Functional model of information security management

I.V. Mashkina
Department of computer engineering
and information protection
Ufa state aviation technical university
Ufa, Russia
e-mail: vtzi@ugatu.ac.ru

V.A. Mordovina
Department of computer engineering
and information protection
Ufa state aviation technical university
Ufa, Russia
e-mail: mord-vera@yandex.ru

R.M. Guzairov
Department of computer engineering and information protection
Ufa state aviation technical university
Ufa, Russia
e-mail: vtzi@ugatu.ac.ru

Abstract[1]

In the work the approach to development of a mathematical decision-making method on organizational-technical management of information security, the approach to construction of system model of information security management with IDEF-BPWin technology use are offered.

1. Introduction

A real practice of information safety management is reduced to sets of rules in most cases for today. The department of information safety functions in compliances with these rules. Also a real practice of management is reduced to sets of appendices and instructions which are poorly structured and interconnected.

It occurs because the concept of a functional model of management information safety absents.

By means of information safety management it's possible to analyze management problems effectively and to optimize expense on information security.

2. Decision-making problem on management of modular structure of information security system and a method of it's decision

During the operation period of information object plans of processing information and requirements to security level

repeatedly change as a rule [1]. Also constantly there's an information system is updated, the structure varies, new information technologies are used, new connections to system are organized. The account of these factors demands a development of new approaches to maintenance of information security.

Engineering of information security system can be such approach. System properties and parameters dynamically change depending on level of critically of the information process on the security object.

Mechanism of *organizational-technical management of information security* should be realized for this purpose. One of problems of these mechanisms is *substantiation of* security *sets* which are used in information security system during the periods of functioning of information object.

A development and practical application of the methodical maintenance are necessary for perfection, evolution and increases of information security system. This maintenance connect with use a decision of problems of information security systems' designing and organizational-technical management of information security: synthesis of structure and development of system algorithms of information security organizational-technical management.

The morphological approach's idea for modeling and synthesis of rational security sets for information security system uses in the work.

The morphological method of synthesis is used at designing of information security system and at a process of organizational-technical management of information security. It's because this method allows to realize a multiobjective and multialternative choice when system is a difficult complex. There're security sets for certain points of their installation on security object; every set is synthesized from some variety of functional security subsystems. Every subsystem has more one elementary alternative for realization.

The morphological method includes a definition of necessary functional subsystems for every security

Proceedings of the 11th international workshop on computer science and information technologies CSIT'2009, Crete, Greece, 2009

boundary according to security requirements; their representation in the form of matrixes-lines including alternatives security means as alternatives. Next all possible combinations of security means are defined on one of every matrix's line.

After construction matrixes for security boundaries start definition a functional value of every elementary alternative and costs from every security mean. The most popular method for an estimation of alternatives is a criteria method, when each alternative is estimated by concrete number.

The generalized indicator of security mean's quality is a vector which components are indicators of it's separate properties. Vector dimension is defined by number of essential properties of security means. Private quality indicators have a different physical nature and dimension. Exposure of total of quality private indicators of security means for every functional subsystem to conducting of comparative analysis and substantiation of security means' choice for exploitation in a concrete security information system is a one of problems which are solved at security system's synthesis.

The decision-making problem about a choice of security means set's rational variant for a security boundary is a transformation function of the information maintenance about requirements. It's shown to security means of the certain functional subsystem entering into a set. Also the decision-making problem is a transformation information function about security means' characteristics in a subset of the best variants $S' \subseteq S$.

Class of set's variants

$$S = \{S_1, ..., S_r, ..., S_R\},$$

where R – alternative variants' number from which the choice is carried out.

A concept of the choice mechanism is used in a decision-making problem. This concept is a train from two elements: information set allowing to compare variants or variants group, and choice rule indicating as, using a data structure, to eliminate a subset S' or one alternative SR from alternative set S.

Let's designate the general data set about security means of a boundary functional system, allowing to assign binary relations of similarity and preference, through W; data set on security means l's functional subsystem allowing to assign the same relations, - through Wl. Then the choice mechanism:

$$M = \{W; J\}.$$

For security means of l's function subsystem a set Wl includes two subsets:

$$W_{sil} \subset W_l \text{ or } W_{cl} \subset W_l,$$

where W_{sil} – security indicator;

W_{cl} – security mean's costs indicator for l's functional subsystem.

It's necessary to notice that in a decision-making process would speak about the rational decision(even in a case of choice's formalized rule) instead the optimum decision.

It's possible the decision-making model to present in a following kind using a morphological synthesis method:

$$DM : \langle P, D, R_s, S, W_l, J, S_r(S') \rangle,$$

where DM – the decision-making;

P – the decision-making purpose;

D – given data for alternatives' generation (functional subsystem's set for a security boundary);

R_s – the rule of alternatives' generation;

S – set of the generated alternatives;

W_l – the data for a choice of rational variants: the set of security characteristics and cost of elementary alternatives – the security means for every l's functional subsystem;

J – the rule of the best alternative's choice;

Sr – the chosen alternative,

$$D = \{D_1, D_2, ..., D_l, ..., D_L\}.$$

The rule of alternatives' generation Rs can be presented in an analytical kind as a sets' vector product:

$$S = D_1 \times D_2 \times ... \times D_l \times ... \times D_L,$$

where D_l – l's function subsystem – the set consisting of elementary alternatives (security means for the subsystem),

$$D_l = \{A_{l1}, A_{l2}, ..., A_{lm}, ..., A_{lk_l}\}.$$

The decision-making problem provides a given data's transformation to the decision for choice a sets' rational variant for a boundary. This problem can be presented in the form of alternatives' generation's rules' sequence and a best choice on the set criterion function.

The criterion function is a choice principle on which the security means' rational set's choice is carried out.

Let's designate a criterion function through J. Then the chosen alternatives' set, in particular, one:

$$S_r = J(S, W).$$

The knowledge processing method is developed for the decision of this problem. This method uses the experts' non-formalizable experience in a field of information security. The method provides the data's transformation from the knowledge base and decisions' conclusion in the analytical form.

The planning of the information security as a management function in a process of organizational-technical management is a uncertainty's consecutive

removal process concerning of information security system's process and security means' structure on a management object. First time it's necessary to formulate a requirements list. The demanded condition of information security system can be estimated by level's value of security (risk). It's necessary to form an information security structure and to set a target operated value's change's range. Then way's choice the planned, demanded security level's achievement is realised. The expression which describe a structure of planning process is resulted in [3]:

$$\rho_{PL} = \langle I, F \rangle,$$

where I – the information component which the data used for current decision's reception in the form of a decision-making problem;

F – the procedural component which include the basic decision-making functions (information interchange, calculated and heuristic procedures).

Heuristic procedures are based on informal experts rules.

Procedures of alternatives' generation and use of choice's rule of the best alternatives form the decision reception's mechanism in each planning process. The functional subsystem's set is set for every security boundary. The result of planning process is a command information which contains the concrete data on allocation resources. These resources are directed on achievement of information security system's target safety as a management object.

3. Structurally-system analysis' result of the information security organizational-technical management with use technology IDEF

The attempt to expand a computerized, instrumental analysis methods' spectrum with use technology IDEF-BPWin on studying of processes of organizational-technical management by information security is made in the work.

First of all, the function describing a system as a whole should be defined. There is a contextual function. The reason is a model IDEF0 [4], which represents a system as a set of hierarchical (enclosed) functions.

The contextual block's name (the functional block of the highest level) generalizes modeling delimitation.

The functional block of the highest model IDEF0 level of a contour of the organizational-technical management by information security is presented on the figure 1.

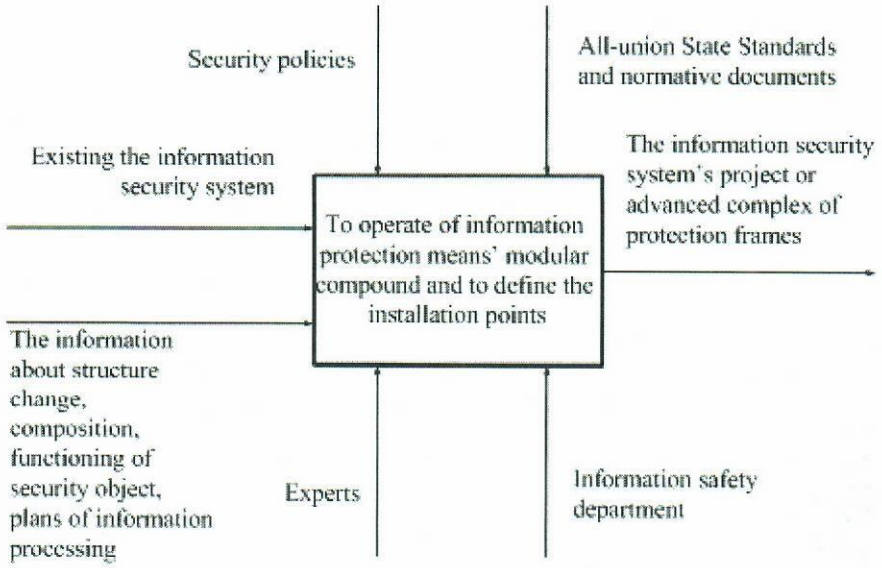

Fig. 1. Functional block of the highest level – the contextual function

The system as a functional block is resulted at zero level of a detail. Then the system is detailed, getting hierarchical structure with the increasing number of levels.

The diagram of splitting of information security organizational-technical management process on functional blocks (subprocesses) is presented in figure 2.

Any block of diagram can be decompositions to blocks. To be useful, the description of any block should include the description of objects which the block creates at a result of the works (exit), and objects block consumes (input). The functional decomposition is defined as a modelling «outside inside».

The result of decomposition of functional block "To plan" is presented in figure 3.

The result of decomposition one of the most substantial functional blocks of the diagram «to develop the concept» is presented in figure 4.

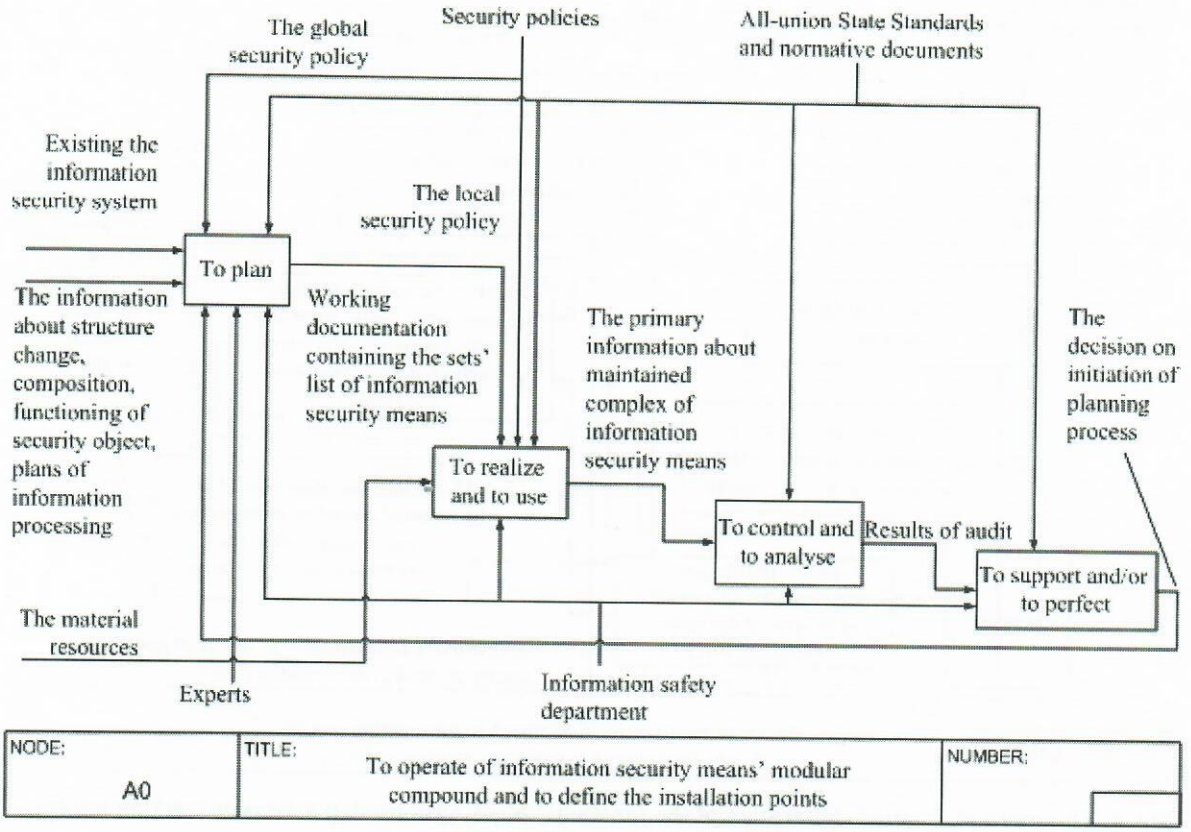

Fig. 2. Daughter diagram of the contextual functional block

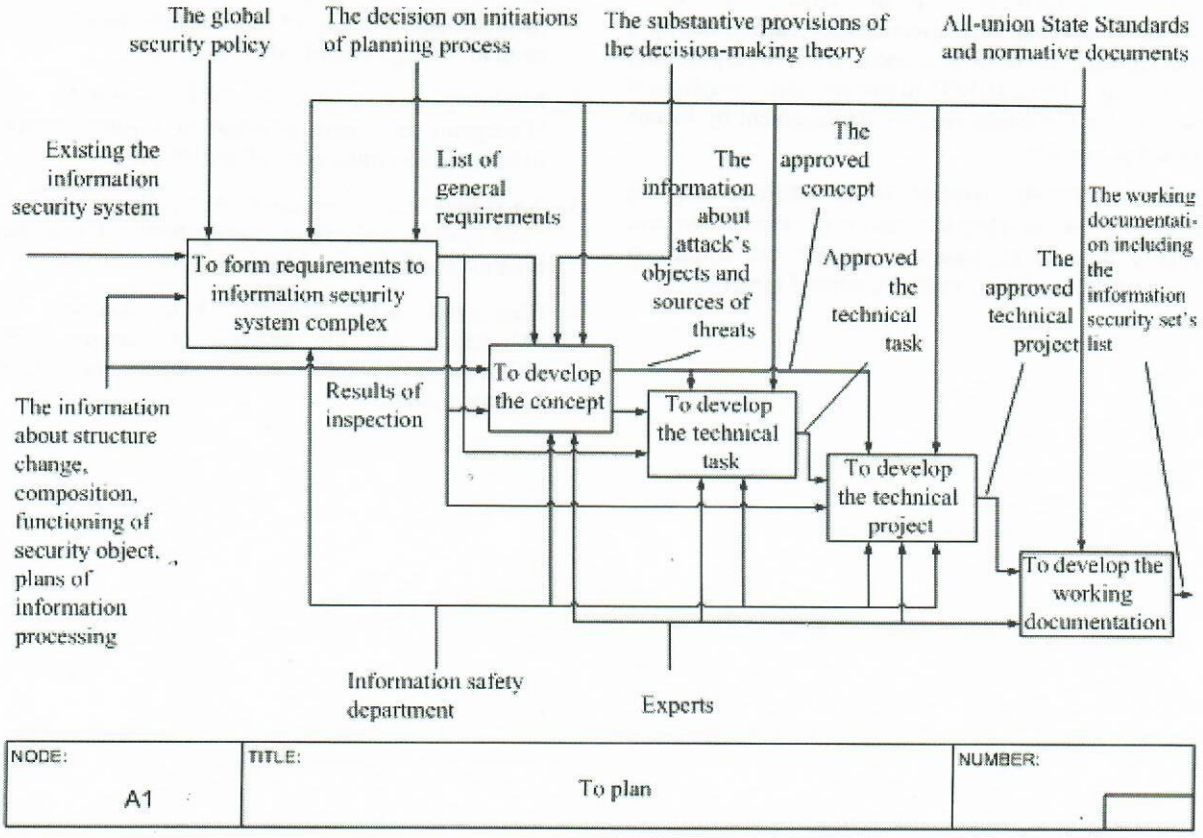

Fig. 3. The result of detailed elaboration of the functional block «To plan»

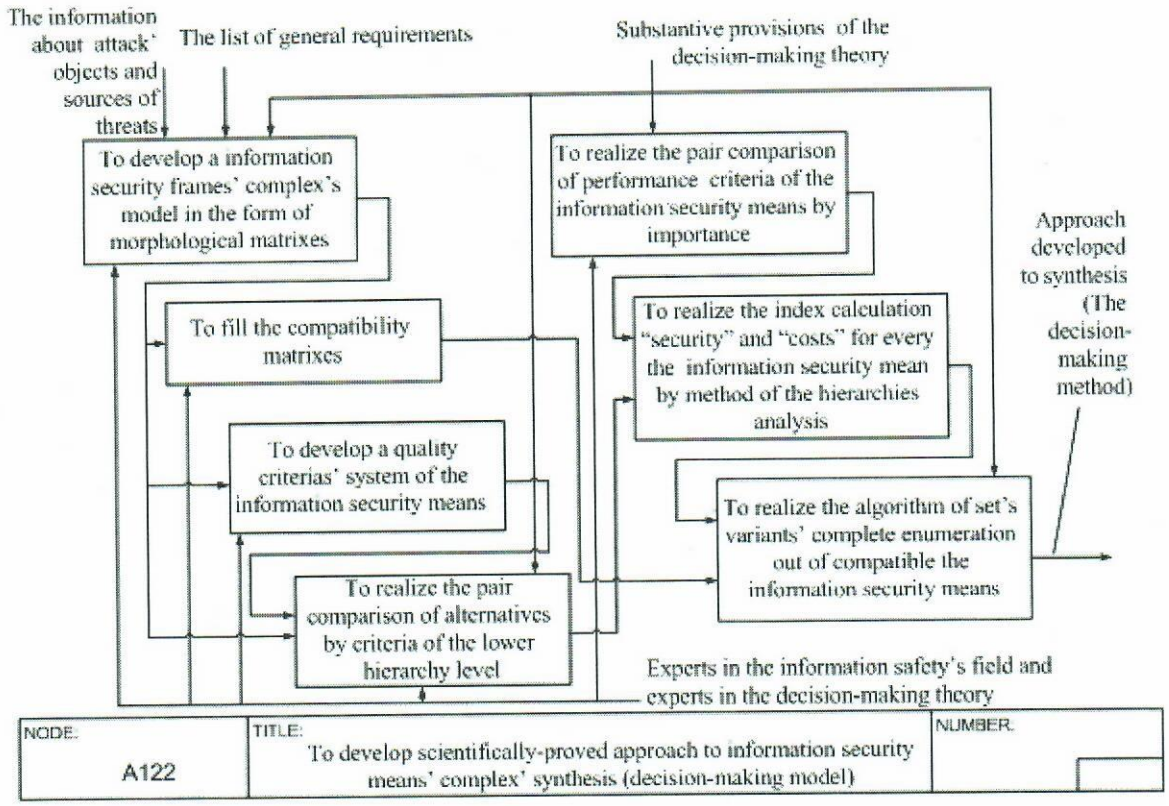

Fig. 4. The result of detailed elaboration of the functional block «To develop a decision-making model»

4. Conclusions

The IDEF0-diagramme give the chance to answer questions as a result: what functions are carried out by a control system, in what sequence, who is responsible, what is result? Thus, IDEF0 allows to solve complicated questions of information security management by means of the simple toolkit.

The use of IDEF0 standard is an effective way of optimisation of information security control system, especially because management projects are connected with construction of the automated control systems.

References

1. Malyuk A.A. "Information security: conceptual and methodological bases of information security". The manual for high school, Moscow, 2004
2. Mashkina I.V., Vasiljev V.I., Rahimov E.A. "Designing of object information security system". *Information technologies*, 2006; 10: 17-26.
3. Anfilatov V.S., Emeljanov A.A., Kukushkin A.A. "The system analysis in management": The manual. Finance and statistics, Moscow, 2006.
4. Cheremnih S.V., Semenov I.O., Ruchkin V.C. "Modelling and the analysis of systems. IDEF-technologies: a practical work". Finance and statistics, Moscow, 2006.