The Information Security Risk Management

Valeriy G. Semin, Elena G. Shmakova[1]
Russian State Social University
Moscow, Russia
[1]rusja_lena@mail.ru

Alexei B. Los
Research University Higher School of Economics
Moscow. Russia
alexloss2011@mail

***Abstract*— The main formal tasks of the information security risk management process using functional and contextual models reflecting the basic concepts and basic functions of information security risk management systems.**

Keywords— threat; vulnerability; risk; risk management; the membership function; threat structure

I. INTRODUCTION

It is known, that the development of a risk management system is an important task of the overall problem of ensuring information security [7]. Development and implementation of systems of risk management information security are regulated by international standards (ISO / IEC 17799, GOST R ISO 9001-2008, GOST R IEC 61508-5-2007). The purpose of this work is the structural and functional modeling of a multi-stage process of information security risks management and game-theoretic algorithmicization of the context, that is the definition of internal and external parameters of risk management process under study. At the same time, for the stages of qualitative and quantitative risk analysis, a fuzzy logic-probabilistic approach to the task of synthesizing threats to information security was proposed. Based on the results of the algorithmization of the context under investigation, a minimax algorithm for information security risk management was developed in the class of matrix antagonistic games, which reduces to the problem of linear mathematical programming. It is shown that the application of the principle of guaranteed result in the task of developing a risk management algorithm ensures the invariant nature of the algorithm in relation to application areas [1, 2, 5, 6].

II. METHODOLOGY

Let's consider the structural and functional model of the information security risk management process. This model includes the following: a risk management plan - selecting an approach, establishing a primary risk register and risk management operations; Risk identification - definition of the register of risks to be investigated, documentation of their parameters. Stages of qualitative and quantitative risk analysis are presented in one block "Risk Analysis". Qualitative analysis - the structure of the register of risks is created in accordance with the level of priority of the probability of their occurrence and possible losses. Quantitative risk analysis - quantitative assessment of potential damage to identified risks of information resources. Planning for a response to risks - developing possible options for countermeasures to minimize the consequences of risk realization. Monitoring and risk management - monitoring of risks contained in the register, as well as residual risks, identifying new ones, responding to risks during the life cycle of the information resource. Therefore, the task of creating, documenting, developing and updating the structure of the risk register, calculating the maximum possible damage, manufacturing and distributing protective measures for vulnerabilities is the essence of the risk management process. At the same time, the task of developing a threat structure (forecasting) should be the main tool for organizing risk management. The process of continuous management begins and ends with a structurally-parametric description of the risk register. To determine the context of the problem of risk management, consider a conceptual model of risk management [6, 7]. This model, reflecting external and internal factors, the basic concepts of this control problem, is shown in Fig.1.

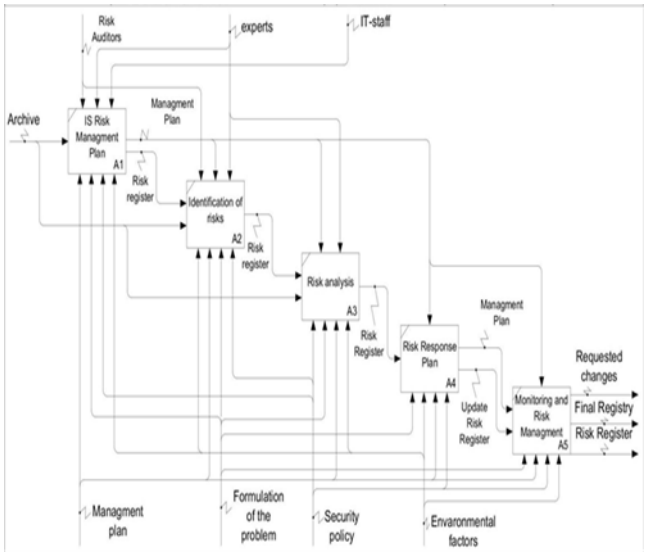

Fig.1. Structurally functional model of information security risks management.

Let's consider the basic elements of the conceptual model and their definitions: Risk owner is the person who responsible

978-1-5386-0703-9/17/$31.00 ©2017 IEEE

for managing information risks, in order to preserve information resources; Counterparties are undefined factors of the external and internal environment that influence the decision-making process; Countermeasures are measures to counter information risks; Threat is a combination of factors and conditions that arise in the process of interaction of the object of protection with the external environment, potentially capable of adversely affecting the result and purpose of management; Vulnerability is a state of the protection object that affects the likelihood of the threat. It should be noted that from the point of view of the problem of operations research, the context model of the risk management process, reflecting the parties' antagonistic goals, can be interpreted as a schematic description of the simplest operation of choice.

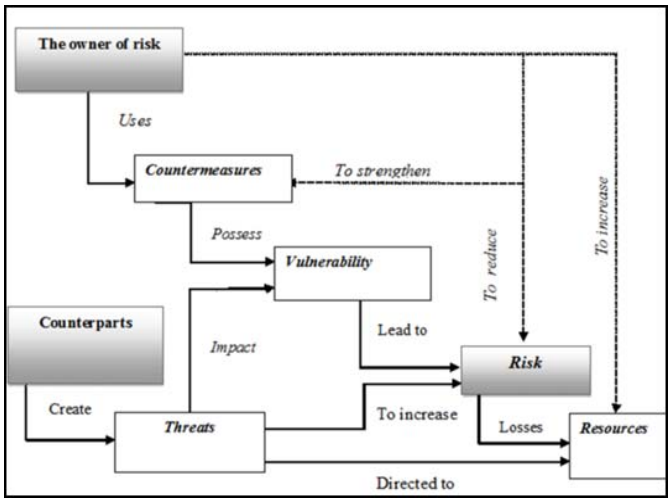

Fig. 2. The conceptual model of the context of the task of information security risk management.

In the absence of knowledge of the probabilistic distribution of a set of uncertain factors, it is necessary to choose a risk management strategy that maximizes the selected efficiency criterion for the operation with the least favorable behavior of uncertain factors.

As a rule, when making decisions, X has the ability to choose only a part of the coordinate vector (x, y, ..., t) consisting of x = (x1, ..., xn) and Y = (y1, ..., Ym). It is required to choose such a strategy that the criterion of the effectiveness of the operation should have the maximum value [4.7].

This approach leads to the choice of strategy in accordance with the principle of guaranteed result by the criterion:

$$\min_{x} \max_{y} K(X,Y)$$

Let the function K (x, y) be the matrix of gaming payments. The value of the payment function when choosing the first player of strategy x and the second player of strategy y will be called the player's prize. Such a game with opposite interests of players is called antagonistic game. Let x and y be vectors of n- and m-dimensional Euclidean spaces; X and Y are closed bounded sets of n- and m-dimensional Euclidean spaces, respectively. In this case, all points of these spaces can be ordered lexicographically, so that K (x, y) enters the function K (i, j), i arg = 1, ..., r; J = 1, ..., r, and then consider the function of two points with payment function K (i, j). The finite matrix game has a saddle point, there are pure strategies i_0, j_0 and constant w for which $K(i_0, j_0) = max\ min\ K(i, j) \le\ min\ max\ K(i, j)$, where $w = K(i_0, j_0)$. The paper [1] gives a formal justification for the solution of a finite matrix game with zero sum, it is shown that it reduces to the solution of the problem of mathematical programming. In the format of the conceptual model of the context of the risk management task, we introduce the following notation:

$T = \{T_i\}, i = (1,...,I)$ - set of threats; $R = \{\langle E_j, Q_j \rangle\}$, $j = (1,...,J)$ - set of risks, where E_j - event of risk Q_j - size of damage; $U = \{U_d\}$, $d=(1,...,D)$ - A number of vulnerabilities - the states of objects (conditions) that facilitate the implementation of threats; $S = \{S_k\}$, $k=(1,...,K)$ many sources of negative influences (threats); $O = \{O_b\}$, $b=(1,...,B)$ set of objects influences; $Z = \{\langle F_n, C_n \rangle\}$, $n = (1,...,N)$ - set of measures aimed at minimizing risks, where F_n - implemented function, C_n - the cost of measures to counter the negative influences.

For given sets, we define the structure by setting the following relations:

- $O \times R \xrightarrow{f_1} A$, where A is a set of numbers from 0 to 1, determine the degree of conditionality of risks there is a set of objects;
- $S \times T \times O \xrightarrow{f_2} V$, where V-set of numbers from 0 to 1, determine the degree of criticality of the impact of negative factors;
- $T \times U \times R \xrightarrow{f_3} P$, P- where a plurality of pairs of numbers $\langle P^{(E)}, P^{(Q)} \rangle$, that determine the potential risk - the degree of marketability of risk events if there are many negative influences and a variety of corporate vulnerabilities, such that $0 \le P^{(E)} \le 1, P^{(Q)} \ge 0$.
- $Z \times U \xrightarrow{f_4} M$,

where M - is the set of numbers from 0 to 1 - the degree of vulnerability in the conditions of applying several methods of counteraction.

In [1-6, 7] it was shown that in order to reduce information risks, it is necessary to optimize the use of countermeasures by the criterion of type

$$\min_{\Sigma} \max_{T} P_{\Sigma} \quad (1)$$

$$P_{\Sigma} = \left\{ \left\langle P_{\Sigma}^{(E)}, P_{\Sigma}^{(Q)} \right\rangle \right\} \quad (2)$$

where P_{Σ} - consolidated risk taking into account the risks involved in all the activities of the corporation; $P_{\Sigma}^{(E)}$ - the feasibility of a risk event: $P_{\Sigma}^{(Q)}$ - consolidated damage. Expressions (5-6) define the content of the risk management algorithm solve the problems of risk assessment, it is necessary to consider the algorithm for modeling the structure of threats based on typed structures - tree-based threats. The threat T_0 is realized only when implemented by a sequence of threats T_i. Combining a number of trees leads to the formation of the structure G, having a partial order of properties that define how network threats $R = \bigcup_{i=1}^{M} T_i, i \in N$.

The degree of risk is determined by the maximum degree of feasibility of the risk event among all possible risk event:

$$P_{\Sigma}^{(E)} = \max_{j} P_{j}^{(E)}, \quad (3)$$

where $P_{j}^{(E)}$ - the degree of marketability j-risk events.

Consolidated damage is defined as the aggregate amount of the potential j-damages associated risks in all indices j:

$$P_{\Sigma}^{(Q)} = \sum_{j=1}^{J} P_{j}^{(Q)} \quad (4)$$

where $P_{j}^{(Q)}$ - j-potential damage risk.

The degree of feasibility of the j- risk event is a functional of the form:

$$P_{j}^{(E)} = P^{(E)}(T, R, U, S, O, Z) \quad (5)$$

Potential j-damage risk is a functional of the form:

$$P_{j}^{(Q)} = P^{(Q)}(T, R, U, S, O, Z). \quad (6)$$

Consequently, the consolidated risk is defined as a pair - $\left\langle P_{\Sigma}^{(E)}, P_{\Sigma}^{(Q)} \right\rangle$ where the relevant elements of the pair are determined by the formulas (3) and (4).

Numerical implementation of these expressions includes parametrization of the class of structural abstractions used to model threats to information resources. Three structural abstractions are considered as such models: generalization, aggregation and association.

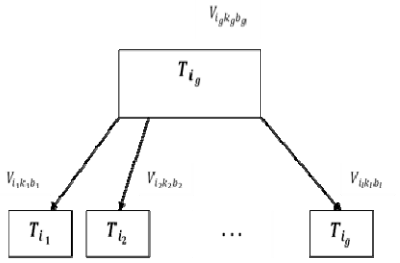

Fig. 3. The model of structural abstraction aggregation.

The indicator of the criticality index of the threat is defined as follows:

Vikb =V kb · Vik · Vib · α (T_i),

where: Vikb is the criticality index of the i-threat from the k-source in relation to the resource b; Vkb - the degree of security (vulnerability) b from the potential impact of the k-source; Vik - degree of realizability of the i-threat from the k - source; Vib - degree of criticality of consequences of i-threat implementation for resource b; A (Ti) is the weight of the criticality of the implementation of the i-threat at a given moment in time. It is known that these structural abstractions allow modeling a wide range of relationships, which means the possibility of implementing the task of parametrization of the threat structure. Qualitative assessments are based on subjective probabilities and fuzzy estimates, such as "low probability", "average", etc., which are associated with the school of probability. An example of such a probability scale is shown in Fig. 4

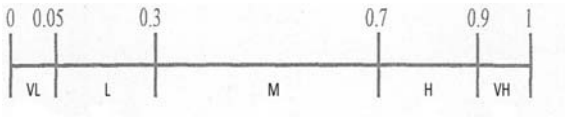

Fig.4. Intervals of the qualitative

Then the qualitative indicators are translated into quantitative values. The structural abstractions under consideration are the basis of the logical-probabilistic method of modeling the structure of threats. Implementation of this method with the use of linguistic probabilities opens the possibility of using an effective modeling tool Fuzzy Logik. It is known that the general logical-probabilistic method realizes all the possibilities of modeling the algebra of logic in the functionally complete base of operations "AND" (connection), "OR" ("Disjunction") and "NOT" (inversion). In this case, the operations of the algebra of logic also apply to fuzzy operators used in fuzzy logic. The following analogues of the usual logical operations are used: fuzzy logical negation, fuzzy-logical disjunction, fuzzy logical conjunction, fuzzy logical implication. This tool can be used as an expert system for solving problems of synthesis and parameterization of the threat structure. Subject to set the values of parameters *T, R, U, S, O, Z* and mappings $f_a, a = 1,2,3,4$ in the form of the corresponding sets of discrete values, which completely describe the domains of definition of the functionals (5) and

(6). The solution of the optimization problem with criterion (1) is considered as a game with a payment matrix. Elements of the matrix are determined in accordance with the following rule

$$p_{i,n} = \left\langle P_{\Sigma}^{(E)}, P_{\Sigma}^{(Q)} \right\rangle_{i,n}$$

In order to solve the problem it suffices to consider one of the dual games. To solve the game in the class of linear programming problems, we introduce a Boolean vector , describes the optimal solution of the problem from the point of view of the criterion (1). The coordinate of the vector takes the value 1 in the case of counteraction to a non-empty set of threats and 0 otherwise. By definition, the degree of vulnerability availability is calculated as follows:

$M_d = (1 - Y_{dn}) \times X_n$ where, M_d - is the degree of feasibility *d*-vulnerability; Y_{dn} degree of efficiency *n*-function counter existing threats by exposing the vulnerability; $X_n = \{1, 0\}$ - vector decision in which: 1 corresponds to the realization of the *n*-ways to counter; *0* - in otherwise.

It is necessary to find such X_n *, (n=1,...,N)*, to achieve:

$$\min_{1 \le n \le N} \max_{1 \le i \le I} P_{\Sigma}$$

with restrictions:

$p_j^E \le P_{j_{\max}}^E$, where, $P_{j_{\max}}^E$ – the maximum allowable risk of realization;

$P_{\Sigma}^{(Q)} \le P_{\Sigma_{\max}}^Q$, where, $P_{\Sigma_{\max}}^Q$ – the maximum damage in the implementation of the risk;

$$\sum_{n=1}^{N} X_n C_n \le C_{\max},$$

where, $C_{\max}$ – the maximum permissible value of the means to counter the risks.

As part of this statement M_d as a vector in n

$$M_d = (1 - Y_{dn}) \times X_n$$

Revealing the consolidated risk, we obtain the expression:

$$\min_{1 \le n \le N} \left[(\max V_{ikb}) \times (\max_{b,j} A_{bj}) \times (\max(1 - Y_{dn}) \times X_n) \right].$$

Similarly conducted substitution and disclosure of formulas for the second criterion of effectiveness:

$$\min_{1 \le n \le N} \left[\sum_{j=1}^{J} (V^{\max} \times A_j^{\max} \times Q_j) \times (\max_{d} (1 - Y_{dn}) \times X_n) \right].$$

Where, $V^{\max}$ - index of criticality threat; $A_j^{\max}$ - index of criticality with respect to *j*-risk;

Q_j - is the magnitude of the damage with respect to *j*-risk.

III. RESULTS

Thus, the game-theoretic concept of the context of the risk management process allowed to develop a general approach to the problem of managing information security risks on the basis of the guaranteed result principle. It is shown that such an approach possesses invariance properties with respect to objects and various application domains [1 - 7]. Application of mathematical fuzzy logic to build the structure of the register of risks using the functions of the software Fussy Logic allows you to develop expert systems in the class of information security risk management tasks.

REFERENCES

[1] Semin V.G. “Risk management of the automated systems on the basis of the principle of the guaranteed result” Quality. Innovations. Education. - 2015. № 1 (116). - pp. 58-63.

[2] Mikheyev V.A., Semin V.G. “Optimization of process of management of scratches of information and functional security of multipurpose intelligence systems at electromagnetic influences” Technologies of electromagnetic compatibility. - 2013. - № 4 (47). - pp. 60-64.

[3] Mikheyev V.A., Semin V.G. “Development of the formal structure of a control system of scratches of information and functional security of multipurpose intelligence systems at electromagnetic influences” Technologies of electromagnetic compatibility. -2013.- № 4 (47). - pp. 65-68.

[4] Mikheyev V.A., Semin V.G. “Development of the conceptual structure of the risk management of information and functional security of multifunctional informftion systems at electromagnetic influences” Technologies of electromagnetic compatibility. -2013. - № 2 (45). - pp. 70-73.

[5] Semin V.G. “The generalized control algorithm of risks of the automated systems” Dynamics of the composite systems - the 21st CENTURY. - 2012. - vol. 6. № 4. - pp. 96-98.

[6] Valeriy G. Semin; Evgeny R. Khakimullin “Game-theoretic algorithmization the context of a risk-management”. 2016 IEEE Conference on Qualite Management, Transport and Information Security, Information Technologies (IT&MO&IS) Year 2016.Pages: 176 – 180.

[7] Mikheyev V.A., Semin V.G. “Principles and methods of implementation of the security police of the electromagnetic safety systems of multifunctional information network” Electromagnetic compatibility technologies. 2014. No. 4 (51). pp. 62-66.