A methodology for assessment and management of process-related risks

I.V. Abramov[1], V. Taratukhin[2], I.V. Illarionov[3]

[1] Voronezh State University, Voronezh, Russia
iva-dak.vrn@mail.ru
[2] University of Muenster, Muenster, Germany
victor.taratoukhine@sap.com
[3] Voronezh State University, Voronezh, Russia
igor.illarionov@gmail.com

Abstract The paper suggests a methodology of risk assessment based on the recommendations and requirements of ISO/IEC 31010 standard regarding the outer and inner parameters of a specific organisation. A System for Prevention and Management of Process-Related Risks (SPMR) is suggested. It helps to forecast and monitor the risks effectively. The system is based on the BI system workflow, which allows the Managers of the organisation to receive graphic information.

Keywords: risk management system, BI System, process-related risks.

1 Introduction

Heads of various organisations always face a range of risks and pay a lot of attention to risk management in decision-making process. The problem of risk management is therefore of great importance for IT developers. The need for information that would allow for timely risk management has led to the development of a new sphere - risk management. Experts working worldwide in various spheres of human activity managed to develop an internationally recognised risk management standard [1] (further referred to as ISO/IEC 31010).

The need to produce quality goods that would meet consumers' requirements resulted in the introduction of quality management systems (QMS) in organisations. The design and introduction of such systems, in turn, led to the development of quality standards. International standards for quality management systems were elaborated over time to meet the requirements of people. It therefore became necessary to assess and manage risks [2].

A specific feature of ISO/IEC 31010 is that it takes into account various criteria applicable to risk management. On the one hand, the standard recommends using clear and consistent risk assessment techniques. On the other hand, it also suggests the most effective risk assessment methods for enterprises. The standard provides a unified description of such methods, their specifics, strengths, and limitations. ISO/IEC 31010

ICID-2019 Conference

also lists the requirements to the risk assessment methods that must be met when designing a risk management system (RMS). According to the standard, RMSs must regard the following parameters: 1) applicability of the methods at various stages of risk assessment and 2) factors influencing the choice of the assessment methods.
The applicability of risk assessment methods (Table A) [1] is strictly determined as "strongly applicable" (SA), "applicable" (A), and "not applicable" (NA). Using this information, developers of a RMS can determine a range of risk assessment methods they should use when designing the system. However, the recommendations provided by the standard also determine a strictly limited set of risk assessment methods that can be employed in specific circumstances. This may result in the ambiguity of the results of the risk assessment process. It also and makes it much more difficult to design a RMS and causes confusion for the developers.
Taking into account the factors determining the selection of risk assessment techniques (Table B) [1], such as "Resources and Capabilities", "Uncertainty", and "Complexity", allows to evaluate their relevance as "Low", "Medium", and "High". ISO/IEC 31010 also provides information regarding the quantitative output of each technique. The necessity to account for the listed factors when selecting the assessment techniques results in the same ambiguity as the necessity to account for their applicability (Table A) [1]. This means that there are two overlapping uncertainties in selecting the assessment methods.
Another issue that should be regarded when selecting risk assessment methods is the fact that ISO/IEC 31010 also focuses on the level of expertise in various spheres. It should be noted that the standard is general in nature - it reflects good practices of selecting risk assessment techniques and provides guidance across various industries and types of organisations.
Corollary. In order to develop a functional RMS, the recommendations of ISO/IEC 31010 [1] should be adapted to the specific parameters of the organisation.
In this paper we suggest a methodology and a BI system for risk assessment and management that has the following benefits.

- On the development stage it is possible to:
  - select risk assessment methods suggested in ISO/IEC 31010 [1] regarding the specifics of a certain organisation;
  - create a risks register of a certain type;
  - generate a graphic representation of the risk level, both for individual risks and ranges of risks.
- On the production stage it is possible to:
  - evaluate the current values of various parameters of risks;
  - monitor the risks and create graphic representations of their level;
  - take risk prevention measures

2 Selection of risk assessment techniques

When designing a RMS, the developers should take into account the recommendations of ISO/IEC 31010 [1] as well as the inner parameters of the organisation where the RMS will be employed [3]. The suggested methodology of selection of risk assessment techniques is based on the analytic hierarchy process (AHP), heuristic logical actions of the experts, and the decisions of the decision maker. The following decision making algorithm is suggested (Fig. 1):

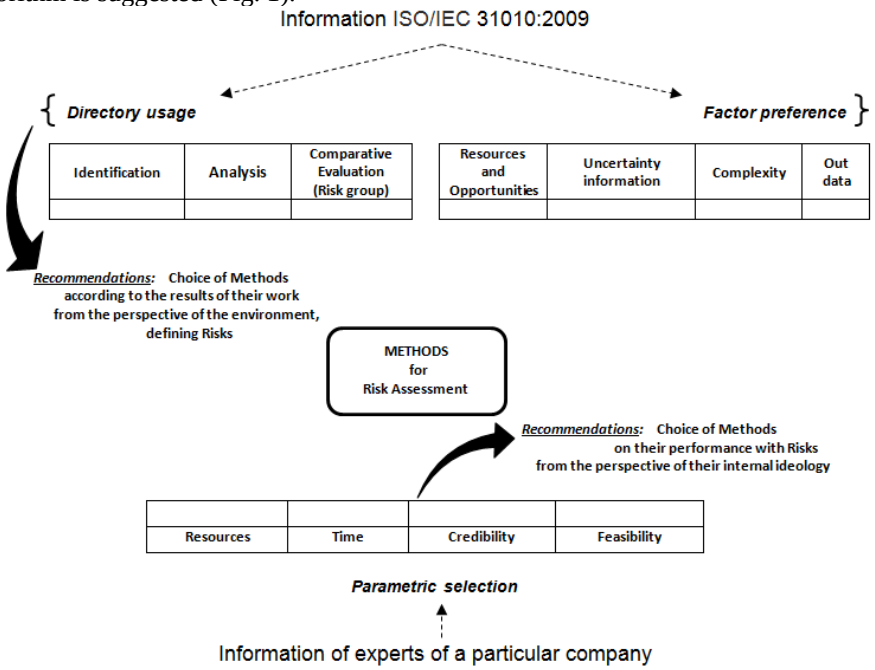


Fig. 1. Recommendations on selecting risk assessment techniques

Strengths and limitations of every risk assessment technique were analysed. At the first stage of the analysis we divided the assessment techniques into 20 groups based on their strengths and limitations. Each group includes techniques with equal characteristics. As a result we obtained two sets of groups (strengths / limitations) with each group including its own set of techniques. Some techniques can be included into several different groups [3]. Each group is ranked by the experts of the organisation, using the expert scale.

At the second stage, the criteria relevant for certain activities of the organisation are determined. and ranked by the organisation's experts. The criteria are universal, i.e. applicable to any group of risk assessment techniques.

As a result, we obtain a hierarchy where the top level is the target (selection of the best group of assessment techniques), the second level contains the criteria for the selection of groups of assessment techniques, and the third level contains the groups of assessment techniques.

The third stage includes selecting groups of techniques (alternatives) using the analytic hierarchy process (AHP).
The selection of risk assessment techniques is performed by means of VBA - a programming language used in Microsoft Excel. The selection process is demonstrated in Fig. 2.

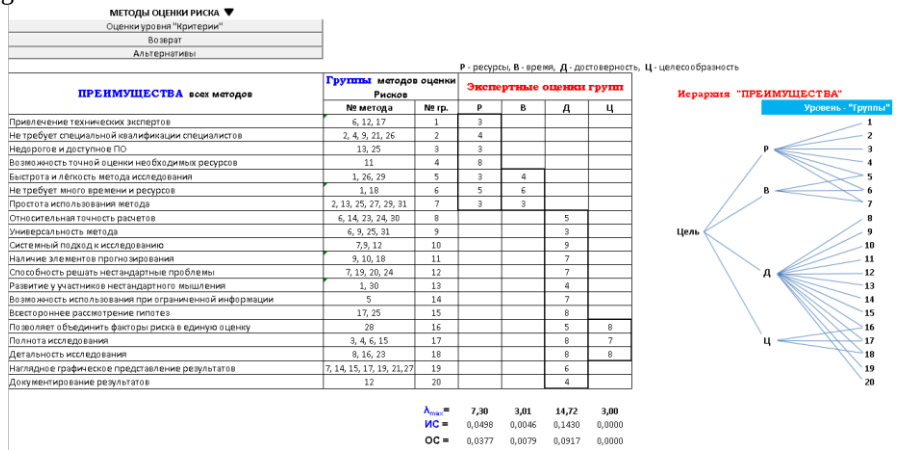


Fig. 2. Ranking of the groups based on the characteristic “STRENGHTS”

The selection process is demonstrated in Fig. 3.
The fourth stage includes graphic selection of risk assessment methods. The selection process is based on the relevance of the groups of methods of both sets.
The fifth stage includes the analysis of the selected techniques regarding the recommendations of ISO/IEC 31010 (Table A, B) [3].

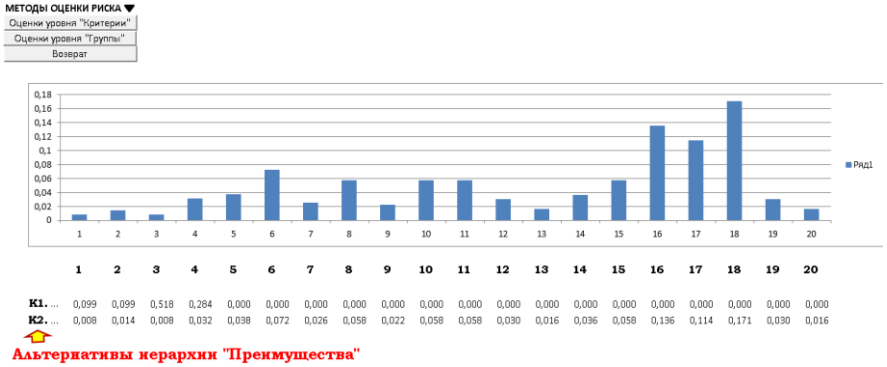


Fig. 3. Value of the alternatives - relevance of the strengths of the groups of risk assessment methods

If the results are not satisfactory, it is possible to repeat the above listed stages correcting the process of expert ranking, the criteria, and the sets of selected risk assessment methods.
Corollary. Development of a RMS includes the following.

- It is necessary and possible to take into account inner and outer parameters of the organisation when selecting risk assessment methods.
- Parameter-based selection process allows the developers to broaden or narrow the search area based on the relevance of the groups of methods.

The process of RMS design involves experts working at the organisation.
Risk assessment methods help to identify the risk, its category, level, and type, the probability of risk and its consequences.
The suggested programme for selecting risk assessment methods is a subsystem of the BI system "System for Prevention and Management of Process-Related Risks" (SPMR).

3 BI system SPMR - development stage

The development stage starts with "Risk Identification" [1]. The interface of the programme is demonstrated in Fig. 4. The ranking chart is generated step-by-step, and is thus completed with the data obtained during the "Risk Analysis" (P - probability of risk, I - impact, R - rank of the risk). Each element (P, I, R) of the BI system SPMR has its own graphic representation.

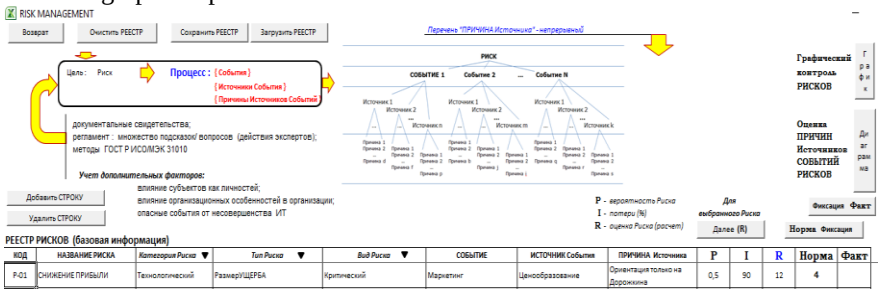


Fig. 4. Interface of the subsystem "Risk Identification"

The last part of the development stage is the "Comparative Analysis of Risks". Risks are first analysed separately with regard to the relevant areas. Then they are analysed all together with regard to a specific area (Fig. 5).

4 BI system SPMR - production stage

The system is operated by three groups of personnel.

- Administrators - members of the IT service. They develop the organisational structure of the system's users: lists if employees and their status, passwords, and directories of personal RISK REGISTERs.
- Status 1 employees - Managers / Executives who can work with subsystems of the risk assessment process and certain RISK REGISTERs.

- Status 2 employees - Managers who can work with subsystem “Risk Assessment METHODS”, subsystems of the risk assessment process, and certain RISK REGISTERs of executives.

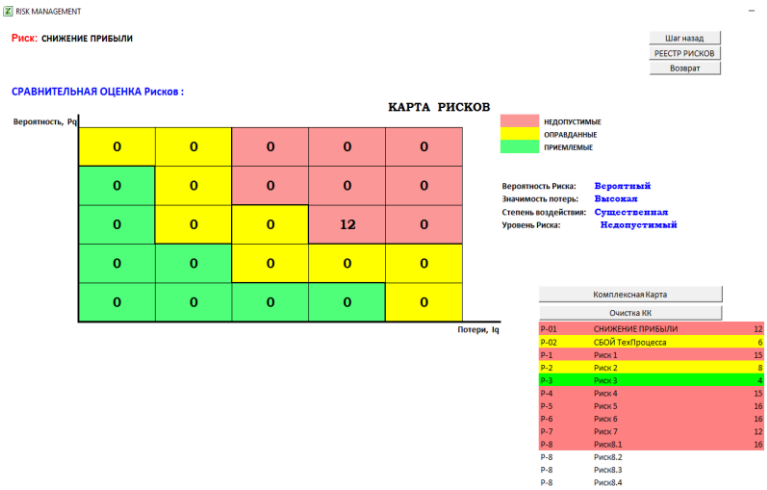
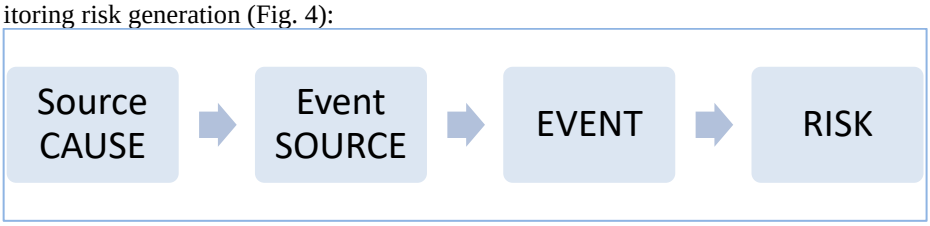


Fig. 5. A comprehensive map of the subsystem “Comparative Analysis of Risks”

To assess the dynamics of risks, the following parameters are used that allow for monitoring risk generation (Fig. 4):



The initial stage of risk occurrence is represented by the parameter “Source CAUSE”. Its value, as well as the set of such parameters corresponding to a certain parameter “Event SOURCE”, denote the moment when the source occurs. The set of parameters “Event SOURCE” denotes the moment when the parameter “EVENT” occurs. The set of parameters “EVENT” results in the occurrence of risk.

As the occurrence of risk has certain impact on the organisation, the parameter “Source CAUSE” is the key one. It allows to identify the initial stage of risk occurrence and take measures to eliminate the cause of risk. These actions correspond to Risk MITIGATION.

To implement this process within the BI system SPMR, the value of the parameter “Source CAUSE” is determined by experts. This value is shown in the column “Norm” of the Risk Register chart (Fig. 4). The BI system can also generate an .xlsx file, which is completed with the current data and the values of the parameter “Source CAUSE” imported in the column “Fact” of the Risk Register (Fig. 4).

The dynamic monitoring of risk probability is performed using the Risk Assessment Graph (Fig. 6).
This graph enables the Manager to see risk probabilities at a certain period of time.
When the Manager of the organisation makes a decision to take certain measures, the BI system locks the values of the parameters in the column “Source CAUSE” in the RISK REGISTER. These values correlate with the values in columns “Norm” and “Fact” and thus, when the value of the “Fact” exceeds the value of the “Norm” the cells of the column “Source CAUSE” are highlighted.
If all the cells of the column “Source CAUSE” corresponding to the parameter “Event SOURCE” are highlighted, the colour of this cell also changes.

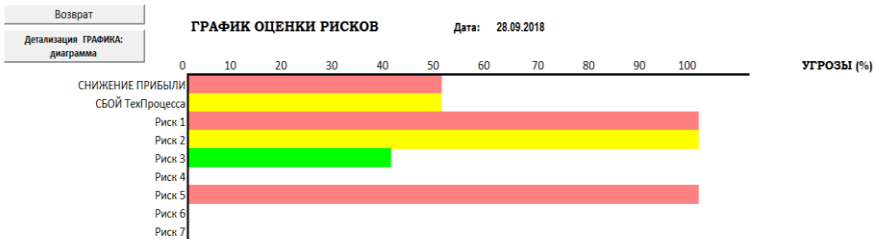


Fig. 6. Graphic monitoring of risks via the graph

The same algorithm is applied to the cells of the RISK REGISTER. If all the cells of the column “Event SOURCE” corresponding to the parameter “EVENT” are highlighted, the colour of this cell also changes.
If all the cells of the column “EVENT” corresponding to the parameter “RISK” are highlighted, the colour of this cell also changes. This denotes the moment of the occurrence of risk at the organisation.
Highlighting of the cells of the RISK REGISTER allows to make a Risk Diagram which reflects the process of risk occurrence in time. An example of such a process is shown in Fig. 7.
In order to prevent and monitor risks, the organisation creates a set of documents, which describe the measures and procedures of elimination of the factors that may cause risks. All the documents are approved by the administration of the organisation and stored in accordance with the rules of the IT service.
The BI system also has a function that allows Managers to take risk prevention measures using the Risk Diagram.

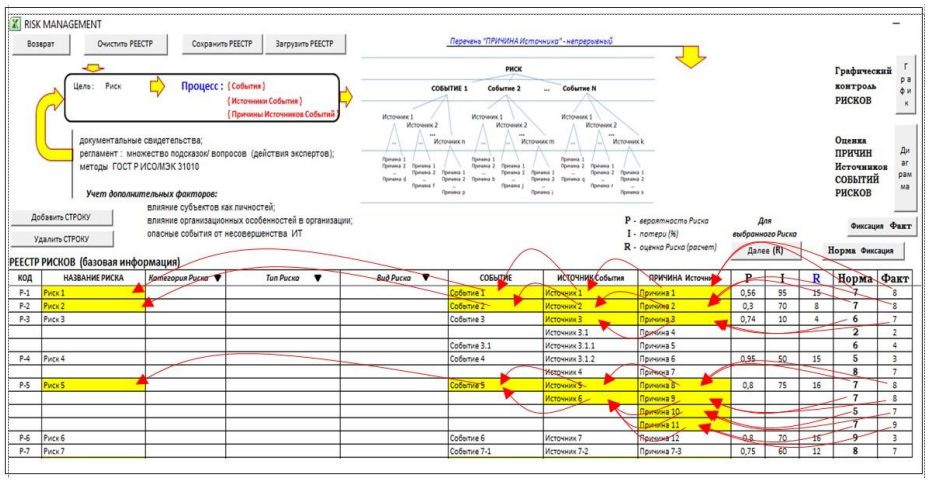


Fig. 7. Graphic monitoring of risks via the Diagram

When a Manager makes a decision to take certain actions to eliminate a threat of risk based on the Risk Diagram, the employees can open a corresponding document and act accordingly. The subsystem responsible for the process is demonstrated in Fig. 8. Thus, the proposed algorithm allows for real time risk elimination.

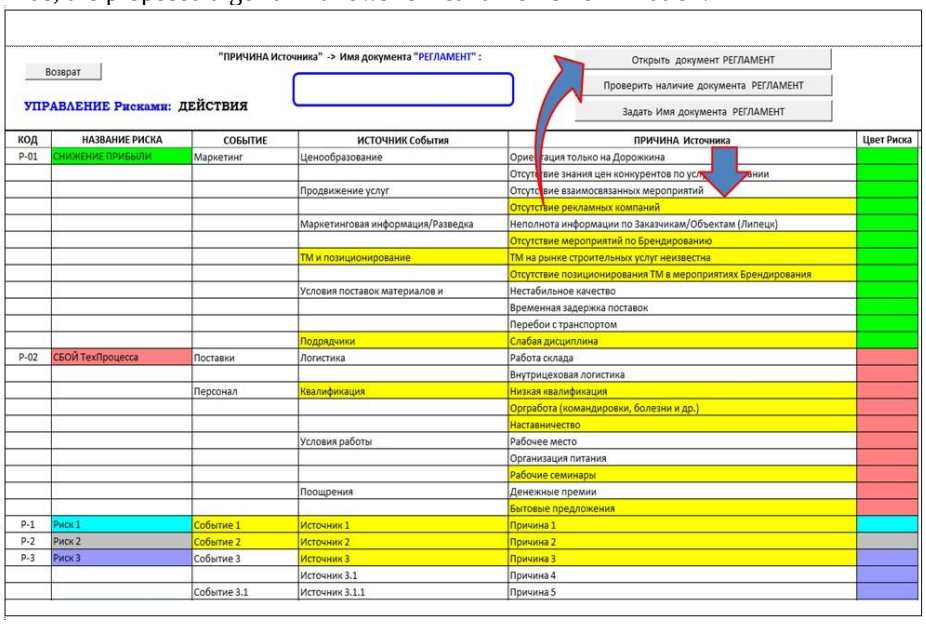


Fig. 8. Additional risk management interface of the BI system

5 Conclusion

- The paper suggests a methodology of risk assessment based on the recommendations and requirements of ISO/IEC 31010 standard regarding the outer and inner parameters of a specific organisation.
- A System for Prevention and Management of Process-Related Risks (SPMR) is suggested. It helps to forecast and monitor the risks effectively.
- The system is based on the BI system workflow, which allows the Managers of the organisation to receive graphic information.

1. At the stage of the RMS design the Managers receive the following information:
   a. - information about a certain risk;
   b. - information about all the risks;
   c. - information about the process of risk occurrence.
2. At the Risk Mitigation and Management stage the Managers receive the following information:
   a. - information about the probability of any risk over time;
   b. - information about the probability of certain risks over time;
   c. - a set of measures that can be taken to eliminate the risk probability, i.e. Risk Prevention Measures.

References

1. ISO/IEC 31010:2009, Risk management - Risk assessment techniques
2. ISO 9001:2015, Quality management systems — Requirements
3. Abramov I.V. Working with risks based on GOST R ISO/IEC 31010. - Economy and society, №4 (23) 2016. 30p.
4. Beasley, M.S., Clune, R. & Hermanson, D.R., 2005. Enterprise Risk Management: An Empirical Analysis of Factors Associated with the Extent of Implementation. Journal of Accounting and Public Policy, 24: 521–531.
5. Hoyt, R. E. & Liebenberg, A. F., 2011. The value of Enterprise Risk Management. The Journal of Risk and Insurance, 78(4), 795-822.