The control model of safety management systems

V G. Burlov, O M Lepeshkin, M O Lepeshkin and F A Gomazov
Peter the Great St.Petersburg Polytechnic University, St.Petersburg, Russia
E-mail: burlovg@mail.ru, fgomazov@gmail.com

Abstract. This article presents a control model of security management systems from destructive software and hardware effects. Considered descriptive and analytical control model of security, presents the structural and logical scheme of a control model of security management systems from destructive software and hardware effects, carrying out the search and elimination of conflicts, associated with the logical inconsistency of the structure of the control system, and conflicts associated with ongoing processes, i.e. with the fulfillment of the tasks of the regulations, operating in the system. It is proposed to realize the model, using the language of radical schemes, based on the stand for providing integrated developments. The model integrates with mathematical means of searching, predicting and eliminating conflicting schemes in the system.

1. Introduction
The impact on information is determined by the results of an evaluation of the capabilities (capacity, equipment and motivation) of external and internal violators, analysis of possible vulnerabilities of the information system, possible ways to implement threats to information safety and the consequences of violation of the properties of information safety (confidentiality, integrity, accessibility).

When determining the threats to information safety, it is necessary to take into account the structural and functional characteristics of the information system, the information technologies used and the characteristics (conditions) of the functioning of the information system. Consequently, the effectiveness of measures taken to protection information depends on the quality of the definition of threats to information safety for a specific information system in the specific conditions of its operation.

Modern management systems must respond promptly to destructive software and hardware effects, both external attacks and internal malicious effects, while preserving their accessibility, reliability and efficiency. In many ways, the purpose of the safety process is to increase network resiliency. Instead of becoming "victims" of unauthorized impacts, networks should be able to "absorb" attacks and remain operational [1-5,7].

Destructive effects on management systems can occur in many ways and can differ from each other. It can also be attacks on the infrastructure, computer network, the denial of services in order to disrupt their normal functioning [6, 8-12].

Any software or hardware is not perfect, and you can always assume, that there are vulnerabilities in it, that allow you to perform any actions, that violate the established order of resources use. In addition, reacting to unauthorized activity or attempts to hack the system in near real-time mode is almost impossible, if these functions are performed manually [13-15].
At the present stage of development of safety systems in management systems the task of developing control of security becomes more urgent, which should ensure detection of destructive effects on the communication network in a time close to real mode [2, 16-18].

To ensure compliance with the safety, requirements for management systems, they need to be represented as a complex system using object-oriented design tools.

2. Structure of the control model of the security of management systems from destructive software and hardware effects

Increasing the security of management systems (MS), it is proposed to make by realizing a process approach, that involves control the logical (regulatory) condition of the system. This can be achieved by registering the current condition of the MS and the processes, implemented by the system; simulation of software and hardware effects, or processes with simultaneous collection and processing of data on the compliance of system characteristics (system parameters) with set requirements, for the goal of identifying vulnerabilities and evaluating security; visualization of the composition, structure and process of the functioning of the system (established segments, fragments, elements); verification of the set condition and the regulations of the functioning of the elements of the system that ensure safety (their compliance with specified protection profiles and regulations) [3, 17-22].

To be able to monitor the logical (regulatory) condition of a MS necessary to develop a control model their security from destructive software and hardware effects, which allows to identify information conflicts (logical inconsistency, vulnerability of the system, violation of the integrity of the process). The tasks, associated with ensuring logical consistency of information processes, also accessibility of MS services can be solved by searching for conflicting schemes in the environment of radicals and their elimination.

2.1. Verbal control model of security management systems from destructive software and hardware effects

The basis of the construction of the MS control system should be laid formalized set of information processes, the structure of which must be developed by mapping the MS in the environment of radicals.

At this stage, the model must solve the problems of searching and eliminating conflicts, associated with the logical inconsistency of structure MS regulations.

At this stage, the model solve tasks of search and resolve conflicts, associated with to the logical inconsistency of structure regulations MS. When functioning in a MS, in the process of execution regulations arise conflicts, associated with the execution of processes (transactional tasks of regulations, operating in the system). The task model is the early detection and elimination of conflicts [4].

From these statements it follows, that the model of the MS must operate in two modes - static and dynamic, realization the solution of tasks of control at each stage of operation of the system.

The order of the functioning of the control model of security MS can be determined in the form of an oriented graph (figure 1), which includes:

**Figure 1.** Oriented graph, reflecting the order of the functioning of the control model of security MS.
- *in a static mode* - the construction of the initial description of the structure of the control system in the environment of radicals, the search and elimination of conflicts - the subgraph ABCD.

- *in a dynamic mode* - the process of searching and eliminating conflicts in the process functioning of the control system in the process implementation of regulations in force in the system - the subgraph BCDF.

The solution of task of control of security MS from destructive software and hardware effects (DSHE) is achieved by identifying and eliminating conflicts, arising in the system support in decision-making in the time mode close to real information signals about detected conflict conditions (associated with the logical inconsistency of the structure of regulations and violation of the integrity of processes (committed transactional tasks of the regulations operating in the system)).

Alignment of the conformity of the current condition and regulation of the functioning of the system to a specified security profile will facilitate with a high probability of identifying conflicting schemes, associated with the logical inconsistency of the structure of regulation and the implementation of processes (regulations), operating in the system.

Thus, the structural-logical scheme of the control model of security MS from DSHE will look like the following (figure 2)

The methodology for solving the tasks of the life cycle of a complex system based on the stands for the provision of integrated development, proposed by professor Chechkin A.V., is completely suitable for solving the tasks of control of the security MS from DSHE, because:

- firstly, it includes a formalized description of the object of control;
- secondly, it includes the means of managing conflicts arising in the process of functioning of the object of control [5, 23].

The control model of MS should be implemented in the language of radical schemes and integrated with mathematical means of searching, forecasting and eliminating conflicting schemes in the system.

In addition, the method of modeling control of MS includes two stages:

- development of a formalized description of the control system of MS, which includes the structure, properties and relationships of the MS elements, also control of MS;
- development of the activation control subsystem of MS, which implements a closed management system for the control model of MS and a formalized description of control of MS with mathematical means for searching, forecasting and eliminating information conflicts in the system.

One of the private scientific tasks is the development of mathematical means of searching and eliminating conflict schemes. Therefore, the task of realization a control model in the language of radical schemes is a formalized description of control elements of MS, also the integration of the developed mathematical means of searching and eliminating information conflicts with this model [6].

Analyzing the composition of MS, it should be noted, that they are fully implemented on the basis of information technology (IT). The equipment consists of the IT elemental base, the so-called "IT products".

The evaluation of the safety of IT products is regulated by GOST R ISO / IEC 15408 "Methods and means of ensuring safety. Criteria for evaluation the safety of information technology".

The term "IT product" is not defined unambiguously, it can be understood by any type of entity, built using IT, whether it is a complete system, used by one organization or a line of ready-to-use IT products for implementation (delivery) to different customers. As an example of an IT system, can be used for example, control means to the alienation (transfer) of information from removable computer storage media, which include the following components distributed by the components of the information system or are themselves finished products:

- specialized removable computer storage media;
- initialization software;
- management software;
- software for interaction with removable computer storage media.

Since IT products can be used in different ways and in many types of operational environments, the notion of safety will vary depending on the IT product. Therefore, the end result of the evaluation can
never be the conclusion that "this IT product is safe", instead it is argued that "this IT product complies with this safety specification".

Figure 2. Structural and logical scheme of the control model of security MS from DSHE

GOST R ISO / IEC 15408 specifies standardized specifications of safety for:
- determining the specific content required to evaluation of IT product for compliance with the safety specification;
- creating conditions for comparing the safety specifications of various IT products.

GOST R ISO / IEC 15408 defines two different types of safety specifications: protection profiles (PP) and safety tasks. The difference between them is determined by their purpose in the typical development process, the evaluation of IT product and its acquisition by the customer. The protection profile, in fact, is a document in which the customer's safety requirements are stated in a formalized, standardized form.

The results of an evaluation of IT product can be used by the asset owner when deciding whether to accept the risk, associated with the exposure of assets exposed to specific threats.

PP, as a rule, are developed by the authorized federal executive body (FSTEC of Russia), large organizations, groups of organizations, departments, etc., as their development requires considerable effort.

PP contains for use as a specification of safety "Functional requirements of safety". The goals of safety according to GOST is a short and abstract statement of the proposed solution to problem.

It is very important to understand that the goals are not the recommendations, but the necessary conditions for the functioning of the object of control (OC) according to the specification. All these goals (tasks) must be fully achieved, and the responsibility for their achievement rests with the user of the object of control or him organization (for example, the information system operator); itself the object of control will not achieve these goals. If at least one of these goals is not achieved, there may be a situation, where the object of control will functioning in an unsafe mode.

Requirements of safety are the result of converting goals s of safety for OC. They are usually presented at a more detailed level of abstraction, but they must be a full representation (goals s of
safety must be fully taken into account) and be independent of any particular technical solution (implementation).

The OC can include resources in the form of electronic data carriers (such as main memory, disk space), peripherals (such as printers), and computing capabilities (such as processor time), that can be used to process and store information and are subject evaluation.

The assessment first of all confirms, that a certain set of functional safety requirements applies to OC resources. Requirements of safety define the rules, by which the OC manages the use and access to its resources and, thus, to information and services, controlled by the OC [7, 24].

In aggregate, those parts of the OC, that are aimed at the correct realization of safety requirements, are defined as safety functions of the evaluation object. Safety functions combine the functionality of all hardware, software and hardware-software of the OC, on which as directly and as indirectly responsible for ensuring safety. In fact, the mechanisms of the safety functions mechanisms are the rules, defined in the safety requirements, and the necessary opportunities are provided.

Safety requirements are selected based on the model of common functionality opportunities of OC. In this functional model defined resources, users, subjects, objects and operations. Then the safety requirements determine the safety functionalities opportunities thus, within the framework of the functional model of the object of control, the safety goals are achieved [8].

In relation to the MS, it is proposed to consider as its safety control objects IT products its constituent elements of the equipment as its constituent parts.

Therefore, for the evaluation of security control MS it is necessary to compare with set relevant protection profile goals, requirements, safety functions and resources of the object of control, the current "stationary" system-state and "dynamic" process execution regulations of object of control.

2.2. Analytical control model of security management systems from destructive software and hardware effects.

For the formation of the initial data, characterizing the conflict situation, set the mathematical notation of the sets, that make up the model of the estimated system:

- \( C(c_1, \ldots, c_n) \) - a set goals of the security system, which should be achieved in the process functioning of the system;
- \( B(b_1, \ldots, b_m) \) - a set of security requirements, the implementation of which is necessary to achieve the set security goals of the system;
- \( D(d_1, \ldots, d_j) \) - a set of functions, the implementation of which is achieved to meet the requirements of security;
- \( R(a_1, \ldots, a_j) \) - a set tasks of the regulations, achieved in the process functioning of the system;
- \( M(m_1, \ldots, m_j) \) - a set of necessary resources to achieve the tasks of the regulations;
- \( C_s, B_s, D_s, M_s, R_s \) - goals, requirements, functions, resources and regulations set by the PP of system;
- \( C_z, B_z, D_z, M_z, R_z \) - goals, requirements, functions, resources, that determine the direct structure of the MS regulations, and regulations achieved in the system.

The first stage of compliance approvals solves the task of eliminating information conflicts, related to the structure of the MS regulations:

If \( C_s = C_z \), then there are no conflict schemes in the system, and if \( C_s \neq C_z \), then in the system there is a conflict, expressed in the absence of compliance of the stated goals with the goals, set by the corresponding PP.

Coordination of the "Goals-Requirements" is to eliminate information conflicts, associated with the lack of the possibility of achieving the stated goals due to non-compliance with the established safety requirements, and, as a consequence, the lack of integrity of the process of implementation of certain regulations.

If \( B_s = B_z \), then there are no conflicting schemes in the system, and if \( B_s \neq B_z \), then in the system there is a conflict, expressed in the absence of compliance with the requirements set by the requirements, set by the corresponding PP.
The coordination of the "Requirements -Functions" is to eliminate information conflicts, related to non-fulfillment of the requirement: for each function, the realization of which is achieved by the corresponding requirement, the functionality possibility, that implement this function must be defined.

If \( D_z = D_z \), then there are no conflict schemes in the system, and if \( D_z \neq D_z \), then in the system there is a conflict, expressed in the absence of compliance of the realization functions with the functions set by the corresponding PP [16-19].

The coordination of the "Functions -Resources" is to eliminate information conflicts, related to the uncertainty of resources for the realization of some function.

If \( M_z = M_z \), then there are no conflicting schemes in the system, and if \( M_z \neq M_z \), then in the security system there is a conflict, expressed in the discrepancy of the available resources, used to realization functions, resources set by the corresponding PP.

Let us present system set PP of the target function of a collectively sets of goals, requirements, functions and resources, necessary to ensure the security of the object of control:

\[
Q_z = f(C_z, B_z, D_z, M_z) .
\]

And the logical condition of the system goal function collectively sets the claimed goals, defined requirements, realized the functions and the resources available in the system:

\[
Q_z = f(C_z, B_z, D_z, M_z) .
\]

Then the assertion, that when \( Q_z = Q_z \) conflict schemas do not exist.

Conversely, when \( Q_z \neq Q_z \) conflict schemes are present in the system, which means, that the integrity of the logical structure of the regulations is violated, which indicates a decrease in the protection of the OC.

The regulations \( R_z \), defined PP, is a sequence of minimal logically-formalized tasks \( a_z \), set PP, meaningful and committed only fully:

\[
R_z = a_z(1) + a_z(2) + \ldots + a_z(n) = \sum_{k=1}^{n} a_z(k) .
\]

The task \( a_z \) of the regulations \( R_z \), set by PP, is the use of certain PP resources \( M_z \), at the set time \( t_z \):

\[
a_z = M_z , t_z,
\]

were \( a_z \in R_z , a_z \) - const.

When performing some tasks \( a_z(i) \) in process of implementation of regulations \( R_z \), in time \( t_{z(i)} \) with using the resources \( m_{z(i)} \), it must belong to a task sequence as performed in the process of implementation of the regulations \( R_z \), i.e. \( a_{z(i)} \in R_z \).

In this case, the task \( a_{z(i)} \) must correspond to the set PP task \( a_{z(i)} \) of regulation \( R_z \), i.e. \( a_{z, i} \in R_z \). Used in the process of making tasks \( a_{z(i)} \) resources \( m_{z(i)} \) and the time \( t_{z(i)} \) must comply with certain resources \( m_{z(i)} \) and a set time \( t_{z(i)} \), also set PP.

If \( a_{z(i)} \notin R_z \), this indicates, that there is a conflict, expressed in violation of the order of implementation of the regulations, and, as a rule, in violation of the integrity of the process of functioning of the system, which is defined by PP.

If \( m_{z(i)} \neq m_{z(i)} \), this indicates a conflict condition, associated with the uncertainty of resources to perform some task \( a_{z(i)} \) of regulations \( R_z \).

If \( t_{z(i)} > t_{z(i)} \), this indicates, that in set PP time the task \( a_{z(i)} \) of regulations \( R_z \) will not be committed, which means availability of conflict schemas and the violation of the integrity of the process of implementation of regulations.

On the basis of this control system is presented in the form of functions of levels of agreement:

\[
\begin{align*}
F_{\text{2nd eq.}} &= f(C, B); \\
F_{\text{3rd eq.}} &= f(B, D); \\
F_{\text{3rd eq.}} &= f(D, M); \\
F_{\text{2nd eq.}} &= f(F_{\text{2nd eq.}}, F_{\text{3rd eq.}}).
\end{align*}
\]
Next, made agreement the dynamic levels:

\[ F_{\text{purs.to1}} = f(M_R); \]
\[ F_{\text{purs.to2}} = f(t_R), \]

where \( M_R \) - the set of regulation resources, \( t_R \) - the regulation time;

\[ F_{\text{purs.to1'st.st.}} = f(F_{\text{purs.to1}}, F_{\text{purs.to2}}). \]

The goal function of control security of MS from destructive software and hardware effects will have the form:

\[ F_{\text{CK}} = f(F_{\text{purs.to1'st.st.}}, F_{\text{purs.to2'std.st.}}). \]

3. Conclusion

To create a control model of security management systems from destructive software and hardware effects proposed to use the concept of building a stand for complex development, which implements the solution of the tasks of complex system life cycle on the basis of two components: the model of the object under study and the means of conflict management of the object under study. The proposed model is based on the agreement of the system components (goals, requirements, functions, resources).

On the basis environment radicals and a model for the agreement of components of the system proposed to develop an activating subsystem for control security MS from destructive software and hardware effects, which realizes a closed management system model control and is able to solve the tasks of detection informational conflicts and their elimination in process of functioning of MS.

Acknowledgment

The research carried out with the financial support of the Program Competitiveness Enhancement of Peter the Great St. Petersburg Polytechnic University.

References

[1] Bolodian I, Melikhov A, Tanklevskiy L 2017 Fire safety arrangement of inhabited pressurized compartments of manned spacecraft Acta Astronautica, 135 pp 92-99 DOI: 10.1016/j.actaastro.2016.10.003
[2] Bardin A, Korotkov A, Kazarnovskij V 2017 Limit of fire resistance of a steel transport structures. Simplified calculation methods IOP Conference Series: Earth and Environmental Science, 90 (1) DOI: 10.1088/1755-1315/90/1/012207
[3] Bolgov I, Kaverzneva T, Kolesova S, Stolyarov O, Tarkhov D 2016 Neural network model of rupture conditions for elastic material sample based on measurements at static loading under different strain rates Journal of Physics: Conference Series DOI: 10.1088/1742-6596/772/1/012032
[4] Bolodian I, Melikhov A, Tanklevskiy L 2017 Fire safety arrangement of inhabited pressurized compartments of manned spacecraft Acta Astronautica, 135 pp 92-99 DOI: 10.1016/j.actaastro.2016.10.003
[5] Gravit M, Gumerova E, Bardin A, Lukinov V 2018 Increase of Fire Resistance Limits of Building Structures of Oil-and-Gas Complex Under Hydrocarbon Fire Advances in Intelligent Systems and Computing, 692 pp 818-829 DOI: 10.1007/978-3-319-70987-1_87
[6] Zybina O, Gravit M, Stein Y 2017 Influence of carbon additives on operational properties of the intumescent coatings for the fire protection of building constructions IOP Conference Series: Earth and Environmental Science 90 (1) DOI: 10.1088/1755-1315/90/1/012227
[7] Korshunov G, Polyakov S, Shumnin L 2017 Assurance of reliability and safety in liquid hydrocarbons marine transportation and storing IOP Conference Series: Earth and Environmental Science, 87 (6) DOI: 10.1088/1755-1315/87/6/062009
[8] Pykhthin K, Simankina T, Sharmanov V, Kopytova A 2017 Risk-based approach in valuation of workplace injury rate for transportation and construction industry IOP Conference Series: Earth and Environmental Science 90 (1) DOI: 10.1088/1755-1315/90/1/012065
[9] Ustinov A., Zybina O, Tanklevsky L., Lebedev V, Andreev A. 2018 Intumescent coatings with
improved properties for high-rise construction (*E3S Web of Conferences*, 33 (1), DOI: 10.1051/e3sconf/20183302039).

[10] Klokhov, Y. (2018). Conflicts between quality management methods. Paper presented at the 2017 International Conference on Infocom Technologies and Unmanned Systems: Trends and Future Directions, ICTUS 2017, January 2018, 34-36. doi:10.1109/ICTUS.2017.8285970

[11] Klokhov, Y., Gazizulina, A., Golovin, N., Glushkova, A., & Zh, S. (2018). Information model-based forecasting of technological process state. Paper presented at the 2017 International Conference on Infocom Technologies and Unmanned Systems: Trends and Future Directions, ICTUS 2017, January 709-712. doi:10.1109/ICTUS.2017.8286099

[12] Bolodian I, Melikhov A, Tanklevskiy L 2017 Fire safety arrangement of inhabited pressurized compartments of manned spacecraft Acta Astronautica, 135 pp 92-99 DOI: 10.1016/j.actaastro.2016.10.003

[13] Bataev, A. V. (2017). Questions of safety of mobile banking in russian financial institutions. Paper presented at the Proceedings of the 30th International Business Information Management Association Conference, IBIMA 2017 - Vision 2020: Sustainable Economic Development, Innovation Management, and Global Growth, January 2017, 89-99.

[14] Burlov, V., Andreev, A., & Gomazov, F. (2018). Development of a model for the management of environmental safety of the region, taking into account of the GIS capacity. Paper presented at the MATEC Web of Conferences, 193 doi:10.1051/matecconf/201819302038

[15] Burlov, V., Andreev, A., & Gomazov, F. (2018). Mathematical model of human decision - A methodological basis for the realization of the human factor in safety management. Paper presented at the Procedia Computer Science, 145 112-117. doi:10.1016/j.procs.2018.11.018

[16] Burlov, V., Andreev, A., Gomazov, F., & Somga-Bichoga, N. (2018). System integration of security maintenance processes in knowledge management. Paper presented at the Proceedings of the European Conference on Knowledge Management, ECKM, 1 112-122.

[17] Burlov, V., & Grachev, M. (2017). Development of a mathematical model of traffic safety management with account for opportunities of web technologies. Paper presented at the Transportation Research Procedia, 20 100-106. doi:10.1016/j.trpro.2017.01.023

[18] Byzov, A. P., Efremov, S. V., & Gomazov, F. A. (2018). Social and economic aspects of acceptable risk of ensuring ecological safety at management of municipal waste. Paper presented at the Proceedings of the 2018 IEEE International Conference "Management of Municipal Waste as an Important Factor of Sustainable Urban Development", WASTE 2018, 10-13. doi:10.1109/WASTE.2018.8554106

[19] Gazizulina, A., Eskina, E., Vasilieva, I., & Valeeva, O. (2017). The reasons for the increase in self-organization in companies. International Journal of Quality and Safety Engineering, 24(6) doi:10.1142/S0218539317400022

[20] Idrisova, J. I., Myasnikov, V. N., Uljanov, A. I., & Belina, N. V. (2018). Increasing the efficiency of labor protection in the enterprise. Paper presented at the International Conference on Information Networking, 2018-January 586-588. doi:10.1109/ICOIN.2018.8343186

[21] Iliashenko, O. Y., Levina, A. I., & Borremans, A. D. (2017). The approach to the formal specification of static structure of the system: Mapping UML to EXPRESS-G. Paper presented at the Proceedings of the 29th International Business Information Management Association Conference - Education Excellence and Innovation Management through Vision 2020: From Regional Development Sustainability to Global Economic Growth, 1177-1187.

[22] Ilin, I. V., Frolov, K. V., & Lepekhin, A. A. (2017). From business processes model of the company to software development: MDA business extension. Paper presented at the Proceedings of the 29th International Business Information Management Association Conference - Education Excellence and Innovation Management through Vision 2020: From Regional Development Sustainability to Global Economic Growth, 1157-1164.

[23] Savoshinsky, O. P., Zakharova, A. A., & Pak, A. V. (2018). Fire safety management in transportation of municipal wastes with the use of geographic information systems. Paper presented at the Proceedings of the 2018 IEEE International Conference "Management of Municipal Waste as an Important Factor of Sustainable Urban Development", WASTE 2018, 55-57. doi:10.1109/WASTE.2018.8554130

[24] Varlataya, S. K., Evdokimov, V. E., & Urzov, A. Y. (2017). Methods for calculating frequency of maintenance of complex information security system based on dynamics of its reliability. Paper presented at the IOP Conference Series: Materials Science and Engineering, 262(1) doi:10.1088/1757-899X/262/1/012207