Managing the Process of Ensuring Information Security based on the Law of «Preserving the Integrity of the Object»

Daria A. Ukraintseva[a], Vyacheslav G. Burlov[b] and Vitaly V. Gryzunov[c]
Russian State Hydrometeorological University (RSHU), 3 Metallists Av, St. Petersburg, Russia

Keywords: Information Security, Solution Model, Inverse Problem, Law of Integrity Preservation, Synthesis, Firewall.

Abstract: Information security management requires forming processes with predefined properties. However, analysis-based models are usually used for management. This requires solving a direct management problem. And its solution does not allow us to fully meet the formulated requirements. The article presents a management concept based on synthesis, which already allows us to meet these requirements more fully. The new approach is based on solving the inverse control problem. The solution of the inverse control problem allows you to create conditions for the application of methods and models of program-target control. The result is the creation of a mathematical model of managerial decisions. The concept of synthesis-based management is presented.

1 INTRODUCTION

Not having the methodological foundations of solving problems of Information security in the form of the conditions of the existence of a process, we cannot guarantee the achievement of the goal of the activity. This situation gave rise to a fundamental problem: "The results of the activity for solving problems of Information security do not meet the expectations of the decision-maker." The decision-maker acts on the basis of three categories. This is System. Model (Andreev et al., 2019). Purpose. Therefore, it is necessary to solve two problems. Problem 1. For the development of the system two approaches are known. The development of the system based on analysis. The development of the system based on synthesis. To solve problem 1 offers to use for the synthesis - the law of conservation of the object's integrity (hereinafter - LCIO), which provides the achievement of the goal of Information security. (LCIO is a stable, objective, repetitive connection of an object's properties and the properties of its actions for a fixed purpose.) Problem 2. The decision-maker carries out Information security on the basis of the model. To do this one must be able to synthesize adequate models. Therefore the author offers to use LCIO for evaluating the adequacy of the model. The decision-maker carries out Information security on the basis of the model. To do this one must be able to synthesize adequate models. Therefore the author offers to use LCIO for evaluating the adequacy of the model. Achieving the goal of information security is possible only on the basis of a properly constructed system (PCS) and adequate model. The criterion of PCS is the use of LCIO for its synthesis. In the prior art publications, this approach to information security is absent. Therefore all the construction of PCS is realized on the basis of LCIO which confirms the appropriateness of considering LCIO as a condition for the existence of Information security. To demonstrate the potential possibilities of the suggested methodology of information security there has been developed the analytic, dynamic model. Model of information security is based on the system integration of three processes. The formation of the threat. The process of recognition of the threat. The process of eliminating the threat. The level of information security is estimated probability that each threat is detected and eliminated. The simulation results confirmed the main trends in the process of information security.

[a] https://orcid.org/0000-0001-6769-5669
[b] https://orcid.org/0000-0001-7603-9786
[c] https://orcid.org/0000-0003-4866-217X

Ukraintseva, D., Burlov, V. and Gryzunov, V.
Managing the Process of Ensuring Information Security based on the Law of «Preserving the Integrity of the Object».
DOI: 10.5220/0010619500003170
In *Proceedings of the International Scientific and Practical Conference on Computer and Information Security (INFSEC 2021)*, pages 116-121
ISBN: 978-989-758-531-9; ISSN: 2184-9862

Also, to ensure the achievement of the goal of ensuring information security, a natural scientific approach (hereinafter referred to as the NSA) should be used (Burlov, 2018). The NSA is implemented through three main principles:

- the principle of three-component cognition;
- the principle of the integrity of the world (implemented through the LCIO);
- the principle of the cognizability of the world (Burlov, 2018).

The principle of three-component cognition consists in the fact that a person, consciously or not, develops a solution in three levels of representation of the situation.

2 BASIC INFORMATION

Based on this, in the case of normal operation of the information security system, a person operates with the categories «object», «action» and «purpose». It is also important to note that these components are interpreted in three levels of cognition – abstract, abstract-concrete, and concrete. These statements form the structure of the concept of «management decision».

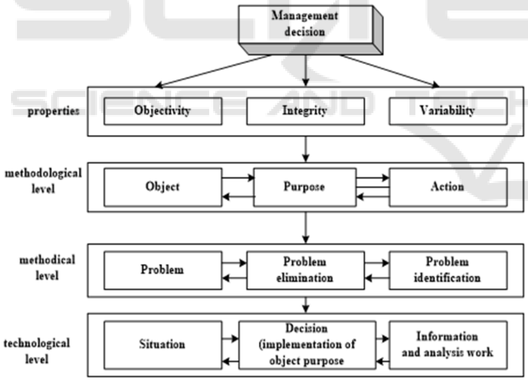

Figure 1: Block diagram of the deployment of the content of the concept of " management decision».

There is a condition for the existence of an information security management process. This characteristic is the time required to predict the characteristics of the system. A graphic illustration of the process is shown in Figure 2.

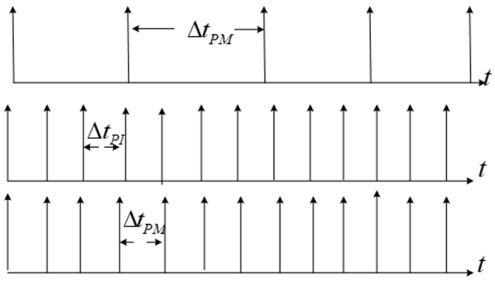

Figure 2: Diagram of manifestation of the basic elements of the decision model.

The diagram shows that a person learns the world through three basic properties. This is objectivity, integrity, and variability. The LPR works with the "process" category. Therefore, the decision is presented at the methodological level as a process in the form of interrelated components "object", "action", "purpose". At the methodological level," object "corresponds to "problem". "Action" corresponds to "identification of the problem", because "identification" is based on the identification of the fact of the manifestation of energy. "Purpose" corresponds to "neutralizing the problem". Since neutralization is possible only if the results of the "identification" match the essence of the "problem". This confirms the fact of identifying cause-and-effect relationships. At the technological level, the "solution" as a" process " is represented as a connection of three components. This is the "situation", "information and analytical work", "solution" (a condition for the implementation of the control object) (Burlov and Popov, 2017).

Having presented the " solution "in the form of a connection of the three components considered, we proceed to the development of a structural scheme for the deployment of the content of the synthesis process of the mathematical model of the «solution».

Figure 3 shows a block diagram of the deployment of the content of the synthesis process of an adequate mathematical model of the "Solution". To synthesize the model, we apply the methods of decomposition, abstraction, and aggregation. Using the decomposition method, we present the solution in the form of three interrelated components. This is the setting. Information and analytical work. Decision. The basis of such a relationship is the LCIO (Burlov et al., 2018). Using the abstraction method, we form three elements corresponding to the elements obtained from the decomposition.

In this paper, in order to use the method of decomposition, abstraction and aggregation, it is necessary to transform the concept of "management decision" into an aggregate-a mathematical model of a management decision of the following type:

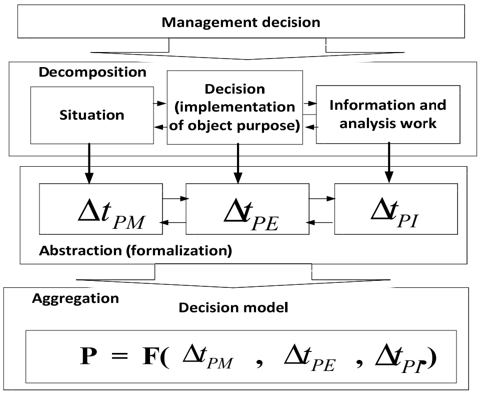
Management decision
Decomposition
Situation
Decision (implementation of object purpose)
Information and analysis work
Δt_{PM}
Δt_{PE}
Δt_{PI}
Abstraction (formalization)
Aggregation
Decision model
P = F(Δt_{PM} , Δt_{PE} , Δt_{PI})

Figure 3: Block diagram of content of synthesis of the mathematical decision model.

$$P = F(\Delta t_{PM}, \Delta t_{PE}, \Delta t_{PI}) \qquad (1)$$

The above mathematical model is a condition for the existence of the information security management process.

3 RESULTS AND DISCUSSION

When implementing this approach, a system of Kolmogorov – Champen differential equations should be developed (Burlov, Grobitski, and Grobitskaya, 2016). In this regard, we will make a characteristic of the system transitions in Figure 4.

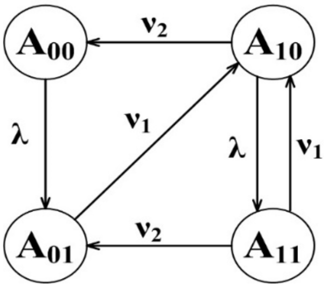

Figure 4: Graph of states, the process of forming a management decision.

In the process of performing the activity, it performs a certain order of actions, which can be carried out with sufficient information support, as well as with certain capabilities. Based on this, the security system is in four basic states:

- state «A_{00}»;
- state «A_{01}»;
- state «A_{10}»;
- state «A_{11}».

The «A_{00}» state is an initial situation that does not require any further actions. During the activity, it switches to the «A_{01}» state during the Δt_{PM}. State «A_{01}» - the situation in which the system is located after identifying and neutralizing the problem, Δt_{PM} the average time of implementation of the destination.

As a result of the destructive impact of the environment, there are two types of threats:

- regular ones, in which already worked-out scenarios are executed;
- non-standard ones that cause problems.

It is in an emergency situation that the system will be in the «A_{10}» state.

State «A_{10}» - a situation in which threats appear in the control system. State «A_{11}» - a situation in which a threat is identified that needs to be resolved by the security management. After that, the system goes to the «A_{01}» state, if it successfully solves the problems with an acceptable amount of time, or a failure occurs, and it returns to the «A_{00}» state.

In the «A_{01}» state, two situations can occur:

- the system has spent too much time, which is equivalent to the failure of the target task of the management process;
- the system has spent the allowed amount of time.

I will consider the process of changing states using the example of an information security tool – a firewall. Firewalls is a type of network device in hardware and software implementation, used to control access between trusted networks and untrusted networks based on pre - configured rules. Most firewalls are located on the edge of the network perimeter, and they are primarily designed to protect internal hosts from external attacks. Thus, to describe the process of changing states on the graph, it is necessary to make the following assumptions and assumptions.

During the transition from one state to another, the average time and frequency are determined:

Δt_{PM} the average time of the problem, and λ is the frequency of the problem:

$$\lambda = \frac{1}{\Delta t_{PM}} \qquad (2)$$

Δt_{PI} – average time to identify the problem, ν1 is the frequency of identification of the problem:

$$\nu_1 = \frac{1}{\Delta t_{PI}} \qquad (3)$$

Δt_{PE} – average time of neutralizing the problem, ν2 frequency of neutralizing the problem:

$$\nu_2 = \frac{1}{\Delta t_{PE}} \qquad (4)$$

ζ^{+}– frequency realization of the destination system:

$$\zeta^{+} = \frac{1}{\Delta t_{PE}} \tag{5}$$

ζ^{-}- frequency breakdown of the system «firewall».

1. The scheme of forming a human decision in the form of an information and control system is considered. In this regard, a security process is being created.

2. The time intervals between the detection of attacks that cause problems are random variables.

3. The detected attacks in time form a flow that is close to the Poisson flow.

4. The processing time of the required data stream is random.

5. Data on signs of unauthorized access will be further distributed among the allocated resources that correspond to the goals of ensuring information security.

6. The case is considered when the time of stay of the required facts in the area of operation of the information system is very limited and is proportional to the time required for their identification, as well as for data processing and corresponding actions based on these facts.

7. The information system is ready to solve problems of recognition and neutralization of problems.

8. The system under development (human solution - firewall) is designed to assess the potential capabilities of the information security system, depending on the situation.

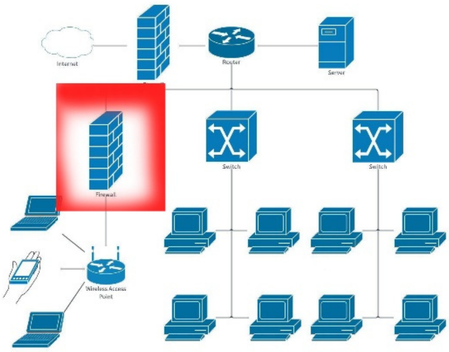

Figure 5: Firewall operation diagram.

A model establishing a correlation between these four processes and the facility performance indicator can be developed now. In this case, the facility performance indicator is equivalent to the probability of identification and neutralization of each security threat.

The Kolmogorov equations can be used:

$$\begin{cases} \frac{d}{dt}P_{00}(t) = -P_{00}(t)\lambda + P_{01}(t)\nu_2 \\ \frac{d}{dt}P_{01}(t) = -P_{01}(t)(\lambda+\nu_2) + P_{11}(t)\nu_1 + P_{10}(t)\nu_1 \\ \frac{d}{dt}P_{10}(t) = P_{00}(t)\lambda - P_{10}(t)\nu_1 + P_{11}(t)\nu_2 \\ \frac{d}{dt}P_{11}(t) = P_{01}(t)\lambda - P_{11}(t)(\nu_1+\nu_2) \end{cases}$$

Nonzero probabilities of occurrence can be calculated by solving a system of linear algebraic equations derived from the Kolmogorov equations, if the derivatives are equal to zero, and the probability functions of states $P_1(t)$, ..., $P_n(t)$in the right part of the equations pass into the unknown finite probabilities P_1 , ..., P_n.. To find the value of P_1 , ..., P_n , a normalizing condition is added to the equations $P_0 + P_1 + \cdots + P_n = 1$ .This system will be solved for the given initial conditions.

Let us assume that the process is stationary, in which case the initial system of differential equation is transformed into a system of linear homogeneous algebraic equations of the following form:

$$\begin{cases} -P_{00}(t)\lambda + P_{01}(t)\nu_2 = 0 \\ -P_{01}(t)(\lambda+\nu_2) + P_{11}(t)\nu_1 + P_{10}(t)\nu_1 = 0 \\ P_{00}(t)\lambda - P_{10}(t)\nu_1 + P_{11}(t)\nu_2 = 0 \\ P_{01}(t)\lambda - P_{11}(t)(\nu_1+\nu_2) = 0 \\ P_{00}(t) + P_{01}(t) + P_{10}(t) + P_{11}(t) = 1 \end{cases}$$

The above system is a system of linear algebraic equations with respect to the four unknowns P_{00}, P_{10}, P_{01}, P_{11}, which are related by the following relation. The probabilities we are looking for do not depend in time (Anokhin, 1979). The solution of this linear algebraic system of equations is the following relations:

$$P_{00} = \frac{\nu_1\nu_2}{\lambda(\lambda+\nu_1+\nu_2)+\nu_1\nu_2}$$

$$P_{10} = \frac{\lambda\nu_2(\lambda+\nu_1+\nu_2)}{(\nu_1+\nu_2)[\lambda(\lambda+\nu_1+\nu_2)+\nu_1\nu_2]}$$

$$P_{01} = \frac{\lambda\nu_1}{\lambda(\lambda+\nu_1+\nu_2)+\nu_1\nu_2}$$

$$P_{11} = \frac{\lambda\nu_1}{(\nu_1+\nu_2)[(\lambda+\nu_1+\nu_2)+\nu_1\nu_2]}$$

The most significant for the process of ensuring information security is. It relates three parameters (λ, υ1, υ2) and determines the probability of neutralizing and identifying the problem. It is also a system-forming factor in the creation of an information security management system.

The synthesis-based approach allows us to solve inverse problems. To achieve the required indicator of the effectiveness of the security system, measures should be developed to establish the necessary values for the indicators of the appearance, identification, neutralization of the problem and the qualification of the manager.

4 CONCLUSIONS

The resulting management decision model allows us to quantify the performance of the firewall and information security in general. As a result, it is necessary to control the control by setting the level of the safety indicator and the frequency of failures, in order to obtain the necessary values for the time of identification and neutralization of the problem. Based on the data obtained, the information security plan can be adjusted in the future.

Without a doubt, a firewall is one of the main security tools, but its presence alone cannot guarantee complete security. Firewall settings should be tailored to your needs, taking into account your threats, risks, and IT infrastructure. You should also constantly check the operation of the firewall and document all actions so that the firewall protects you as effectively as possible.

The developed model is based on the NSA and LCIO, therefore, meet the requirement of adequacy (Burlov, 2017.). On its basis, it is possible to develop a technology for ensuring information security.

The information security model is based on the system integration of three processes. Threat formation. The process of recognizing the threat. The process of eliminating the threat. The level of information security is assessed by the probability that each threat will be detected and eliminated. The results of the simulation confirmed the main trends in the process of ensuring information security. The new concept of ensuring information security, in contrast to the known ones, allows you to create conditions for ensuring information security according to the developed model. The use of LCIO allows the decision-maker to form processes with predefined properties. This reduces the level of risk when achieving the goal of ensuring information security.

The proposed mathematical apparatus allows you to build a mathematical model of a management decision and on the basis of this link the three most important processes in the organization of security. Due to this mathematical model, security is ensured. The use of a synthesis-based modelling approach makes it possible to build such a system as a system for managing the process of ensuring the safety of work in the face of threats of emergency situations based on the required level of the efficiency indicator. Accordingly, a system built on such principles will be devoid of the main drawback – the discrepancy between the management results and expectations. This approach allows you to evaluate any decision made from the perspective of time and resource costs, as well as to establish a clear, scientifically based relationship between the decision made and the results of the action.

ACKNOWLEDGEMENTS

The reported study was funded by Russian Ministry of Science (information security), project № 08/2020.

REFERENCES

Abramov, V.M., Burlov, V.G. and Tatarnikova, T.M. (2021). Digital Technologies Development for Geo-Information Support of Techno-Sphere Security in Arctic and Subarctic. *IOP Conference Series: Earth and Environmental Science,* 666(5): 052076

Andreev, A.V., Burlov, V.G. and Grachev, M.I. (2019). Information technologies and synthesis of the management process model in the enterprise. *2019 International Science and Technology Conference "EastConf"*, 8725428

Anokhin, P. K. (1979). *System mechanisms of higher nervous activity*, M.: Science, p. 453.

Burlov V.G. and Popov N.N. (2017). Management of the application of the space geoinformation system in the interests of ensuring the environmental safety of the region. *Advances in the Astronautical Sciences*, pages 751-760.

Burlov V.G., Abramov V.M., Istomin E.P., Fokicheva A.A. and Sokolov A.G. (2018). The methodological basis for the strategic management of territory development. *18th International Multidisciplinary Scientific GeoConferences SGEM 2018. Conference proceedings*, pages 483-490.

Burlov, V. G. (2017). *The law of preserving the integrity of the object - the method of the basis for solving the problems of information warfare and ensuring security. Neurocomputers and their applications*, pages 261-263.

Burlov, V. G., Andreev, A. V. and Gomazov, F. A. (2018). *Safety management of a technosphere object based on the law of preserving the integrity of the object.* Federal State Budgetary Educational Institution of Higher Education "St. Petersburg State University of Economics (SPbSEU)", pages 56-60.

Burlov, V. G., Andreev, A. V. and Gomazov, F. A. (2018). *Safety management of a technosphere object based on the law of preserving the integrity of the object.* Federal State Budgetary Educational Institution of Higher

Education "St. Petersburg State University of Economics (SPbSEU)", pages 56-60.

Burlov, V., Andreev, A. and Gomazov, F. (2018). Development of a model for the management of environmental safety of the region, taking into account of the GIS capacity. *MATEC Web of Conferences*, 193, 02038

Burlov, V., Andreev, A., Gomazov, F., Somga-Bichoga, N. (2018). System integration of security maintenance processes in knowledge management. *Proceedings of the European Conference on Knowledge Management*, 1, pages 112–122.

Burlov, V., Lepeshkin, O. and Lepeshkin, M. (2020). *IOP Conference Series: Materials Science and Engineering*, 918(1): 012224.

Burlov, V.G. and Gryzunov, V.V. (2020). Evaluation of the effectiveness of geographic information systems adaptation to destabilizing factors. *Journal of Physics: Conference Series*, 1703(1): 012016.

Burlov, V.G., Andreev, A.V. and Gomazov, F.A. (2018). Mathematical model of human decision - a methodological basis for the realization of the human factor in safety management. *Procedia Computer Science*, 145: 112-117.

Burlov, V.G., Grobitski, A.M. and Grobitskaya, A.M. (2016). Construction management in terms of indicator of the successfully fulfilled production task. *Magazine of Civil Engineering*, 63(3): 77–91.

Goode, H.H. and Machol, R.E. (1957). *System Engineering: An Introduction to the Design of Large-Scale Systems New York*: McGraw-Hill Book Co p. 551.

Mitrofanova, E.A., Simonova, M.V. and Tarasenko, V.V. (2020). Potential of the education system in russia in training staff for the digital economy. *Advances in Intelligent Systems and Computing*, 908: 463-472.

Perova, M.V. (1999). *Quality of rural electricity supply: an integrated approach*, Vologda: Vologodskij GTU p. 72.

Polyukhovich, M., Burlov, V., Mankov, V. and Bekbayev, A. (2019). Electric power supply management of the construction site in the interests of facilitating electrical safety. In: *2019 International Scientific Conference on Energy, Environmental and Construction Engineering, Congress Center of Peter the Great St. Petersburg Polytechnic University*, Saint-Petersburg, Russia.

Sokolov, S. S., Alimov, O. M., Golubeva, M. G., Burlov, V. G. and Vikhrov, N. M. (2018). The automating process of information security management. *2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, pages 124-127.

Yakovlev, V.B. and Rastorguev, M.V. (2007). Analysis of efficiency of functioning of rural distributive electric networks. *Vestnik RGAZU*, 3: 122-124.