New approach to risk controlling in information security

G Zolotareva, V Zolotarev, S Filko
Siberian State University of Science and Technology named after Academician M.F. Reshetnev
31 “Krasnoyarskiy Rabochiy” prospect, Krasnoyarsk, 660014, Russia
E-mail: astra07@inbox.ru

Abstract. At present, current methods and means of enterprise risk management are not integrated within the framework of a single methodology. Accordingly, they can be used only when solving particular problems. In connection to this, one of the most prosperous risk management concepts is controlling. It provides wide opportunities for integrated consolidation and development of various management schools scientific views. At the same time, attention is focused on the instrumental and information support of management processes. The target of current research is to improve the process of information risk management on the basis of an organizational approach. Objectives of the research: to study the possibilities of existing organizational management methods application to protect information in corporate systems, to develop the concept of an organizational approach to the formation of an information risk management system. The object of research are the risks that arise during the information processing. The subject of the study are models, algorithms for managing information risks.

The result of the research is the risk-controlling of information security method, which made it possible to improve the efficiency of information risks management at the ship repair enterprise due to the synergy together with the improvement of various business processes. The method was tested, positive economic effect received up to 16% of the annual budget. The obtained results can be used as a fundamental basis for research the methodology of information risk-controlling development. It is possible to apply the assessment results obtained by the method implementation in simulation models, statistical calculations, the ISO 27001 PDCA cycle, and quality management.

1. Introduction

Ensuring the stable and correct functioning of the corporate information system (CIS) of the enterprise is one of the fundamental goals in the context of providing it with information and economic security. it is necessary to organize the risks management of the CIS operation To achieve the goal, including information security risks.

There are many approaches to risk management, including those that implement various aspects of information and economic security monitoring. The issues of network management and the model of risk distribution taking into account the structure and features of the systems [1, 2] and models for analyzing the correctness of business processes are interesting in the key of the problem considered [3]. Of course, the approach chosen in the article is not the only one. You can consider schemes with indicators of utility, which are also successfully used in economic systems, from the perspective of
risk assessment [4]. A variety of evaluation methods are also popular, based not so much on monitoring as on predicting the level of risk, such as the Monte Carlo method [5].

Of course, information security risk management is usually connected to determining the level of security. As in quality management, the SLA accordance is the estimated parameter here [6]. The management of information flows and the consideration of different levels of security requirements for various types of subsystems, for example, controlling and controlled, are of great importance for risk management techniques in the field of information security [1, 2, 7].

Various methods of applied probability theory are usually used when choosing risk management techniques. These methods are the basis for many methods and directly in the tasks of information security ensuring [8] and are a universal tool for their solution.

As a rule, the formation of an information security (IS) risk management system begins with the definition of the methodology. The most difficulty is the choice of methods for planning and organizing a risk management system. On the one hand, it is practically impossible to find a methodology that would satisfy all modern requirements, on the other, as a rule, there is the problem of limited resources, which are economically expedient to use in the tasks of ensuring information security. Taking into account the above, we will try to consider the task of forecasting and managing information security risks, as well as monitoring information security based on the controlling approach.

2. Problem statement
As initial assumptions in the development of the methodology for process of planning and organization risk management system, the following were accepted:

• the information system is affected by risks that may lead to the lack or partial accordance to information security requirements;
• the impact of information risks can be both external and internal direction;
• a significant number of unstructured risks;
• the impact of information risks has probabilistic nature.
• an acceptable level of risk $R'$, not requiring measures to counter threats, is set.

In this situation, characterized by a high degree of uncertainty, the application of methods of fuzzy sets theory and fuzzy logic in the planning and organization of the information risk management system is proposed.

3. Description of the proposed methodology
Based on the analysis of different approaches to the essence of controlling and its genesis, controlling can be characterized as a new management paradigm ensuring a high degree of enterprise adaptability in an unstable environment and the possibility of global automation of managerial processes [9].

The novelty of controlling is concluded in the approach to a combination of principles, methods and tools that allow to effectively develop the management system in the sphere of providing managers with relevant, timely, objective and valuable information for decision-making.

That is why, controlling is the main applied area of information management systems development currently, for example, ERP-systems.

The most important, in our opinion, feature characterizing modern controlling and predetermining its further wide development is the combination of the traditional functional and process approaches to management, which has become relevant over the past two decades. The functional approach is implemented in controlling in various forms, for example, in the management by the responsibility centers, providing a clear regulation and distribution in the management structure of the basic management functions. The functional approach is the structure-forming basis of controlling and gives it the necessary "rigidity".

The main problems of functional management are the next one:

• low speed of response to management impact and adaptability to a changing external environment;
The lack of direct interest of the company's employees in improving the final result.

The process approach to management used by most Russian corporations in accordance with the requirements of the national Russian quality management standard ISO 9001-2015 allows to overcome these disadvantages of the functional approach. The process approach is aimed at obtaining a qualitative result for consumers, which is achieved due to the interconnectedness of successive processes, that is, the system of actions that convert resources at the input of the process to a certain output result and provides adaptability and flexibility of the control system [2, 9].

The increasing role of risk controlling in the further improvement of the controlling concept is predetermined by the development of the theory and practice of modern management, accompanied by the constant update, development and transformation of tools that have become traditional. The isolation of risk controlling is mainly due to the increasing turbulence of the external environment, growing risks, uncertainty and general instability, and is logical, reasonable and expedient [9-11].

![Figure 1](image-url)

**Figure 1.** Scheme of organization of information security risk-control based on the requirements of ISO 27000 series standards

The proposed scheme for organizing information security risk control, based on the model of information management of the enterprise in accordance with the requirements of international standards (primarily ISO 27000 series) is shown in Figure 1.

Risk-controlling security of corporate information systems is understood as a system of coordinated functions, methods and tools implemented and applied by the company's personnel in order to optimize the costs of countering information risks and minimizing the damage from their implementation.

The process model of information risk controlling should consist of the following stages or subprocesses: 1) planning and organization, including identification, quantification and assessment of risks; 2) operation of the established risk management system; 3) control; 4) improvement.
The procedures for assessing and processing risk in information risk control can be performed iteratively. Such an approach in risk assessment, as a rule, can increase the detail and depth of the assessment at each subsequent iteration [2, 12].

The presented concept of risk control of information security assumes constant monitoring and control of all managerial and technological processes of the information system of the organization.

Further, we will consider the model of the process of planning and organizing a risk management system in more detail, which is the key in the proposed methodology.

The model of the planning and organizing a risk management system process consists of eight modules (Figure 2).

![Figure 2](image.png)

**Figure 2.** Scheme of interaction between the modules of the planning process and organization of the risk management system

Let us consider the tasks of each module, methods and algorithms for solving module tasks.

The task of module 1 is to obtain metrics that characterize the effectiveness of the information risk-controlling system. For each security function considered $SF_i (i = 1, 2, ..., n)$ the main metric will be the failure-free operation of the function for a given time interval. For the probability of failure-free execution of functions $P(Y_i)$, where $i$ is the time of failure-free execution $SF_i$.

The output value of module 2 is a list of risk factors that are taken into account.

Module 3 is designed to obtain a quantitative estimate of the level of information risks, and statistical estimates of the impact indicators of threats that are used in Module 1 when determining the levels of performance of the security functions of the information risk-controlling system.

The algorithm of module 3 is based on the following assumptions:

- there is a set of input parameters $Y_i (i = 1, 2, ..., M)$, the estimates of which were obtained in module 1;
it is necessary to obtain a quantitative estimate of the parameter $r$ (the current level of information risk);

there is a set of linguistic terms characterizing the values of the input $\alpha^k, k \in [1, N_i]$

To solve the problem of module 3, it is expedient to apply fuzzy logic methods. The algorithm of module 3 includes the following steps [13-15]:

The controller specifies a set $Y = \{Y_i : i \in [1, M]\}$, that includes a set of indicators characterizing the levels of performance of the safety functions of the risk-controlling system, as well as the number of terms and their meanings.

A knowledge base is formed in the form of a rules set

$$F : \prod_{i=1}^{M} \{\alpha^k : k \in [1, N_i]\} \rightarrow \{\delta : j \in [1, N]\}$$

Where $\alpha^k$ is the set of linguistic terms
$y_i$ is variable values of input parameters
$r$ is variable values of output parameters
$N_i$ is number of terms of the parameter $y_i$
$N$ is number of terms of the parameter $r$

From module 4, we obtain metrics for elements of sets $Y$: $\{P_{\alpha^k} (y_i): i \in [1, M], k \in [1, N_i] \}$ and $R$: $\{R_{\delta_j} (r): j \in [1, N] \}$.

From module 1, we obtain estimates of the input parameters $Y_i (i \in [1, M])$, corresponding to the current level of performance of the security functions of the information risk-controlling system.

Fuzzification of the input parameters is carried out, the values of membership functions are determined, corresponding to the estimates obtained in step 4: $\tilde{P}_{\alpha^k}, k \in [1, N_i] i \in [1, M]$.

The resultant membership function $\tilde{R}(r)$ is constructed for the output parameter.

The resultant value $R$ of the output parameter is calculated by defuzzification the fuzzy set $\tilde{R}(r)$.

The calculated current level of the risks $R$ is the input parameter for the module 5.

The task of module 4 is to build membership metrics for fuzzy sets, which are necessary for estimating the current level of information risk in Module 3 [7].

$$y_i = \alpha^j (i \in [1, M], k \in [1, N_i]), \quad r = \delta (j \in [1, N])$$

Since the tasks of module 4 have a high level of uncertainty, in our opinion, it is expedient to use expert estimation methods when solving them.

The task of module 5 is the planning of risk processing. To solve the problem of module 5, the following approach is used. The input parameters of the risk management planning module are the specified level of acceptable risk $\tilde{R}$ and the level of risk $R$ estimated in module 3. To implement the decision making task in Module 5, algorithms for finding the maximum and optimal elements on the graphs can be used. The result of module 5 operation is the decision to choose a risk processing method.

The module 6 for forecasting the ratio of alternatives and the outcomes of the importance of the criteria and alternatives is necessary for calculating the importance coefficients or the value of local priorities characterizing the relative influence of the set of elements of the hierarchy on the element of the upper level adjacent to them. Based on the predicted outcomes, the decision maker chooses the preferred solution.

The chosen variant of risk processing is the basis for the formation of the budget for managing the information risks (module 7). The purpose of module 7 is to form the main economic source for
monitoring the compliance of the information security risk-controlling system to the criteria developed and to analyze the costs and economic results from the implementation of the activities for managing the information risk budget for managing the information risks. In the allocation of authority in the implementation of measures to manage information risks in information security, it is necessary to ensure the binding of duties to the documents regulating information security [16]. The key task of this module is to optimize the cost of risk management, which consists of the costs of countering information risks and damage. This module should be in accordance with the conceptual principles of controlling inextricably and dynamically linked to the developed risk-controlling policy (module 8). This ensures the flexibility and efficiency of the entire proposed method of risk-controlling information security.

The proposed model of the process of planning and organization of the risk management system makes it possible to effectively use the organizational approach to risk management in the field of information security and enter a qualitatively new level of risk management.

4. Discussion
The proposed methodology was practically used in the development of scientifically grounded recommendations on the creation of an information risk management system in ship repair divisions of JSC "Yenisei River Shipping Company".

A software package for information risk management has been developed that implements the proposed methodology and allows to create a knowledge based on fuzzy logic methods and to carry out a logical conclusion based on expert estimates of metrics.

In order to obtain the initial data for the evaluation of the results, we used network monitoring systems, virus detection statistics of the network antivirus server, and others. Experts in assessing the cost of resources were employees of the Krasnoyarsk Ship Repair company. Data on the network was collected and processed before and after the implementation of the proposed approach.

Studies have shown that, for example, after introduction, the volume of spam on average dropped by 12-14%. The risk indicators for the changed information security system were calculated. It showed that the minimum total risks for all threats correspond to the basic structure of the system.

In the course of assessing and ranking the economic feasibility of a set of measures for information protection, a set of tools that significantly does not affect the overall information security indicators of an enterprise but is costly (for example, a unused VPN service) has been identified and decided not to use them. In addition, studies have shown that the reliability of the security system (reducing the probabilities and overall risks) can be enhanced by using low-cost tools such as strengthening antivirus protection and adding elements to filter spam. As a result, the expected savings in the budget for managing information risks will be about 16% in 2018.

5. Conclusion and results
The implementation of the proposed methodology for managing information risks within the framework of the information security risk-controlling made it possible to reach a qualitatively new level of management:

- the effectiveness of monitoring and control of information threats has increased (up to 14% in quantitative terms);
- the level of coherence and, accordingly, the effectiveness of the application of the whole complex of the mechanisms of the management system of ship repair enterprises has increased (savings by means of increasing efficiency amounted to 16% in the whole for the enterprise.);
- the implemented approach has radically changed the essence of the organization of risk management in enterprises - managers and employees are actively involved in the management of information risks.

The presented concept of information security risk-controlling assumes constant monitoring and control of all managerial and technological processes of the information system of the organization.

An interesting consequence of the methodology used can be a single frame of assessment for economic processes, including processes related to security, as well as their simulation models. It is known that such models are used as an element of changes management within the process approach for estimating the predicted number of errors in individual processes, including automated ones [17]. Thus, assessing the safety requirements using proposed methodology, the expert can predict the
development of the situation in the system as a whole, including business processes adjacent to the analyzed, and indicate the necessary adjustments, arguing them with quantitative indicators.

Using the methodology of controlling in the formation of an organizational and economic approach to the management of information risks allows to create an integrated system of information risk management. The use of controlling as a structuring concept of information risk management will make it possible to unite similar processes and ensure the effective and safe operation of the enterprise.

References
[1] Beckers K, Côté I, Faßbender S, Heisel M and Hofbauer S 2013 A pattern-based method for establishing a cloud-specific information security management system: Establishing information security management systems for clouds considering security, privacy, and legal compliance Requirements Engineering 18-4 pp 343-395
[2] Beckers K. 2015 Pattern and Security Requirements: Engineering-Based Establishment of Security Standards pp 474
[3] Burattin A, Maggi F and Sperduti A 2016 Conformance checking based on multi-perspective declarative process models Expert Systems With Applications 65 pp 194–211
[4] Rubinstein A 2013 Lecture Notes in Microeconomic Theory (Princeton University Press) p. 153
[5] Petrone D and Latora V 2018 A dynamic approach merging network theory and credit risk techniques to assess systemic risk in financial networks Scientific Reports 8-1 pp 5561
[6] Saadaoui A and Stephen Scott L 2017 Web Services Policy Generation Based on SLA Requirements Proceedings 2017 IEEE 3rd International Conference on Collaboration and Internet Computing pp 146-54
[7] Weerakkody S, Sinopoli B, Kar S and Datta A 2016 Information flow for security in control systems 2016 IEEE 55th Conference on Decision and Control pp 5065-72
[8] Thakur K, Ali Md L, Kopecky S, Kamruzzaman A and Tao L 2016 Connectivity, Traffic Flow and Applied Statistics in Cyber Security Proceedings 2016 IEEE International Conference on Smart Cloud pp 295-300
[9] Filko S B and Filko I V 2014 Controlling in innovation sphere: instruments, methods (Krasnoyarsk: KrasGUA) pp 154
[10] Lyubimov A, Cheremushkin D, Andreeva N and Shustikov S 2011 Information security integral engineering technique and its application in ISMS design Proceedings of the 2011 6th International Conference on Availability, Reliability and Security 6045981 pp 585-90
[11] Zolotareva G.I. and Fedorenko I.V. 2015 Methodology of accounting system information security audit (Krasnoyarsk: Siberian state aerospace university) p 176
[12] de Araujo M, Oliveira E and Monteiro S 2017 Maturity assessment of IT risk management processes: support tool for quality and efficiency of process Revista brasileira de computacao aplicada 9-2 pp 111-24
[13] Huang X and Xu W 2018 Method of Information Security Risk Assessment Based on Improved Fuzzy Theory of Evidence International journal of online engineering 14-3 pp 188-96
[14] Anikin I V 2016 Information security risks assessment in telecommunication network of the university IEEE Conference 2016 Dynamics of Systems, Mechanisms and Machines pp 1–4
[15] Zyrionova T U and Yalishev U I 2006 The algorithm of information risk assessment based on fuzzy sets and fuzzy logic MIET bulletin moscow institute of transport engineers 14 pp 18-22
[16] Pyatkov A and Zolotarev V 2013 About responsibilities distribution for information security Proceedings of the 6th International Conference on Security of Information and Networks pp 380-83
[17] Popov A, Zolotarev V and Bychkov S Implementation of a combined algorithm designed to increase the reliability of information systems: simulation modeling IOP Conference Series-Materials Science and Engineering 155-1 012010