ФИЗИКО-МАТЕМАТИЧЕСКИЕ

METHOD OF THE STUDY OF PRIVACY PROTECTION IN INFORMATION SYSTEMS

Voevodin V.A.
Candidate of technical Sciences, associate Professor,
National Research University of Electronic Technology Zelenograd, Moscow, Russia

Abstract. The article presents an analysis of the problem of investigating the security of confidential information, formulates a goal, principles, and provides a multi-level research scheme, the content of work at each level (problem, concept, system, and detail). The description of single-level and multilevel models for analysis and synthesis of confidential information protection subsystem. The article describes the conditions for selecting an effective concept for building a subsystem for information confidentiality protection based on sufficient result and minimizing costs principles. Practical considerations for the application of the method of justification of requirements to the subsystem of protection of confidentiality, conclusions, and directions for further research.

Keywords: security system, confidentiality, system of information protection, privacy protection subsystem.

Introduction

The need for research on the protection of information confidentiality (IC)) occurs at all stages of the information system life cycle (IS).

The urgency of the problem is determined primarily by the fact that the effectiveness of decisions depends largely on the completeness and reliability of the data obtained at the IC study stage.

The requirement to ensure the reliability and completeness of the data, when performing the IC study, is one of the key points to effectively build the information protection subsystem (SPP) and information protection management in the corresponding information system (IS) as a whole. The nature and content of the stages of the IS life cycle are given in [6, 3], these stages are typical for SPP. The basic concepts, models and methods for developing similar solutions are given in [1, 2, 6, 7, 8, 9].

The General theoretical provisions for the synthesis of complex hierarchical (multilevel) systems is given in [9, 10, 11].

Based on the study of the material given in [3, 4, 5, 6, 7, 8, 9], it can be argued that the IC study at each stage of the IS life cycle is expedient to spend in accordance with the general scheme of multilevel analysis and synthesis shown in figure 1.

THE PURPOSE OF THE RESEARCH IS THE INFORMATION CONFIDENTIALITY PROTECTION

Studies on the information confidentiality protection are carried out in order:

The formulation of the problem as of the IC provision, establishing its causes, relationship to other problems (for example, ensuring the availability, integrity, etc.), to understand its nature, relevance, solvability.

Identification and modelling of the situation, in which this problem has arisen or may arise.

The formulation of the problem situation, the definition of completeness, reliability or adequacy of the information about a problem situation.

Formation and analysis of multiple alternative goals, the achievement of which will solve the problem of ensuring that CI, justification of selection rules work from many acceptable alternatives.

Research ways to implement the working alternatives and the definition of significant limitations that affect the choice of means and methods of a goal achievement, the decomposition of complex goals on private.

Justification of the necessary resources.

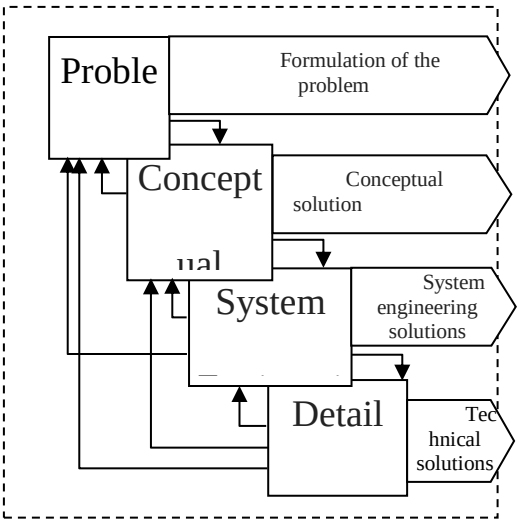

Fig. 1. The scheme of the study the confidentiality of information

The purpose of the CI study at the problem level [9, 11]:

To determine whether there is the problem of protecting CI, its causes, relationship to other problems, to assess the relevance, solvability, and the urgency of a solution.

To identify and describe the situation in which there is and can be a problem exists or may exist.

To formulate and define the problem situation the heuristic and formal methods.

To determine the completeness and reliability of information about the problem situation for measures to be taken in order to obtain the information missing.

To explore alternative goals, the achievement of which solves the problem, and to choose one of them as the main one.

To explore ways to achieve the goal, perform its decomposition.

To choose the means to achieve the goal.

To formulate the General problem, statement the information confidentiality study.

The purpose of a problem situation conceptual study:

To build an adequate model of the problem situation, to plan the experiment with the model constructed and to formulate conclusions on the experiment results.

The allocation of privacy protection subsystem in the information protection system.

Substantiation of rational behavior of the privacy protection subsystem.

To ensure the selection of the subsystem functioning efficiency indicators on the life cycle stages and descriptions of research results.

Assessment of conformity of the selected indicator current values, the desired level and justify the selection of the indicator measurement scale.

Conceptual modelling of confidentiality subsystem functioning process in the information system.

Decomposition of the confidentiality study purpose.

Definition of an external supplement for system-technical research.

The purpose of engineering research:

Statement of the task of system-technical research regarding the problem of the information confidentiality ensuring.

The formation of a complex system and technical strategies of building a privacy protection subsystem

Analysis of engineering characteristics of the privacy protection subsystem (SPP).

Assessment of structural and functional redundancy.

To provide a choice of means and methods of engineering modelling of processes of information security (of the information security processes engineering).

To justify the set of initial data, clarifying their limitations and efficiency.

To ensure the processes of the confidentiality protection system engineering.

The purpose of the CI detailed studies:

1. To ensure the work statement for the Confidentiality of detailed research.

2. To specification, external additions resulted from the Confidentiality engineering research.

3. To ensure the selection of performance indicators and sustainable solution criterion for SPP elements construction.

The procedure for the development of solutions to protect information confidentiality.

When formulating the general procedure for a solution development aimed to ensure the information confidentiality as well as for its further improvement it is necessary to follow the principles of complex systems multi-level synthesis, specified in [1, 2, 6, 10, 11], taking into account the information security peculiarities:

The principle of decomposition is to split the system into parts.

The principle of system modelling and the processes of its functioning.

The principle of levels harmonization.

The principle of external additions. The validation of research results obtained at each level is carried out using the models and methods listed above in the hierarchy of systems.

The principle of the field-proven methodological support. It is necessary for the research to use experimentally tested models and methods to make sure the model is adequate to the process researched and to obtain reliable results.

III. General characteristics of the model

The single layer model (method) allows determining the relationship between output and internal variables under the given selection conditions of the input variables at appropriate levels research privacy.

$$y_i = F_i(u_i, g_i, \lambda_i), \quad (1)$$

where:

y_i - is the output value characterizing the CI at the *i-th* level of the study;

F_i is a model of the SPP at the *i-th* level of research in the form of a certain set of techniques that allow u_i, g_i, λ_i to be displayed in the value of y_i or (and) to calculate the value of y_i;

u_i - the values of the input variables that characterize the external addition at the *i-th* level of the study;

g_i - the value of the internal variables characterizing the SPP in the ISS at the *i-th* level of the study;

λ_i - a variant of internal variables choice, which corresponds to the option of constructing an SPP as part of the ISS at the *i-th* level of the study.

Multilevel models (methods) allow determining the connection between the *i-th* level choice parameters and values of outcome variables of the following *(i+1)* level.

$$y_{i+1} = F_{i+1}(u_{i+1}, u_i, g_{i+1}, \lambda_i, \lambda_{i+1}), \quad (2)$$

Where:

y_{i+1} is the value of the output variable characterizing the CI at the *(i + 1)-th* level;

F_{i+1} - the model of the SPP as part of the ISS on the *(i+1)* level of the research in the form of some functional, the techniques allowing to display (u_{i+1}, u_i, g_{i+1}, λ_i, λ_{i+1})$_i$ in the value y_{i+1} or (and) calculate the value of y_{i+1};

u_{i+1}, u_i - the values of the input variables that represent the outer complement at the *i-th* and *(i+1)-th* levels of the investigation;

g_{i+1} - the values of the internal variables characterizing the CI in the ISS at the *(i+1)-th* level of the study;

λ_i, λ_{i+1} - *the* values of the internal variables characterizing the CI in *i-th* at the *(i+1)-th* level of the study.

The criterion for selecting internal variables defines the set of values of the internal variables $G^*_1 \subset G_1$, which satisfies the requirements imposed on the output variables at the corresponding level $g_1 \subset G_1^*$.

The choice of criterion depends on the purpose.

For the criterion of the suitability of $g_i \geq g_0$ and a scalar metric g_i region G_1^* is poll interval $[g^0, \infty)$.

For the optimality criterion $g_i \rightarrow max$ the domain degenerates to a point corresponding to the maximum value of internal variables selection parameters and given selection conditions λ_i, λ_{i+1}.

IV. GENERALIZED PROCEDURE OF MULTI-LEVEL SYNTHESIS

Taking into account the accepted notation and the above principles, we propose the following generalized multi-level synthesis procedure, as well as how to use it [11]:

formulation and decomposition of the objective function;

choice of the list of input, internal and output variables, private methods and methods of different levels;

definition of the conditions for the selection of internal variables values showing an indirect influence of the external environment;

to evaluate the possibility of integration with other private methods;

the need to use multilevel algorithms as well as to define constraints for variable values;

the choice of efficiency criterion that determines the order of selection effective concept engine protect privacy.

The modelling of the process for application of the confidentiality protection subsystem is the part of the information protection system as an element and forecasting of the ranges of $Y^* \in Y_i$ output variables values, characterizing the subsystem development concept and meeting system requirements and their limitations λ_i.

$$g_i = F_i(u_i, y_i, \lambda_i) \subset G_i^*, \quad (3)$$

where

$F_i(u_i, y_i, \lambda_i)$ - a function that allows calculating the value of the CI indicator at the *i-th* level;

$G_1^* \subset G_1$ - the selection criterion in accordance with the accepted preference. If $Y_1^* \not\subset Y_1$, then it is necessary to clarify the concept of constructing the SPP as part of the ISS, to adjust the accepted constraints λ_1 and repeat the definition of Y_1^*;

Y^* - the required value of the CI indicator, which is specified by the IS as an external addition;

Y_i - the value of the CI indicator in the choice of the *i-th* alternative to constructing the SPP as part of the ISS;

If the set Y_1^* satisfying the condition $Y^* \subset Y_1$ is empty, $Y_1^* = \varnothing$, then the assertion about the non-feasibility of the ISS development concept in terms of providing CI with the specified requirements from the IS side is accepted;

forecasting the possibility of achieving the required values of the output variables Y_1*, using the existing functional and physical structure of the ISS and determining the need for its improvement.

For this purpose, using the inter-layer dependencies F_{12} the region G_2^* of the required values of g_2 satisfying the condition:

$$y_1 = F_{12}(g_2, u_1, u_2, \lambda_1, \lambda_2) \subset Y_1^*, \quad (4)$$

and the condition $G_2^* \subset G_2$ is verified. If $G_2^* \not\subset G_2$, then it is necessary to return to the previous level, make changes to the concept of the SPP development as part of the ISS, make corrections to the constraints, and repeat the definition of the region Y_1^* and verify the feasibility of g_2.

The iterations are repeated until the condition $G_2^* \subset G_2$, is fulfilled, after which a set of G_2^* values are fixed and a transition to the next lower level occurs.

A similar procedure is repeated for each of the levels until the required characteristics of the SPP in the ISS are determined.

With a multi-level conceptual study of the system, the guiding principle is the principle of minimum costs.

The sufficient results principle is realized in case of selecting the sufficiency criterion and development of models fan of SPP elements being a part of ISS and a link between. This allows choosing a constructive solution at each level of SPP concept development. In accordance with the general task formulation it is possible to write down the condition for choosing SPP construction effective concept as a part of ISS.

In accordance with the general formulation, of the problem, it is possible to write down the condition for choosing an effective concept of SPP constructing as part of the ISS:

$$\begin{gathered} C(\Delta y) \to \min, \\ g_m(\lambda, y) = g_m(\lambda, y_0) + \Delta g_m(\lambda, y_0, \Delta y) \geq g_m^o, \\ y \in Y, \end{gathered} \quad (5)$$

where Δg_m is the predicted increment in the effective index of the SPP as part of the ISS.

In the event that feasible assumptions on monotonicity increasing function $C(\Delta y)$ and $\Delta g_m(\Delta y)$, the solution of the problem must be sought on the borders of inequality $g_m(y) \geq g_m{}^0$ by sequentially increasing the values of the relevant variables.

In this case, a rational sequence of levels (stages) improvement of ISS will be determined using the following ratios:

$$\Delta y_1=0,\ C_1(0)=0,\ \Delta g_{m1}(0)=0,$$
$$\Delta y_2=0,\ C_2(\Delta y_2)=0,\ \Delta g_{m2}(\Delta y_2)>0,$$
$$\Delta y_3=0,\ C_3(\Delta y_3)=0,\ \Delta g_{m3}(\Delta y_3)=\Delta,$$
$$\Delta y_4=0,\ C_4(\Delta y_4)>C_3(\Delta y_3),\ \Delta g_{m4}(\Delta y_4)=\Delta,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\Delta y_n=0,\ C_n(\Delta y_n)>C_3(\Delta y_{n-1}),\ \Delta g_{mn}(\Delta y_n)=\Delta. \quad (6)$$

In accordance with the above relations:

at the first level, the compliance of the characteristics of the existing SPP in the ISS with the requirements imposed by the IS is checked;

on the second one only those characteristics that do not require additional resources are improved;

at the third one and subsequent levels, the characteristics are improved using external resources.

Moreover, the distribution of changes in internal variables and resources is carried out in such a way as to ensure the same increment in the performance indicators $\Delta g_m(\Delta y_k)=\Delta$, $k=3,4, \ldots, n$ increase in the increment of costs when moving to the next level, i.e. $C(\Delta y_k) > C(\Delta y_{k-1})$, $k=4, 5, \ldots,n$.

The solution ends at the *i-th* level when the condition is fulfilled:

$$g_m(y_i,\lambda)=g_m(y_0,\lambda)+\sum_{i=1}^{j}\Delta g_{mi}\geq g_m^0,$$
$$g_m(y_{j-1},\lambda)=g_m(y_0,\lambda)+\sum_{i=1}^{j-1}\Delta g_{mi}<g_m^0. \quad (7)$$

This approach to the justification of the concept of the design and development of the SPP (SPP design and development concept) as part of the ISS will ensure minimum or near-minimum costs for building and further ISS improvement in terms of providing the required level of CI.

Indeed if the process ends at levels 1 and 2, and the solution is found at the third and subsequent levels, then the costs of $C(\Delta y)=0$ will be minimal compared to another sequence of levels providing the same increment of a performance indicator.

We can distinguish the following generalized levels of ISS improvement [6]: initial, organizational, additional resources.

Level of SPP concept development as a part of ISS:

$$\text{source: } g_m(y_0,\lambda)\geq g_m^0,\ y_1=y_0,\ C_1=0; \quad (8)$$

$$\text{organizational: } g_m(y_2,)\ gm^0,\ y_2=y_0,\ C_1=0; \quad (9)$$

additional resources: $C(\Delta y_3)\rightarrow min$ или $C(\Delta y_3)\leq C^0$, (10)

CONCLUSION

Thus for an empiric study of the information sensitivity processes and practical application of the results received it is necessary to follow the multilevel synthesis of complex systems, adapted to features of construction of personal data protection subsystem.

The results are accepted for implementation as part of a project to develop an educational and methodological complex for organizing a practical audit. This project has been applied at the National Research University of Electronic Technology [12].

This article presents the general strategy of the empiric study. In fact the transition from models (1), (2), (3), (4), (5), (6), (7), (8). (9), (10) to model of a specific operation, i.e. the construction of a mathematical or other formal model is very complex and time-consuming. This is particularly evident when the target of research is under the design, development, application or re-engineering the author keeps working on these tasks.

Confirmation

The work is done in the framework of the task of justification of the annual budget on information security of the Department "Information "Information security".

References

ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems — Requirements (IDT).

ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements (IDT).

Volkova V. N., Voronkov V. A. and Denisov A.A. System theory and systems analysis methods in management and communication. − M.: Radio and communication. − 1983.

Romanov V. N. The technique of the analysis of complex systems. − SPb.: SZTU 2011.

Ovchinnikov V. A. The graphs in problems of analysis and synthesis of structures of difficult systems / V. A. Ovchinnikov. − M.: MGTU N. E. Bauman, 2014.

Larin A. A. Theoretical bases of management. Part I. Processes, systems and control. M.: RVSN, 1998.

Mesarovic, M. D. Macko and Y. Takahara. Theory of Hierarchical Multilevel Systems. Academic Press, New York and London, 1970. pp. 4-34, 34 -63.

Khokhlachov E. N. The theoretical foundations of management. Part 2. Analysis and synthesis of control systems. – M.: RVSN, 1996.

G. J. Klir, Architecture of Systems Problem Solving. Springer Science+Business Media New York, 1985, pp. 1-29, 175-293, 417-468.

Utkin L.V. Risk analysis and decision making with incomplete information. SPb.: Science 2007, 404 p.

Reliability and efficiency in technique. Reference guide in 10 volumes: vol. 3. The effectiveness of technical systems./ Under the General editorship of V. V. Utkin, Y. V. Kryuchkova. M.: Mechanical engineering, 1988.

Associate Professor Voevodin V.A., Igoshin V.V., Makoveev K.D. and Makhaylovskaya A.S. About APCS public key infrastructure unauthorized access information security audit program. – M.: Processing of the international Conference REDS-2018 Radio-electronic devices and systems for information and communication technologies, 2018. pp. 318 -322.