical Systems Choosing. *2021 Systems of Signals Generating and Processing in the Field of on Board Communications, Conference Proceedings*, Moscow, March 16-18. P. 9416017. DOI 10.1109/IEEECONF51389.2021.9416017.

19. L.V. Volkova, D.V. Makarova, V.A. Dokuchaev (2021). Using the CRAMM method to assess information risks. *Telecommunications and information technologies*. Vol. 8. No. 1, pp. 103-109.

20. V.A. Dokuchaev, V.V. Maklachkova, D.V. Makarova, L.V. Volkova (2020). Analysis of Data Risk Management Methods for Personal Data Information Systems. *2020 Systems of Signals Generating and Processing in the Field of on Board Communications*, Moscow, 19-20 March. P. 9078547. DOI 10.1109/IEEECONF48371.2020.9078547.

21. S.V. Pavlov, V.A. Dokuchaev, V.V. Maklachkova, S.S. Mytenkov (2019). Features of supporting decision making in modern enterprise infocommunication systems. *T-Comm*. Vol. 13. No 3, pp. 71-74. DOI 10.24411/2072-8735-2018-10252.

22. V.A. Dokuchaev, Rahmai Jahed (2020). Analysis of the Iranian legislative framework for working with personal data. *Actual problems and prospects for the development of the economy: Proceedings of the XIX All-Russian scientific and practical conference with international participation*, Simferopol-Gurzuf, October 15-17: IP Zueva T.V., pp. 27-28.

23. Rahmani Jahed, V.A. Dokuchaev (2020). Analysis of development trends in the communications industry in Iran. *Technologies of*

the Information Society: Proceedings of the XIV International Industry Scientific and Technical Conference, Moscow, March 18-19. Moscow: Media Publisher Publishing House LLC, pp. 300-301.

24. V. A. Dokuchaev, A. V. Shvedov (2020). Classification of reliability indicators of corporate digital platforms. *Actual problems and prospects for the development of the economy: Proceedings of the XIX All-Russian scientific and practical conference with international participation*, Simferopol-Gurzuf, October 15-17: IP Zueva T.V., pp. 28-29.

25. V.A. Dokuchaev, A.V. Shvedov (2012). Information security on corporate VoIP networks. *Elektrosvyaz*. No. 4, pp. 5-8.

26. N.S. Kalmykov, V.A. Dokuchaev (2020). Analysis of the main methods of ensuring network security in software-defined networks. *Telecommunication and computer systems 2020: Proceedings of the international scientific and technical conference*, Moscow, December 14-17. Moscow Technical University of Communications and Informatics. Moscow: Hot Line-Telecom, pp. 63-70.

27. V.Yu. Statev, V.A. Dokuchaev, V.V. Maklachkova (2022). Information security in the big data space. *T-Comm*. Vol. 16. No.4, pp. 21-28. (in Russian)

XI Ежегодный Форум "XI Telecom & Finance LOYALTY FORUM 2022"

Открыта регистрация на XI Ежегодный Форум "XI Telecom & Finance LOYALTY FORUM 2022", который пройдет 20 октября 2022 года в Москве. Участники могут зарегистрироваться на официальном сайте мероприятия.



В ходе мероприятия будет всесторонне рассмотрена проблематика гарантирования доходов и антифрода, в частности блоки:

- Бизнес и его инструменты при взаимодействии и в борьбе за клиентов, регулирование. трансформация в эпоху санкций;
- Роль сотрудников компании в реализации Customer Experience. "HR Loyalty";
- Аналитика и измерения. системы лояльности во взаимодействии с клиентами, отечественные идеи и решения.

Кроме того, запланирован ряд дискуссий:

- Перестройка моделей продаж, продуктовой линейки и сервисов, риск-моделей;
- Развитие внутренних инструментов для повышения эффективности привлечения и работы с клиентами;
- Возможности взаимодействия с клиентами – от традиционных к перспективным.

Форум объединит топ-менеджеров, руководителей и представителей ТЕЛЕКОММУНИКАЦИОННЫХ КОМПАНИЙ, БАНКОВ, СТРАХОВЫХ КОМПАНИЙ и др., представителей вендоров, поставщиков решений и услуг, представителей госорганов, руководителей отраслевых ассоциаций и СМИ.

ОСНОВНЫЕ ПОДХОДЫ К ОЦЕНКЕ ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ МЕТОДОЛОГИИ АНАЛИЗА И УПРАВЛЕНИЯ РИСКАМИ В ЭНЕРГЕТИЧЕСКОЙ КОМПАНИИ

Рахмани Джахед, МТУСИ, Москва, Россия, jahed@mail.ru

Аннотация

В настоящее время трудно представить предоставление каких-либо глобальных услуг без внедрения информационно-коммуникационных технологий. Энергетическая компания Исламской Республики Иран территориально распределенная, и без корпоративной информационно-телекоммуникационной сети перестала бы существовать. В территориально распределенной компании на 1 648 195 км² имеется несколько сотен точек доступа и несколько тысяч пользователей корпоративной информационно-телекоммуникационной сети и, следовательно, очень важно понимать возможные риски, их оценку и управление. В таких больших территориально распределенных корпоративных информационно-телекоммуникационных высоко нагруженных сетях для применения больших данных нужно иметь полную картину рисков, чтобы разрабатывать модели рисков. Не имея картины возможных рисков, невозможно строить сценарии на различные негативные и экстренные ситуации. Если считать риском вероятность возникновения негативного события в корпоративной информационно-телекоммуникационной сети, то его определение, анализ и принятие меры по минимизации негативного последствия называется управлением риском. Одним из основных свойств рисков корпоративной информационно-телекоммуникационной сети является их неопределенность. Территориально распределенная корпоративная сеть сильно подвержена воздействию внешних факторов, которые могут напрямую повлиять на качество её функционирования. Возникновение таких ситуации трудно предугадать.

Ключевые слова: риск, оценка эффективности, управление рисками, анализ, вероятность, расходы, энергетическая компания Ирана.

Литература

1. Гонтаренко Т.И., Ващенко Н.В. Оценка рисков СМК и процедуры сертификации СМК предприятий нефтегазовой отрасли // II Всероссийская научно-техническая конференция «Отечественный и зарубежный опыт обеспечения качества в машиностроении». 2020. С. 225-227.
2. Аксенова В.А. Управление рисками в управлении организацией // Аллея науки. 2018. Том 5. №4 (20). С. 354-358.
3. Башкинцева Е.И. Оценка риска в деятельности органа по сертификации // Образование и наука в России и за рубежом. 2020. № 5 (69). С. 254-258.
4. Докучаев В.А., Калфа А.А., Маклачкова В.В. Архитектура центров обработки данных. М.: Горячая линия – Телеком, 2020. С. 240. ISBN 978-5-9912-0849-9.
5. Докучаев В.А. Цифровая трансформация: новые драйверы и новые риски // 2020 International Conference on Engineering Management of Communication and Technology, EMCTECH 2020 - Proceedings, Vienna, October 20-22, 2020. Vienna. С. 9261544. DOI 10.1109/EMCTECH49634.2020.9261544
6. Байдерина Д.П., Шепелев И.Г. Оценка и управление инвестиционным портфелем // Управление инвестициями и инновациями. 2019. № 2. С. 23-29.
7. Богатииков В.Н., Бакасов С.Р., Санаева Г.Н. Управление состоянием промышленных технологий на основе критерия риска // Программные продукты и системы. 2019. № 4. С. 725-734.
8. Бондарев Б.В., Тюканко Е.А. Совершенствование методов оптимального управления инвестиционными портфелями с учетом ограничения риска // Вестник Донецкого национального университета. 2019. № 4. С. 13-22.
9. Васильева Я.А. Управление рисками: классификация и методы управления // Общество: политика, экономика, право. 2020. № 12 (89). С. 106-110.
10. Артамонова Т.С., Сотскова Е.А. Оценка рисков небанковских кредитных организаций // Молодые ученые к развитию национальной технологической инициативы (поиск). 2019. № 1-1. С. 265-266.
11. Симонов А.П., Докучаев В.А. Анализ рисков облачных вычислений // Перспективные технологии в СМТ: материалы 14-й международной научно-технической конференции, г. Владимир, 06–07 октября 2021 года. Владимир: Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, 2021. С. 344-347.
12. Петухов Д.А., Докучаев В.А. Анализ показателей качества облачных услуг на мировом рынке // REDS: Телекоммуникационные устройства и системы. 2021. Т. 11. № 1. С. 30-35.

13. *Maklachkova V.V., Dokuchaev V.A., Statev V.Y.* Risks identification in the exploitation of a geographically distributed cloud infrastructure for storing personal data // 2020 International Conference on Engineering Management of Communication and Technology, EMCTECH 2020 - Proceedings, Vienna, October 20-22, 2020. Vienna, 2020. P. 9261541. DOI 10.1109/EMCTECH49634.2020.9261541
14. *Докучаев В.А., Маклачкова В.В., Статев В.Ю.* Классификация угроз безопасности персональных данных в информационных системах // Т-Comm. 2020. Вып. 14. № 1. С. 56-60. DOI 10.36724/2072-8735-2020-14-1-56-60
15. *Докучаев В.А., Горбань Е.В., Маклачкова В.В.* Система показателей оценки риска в высоконагруженных инфокоммуникационных системах // 2019 Systems of Signals Generating and Processing in the Field of on Board Communications, SOSG 2019, Москва, 20-21 марта 2019. Москва, 2019. С. 8706726. DOI 10.1109/SOSG.2019.8706726
16. *Жерनावков П.С.* Формализация процесса организации сертификации на железнодорожном транспорте // Экономика железных дорог. 2019. № 11. С. 59-64.
17. *Лаптева О.Г., Киселева Н.В.* Автоматизация процесса управления рисками на предприятиях нефтегазовой отрасли: анализ автоматизированных систем управления рисками // Вестник науки и образования. 2021. № 5-1 (108). С. 5-13.
18. *Dokuchaev V.A., Maklachkova V.V., Pavlov S.V., Mytenkov S.S.* Comparison of the Spectral and Hierarchy Analysis Methods Applicability for Technical Systems Choosing // 2021 Systems of Signals Generating and Processing in the Field of on Board Communications, Conference Proceedings, Moscow, March 16-18, 2021. Moscow, 2021. P. 9416017. DOI 10.1109/IEEECONF51389.2021.9416017
19. *Волкова Л.В., Макарова Д.В., Докучаев В.А.* Использование метода CRAMM для оценки информационных рисков // Телекоммуникации и информационные технологии. 2021. Т. 8. № 1. С. 103-109.
20. *Dokuchaev V.A., Maklachkova V.V., Makarova D.V., Volkova L.V.* Analysis of Data Risk Management Methods for Personal Data Information Systems / // 2020 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, 19-20 March 2020. Moscow: Institute of Electrical and Electronics Engineers Inc., 2020. P. 9078547. DOI 10.1109/IEEECONF48371.2020.9078547
21. *Павлов С.В., Докучаев В.А., Маклачкова В.В., Мытенков С.С.* Особенности поддержки принятия решений в современных корпоративных инфокоммуникационных системах // Т-Comm: Телекоммуникации и транспорт. 2019. Вып. 13. № 3. С. 71-74. DOI 10.24411/2072-8735-2018-10252.
22. *Докучаев В.А., Рахман Джахед.* Анализ законодательной базы Ирана по работе с персональными данными // Актуальные проблемы и перспективы развития экономики: Материалы XIX Всероссийской научно-практической конференции с международным участием, Симферополь - Гурзуф, 15–17 октября 2020 г. Симферополь: ИП Зуева Т.В., 2020. С. 27-28.
23. *Рахмани Джахед, Докучаев В.А.* Анализ тенденций развития отрасли связи в Иране // Технологии информационного общества: Материалы XIV Международной отраслевой научно-технической конференции, Москва, 18–19 марта 2020. – Москва: Издательство «Медиа Паблишер». ООО «Дом», 2020. С. 300-301.
24. *Докучаев В.А., Шведов А.В.* Классификация показателей надежности корпоративных цифровых платформ // Актуальные проблемы и перспективы развития экономики: Материалы XIX Всероссийской научно-практической конференции с международным участием, Симферополь-Гурзуф, 15-17 октября 2020 г. Симферополь: ИП Зуева Т.В., 2020. С. 28-29.
25. *Докучаев В.А., Шведов А.В.* Информационная безопасность в корпоративных сетях VoIP // Электросвязь. 2012. № 4. С. 5-8.
26. *Калмыков Н.С., Докучаев В.А.* Анализ основных методов обеспечения сетевой безопасности в программно-конфигурируемых сетях // Телекоммуникационные и компьютерные системы 2020: Материалы международной научно-технической конференции, Москва, 14-17 декабря 2020 г. / Московский технический университет связи и информатики. М.: Горячая линия – Телеком», 2020. С. 63-70.
27. *Статев В.Ю., Докучаев В.А., Маклачкова В.В.* Информационная безопасность в пространстве больших данных. Т-Comm: Телекоммуникации и транспорт, 2022. Том. 16. №4. С. 21-28.

Информация об авторе:

Рахмани Джахед, старший преподаватель кафедры "Сетевые информационные технологии и сервисы" МТУСИ, Москва, Россия