UDC 621.396.2.019

DATA PROTECTION WITH INTELLECTUAL SUPPORT OF ORGANIZATIONAL AND TECHNICAL AND OPERATIONAL MANAGEMENT

Toliupa S., Parkhomenko I.
Taras Shevchenko National University of Kyiv
E-mail: tolupa@i.ua

Защита информации с интеллектуальной поддержкой организационно-технического и оперативного управления

Для успешного использования современных информационных технологий необходимо эффективно управлять не только сетью, но и системой защиты информации (СЗИ), при этом на уровне информационной системы автономно должна работать система, реализующая управление составом событий информационной безопасности, планирование модульного состава СЗИ и аудит. Учитывая, что СЗИ является весьма сложной организационно-технической системой, функционирующей в условиях неопределенности, противоречивости и неполноты знаний о состоянии информационной среды, управление такой системой должно быть основано на применении методов теории принятия решений и необходимостью применения интеллектуальных технологий.

For the successful use of modern information technologies it is necessary to effectively manage not only the network, but also information systems security (ISS), the information system on the level of the system must operate autonomously implementing the management structure of information security events, planning the composition of modular ISS and audit. ISS is a very complex organizational and technical system, which works under conditions of uncertainty, inconsistency and incompleteness of knowledge about the state of the information environment, the management of such system should be based on the use of methods of the theory of decision-making and the need for the use of intelligent technologies.

The principles of the protection of information systems should provide effective defense, and not only by criminals, but also by incompetent or poorly trained users and staff. The main challenges in implementing protection systems are that they must satisfy two groups of contradictory requirements. Prevent accidental and deliberate release of information to unauthorized users, and access control to devices and system resources for all users, administrators and staff. On the one hand, reliable protection located in the information system that the more specific terms formulated in the form of two generic tasks should be ensured. On the other hand, the protection system should not cause significant inconvenience in a work process using system resources. In particular they should be guaranteed full freedom of access for each user and the independence of his work within his rights and powers. [1]

The main direction of information protection ways research is a steady increase in the system approach to the problem of protection of the information itself. The concept of systemic is above all the sense that data protection is not only the establishment of appropriate mechanisms and is a regular process which is carried out at all stages of the life cycle of data processing systems in the integrated use of all

available security methods. At the same time all the means, methods and measures used to protect the information, and certainly the most efficient combined into a single coherent system - protection system [2].

Modern approaches to the organization of IS does not fully ensure the requirements for data protection. The main disadvantages of commonly used ISS determined by the prevailing harsh principles of construction and architecture of the application is mainly defensive strategies to protect against known threats. Critical situation in the field of information security is aggravated due to the use of the global network of internal and external electronic transactions of the enterprise and the emergence of previously unknown types of destructive information impacts.

Therefore, for the successful use of modern information technologies it is necessary to effectively manage not only the network, but also ISS, besides on the IS level system implementing the management structure of information security events, planning the composition of modular ISS and audit should work autonomously. Since the object of management - ISS is a very complex organizational and technical system functioning under conditions of uncertainty, inconsistency and incompleteness of knowledge about the state of the information environment, the management of such a system should be based on the application of systems analysis, methods of the theory of decision-making and the need for the use of intelligent technologies [3] .

One solution to this problem is to use the intelligent methods to support decision-making in the management of IS local information system, which, in turn, requires the development based on the principles of system analysis and general scientific approaches methodological framework for the protection of information management, the relevant models, methods, algorithms and software [1].

In order to implement a proactive strategy to protect in ISS the local information system substantiates the need for practically applicable models and intellectual support of rational methods of planning the modular structure of ISS, assessment and prediction of the risk of violation of information security and information security management in an uncertain information influences.

The circuit of organizational and technical management are mechanisms to protect the information management infrastructure with changing business applications, information processing plans and corresponding to the level of data protection requirements. The circuit includes: intelligent decision support for the choice of strategies to protect system security level evaluation system (risk) control action is implemented by employees of information security department. The command information is generated during the planning - targeted selection of a rational complex remedies.

In the control system having an architectural construction, effective solutions are selected and accepted as the basis of information about the technical characteristics of protection, and on the basis of the analysis of the controlled space. The architecture of the system of information security management information system in the local segment is presented in [4].

Thus it can be argued that the methodological basis of the information security management in the segment of the local information system, based on system

analysis and general laws of building management systems, the novelty of which lies in the totality of the developed methods, principles of building architecture information security management system with intelligent support for organizational and technical and operational management, which allows a rapid and informed decisions to ensure the required level of data protection.

In circumstances where the control system does not have full information about the status of the information environment, the necessity to counter threats of a model of development in which there is a choice of control action that is most relevant to the state of the control object. Formulated principles of countering threats to development models, provides a formalized description of the method of decision-making on the choice of management options for responding to security events.

The proposed structure of building intellectual support system of operational management can be built by this principle. By development of the intellectual system of operative management it is suggested to choose an unclear model. It is related to that considerable part of information about reasons and sources of anomalous events can be got only an expert way or as heuristic descriptions of processes. For determination of sources of AP IS must be presented by the model of that informative network to that she is oriented. This model divides the task of moving to information between computers through the environment of network on the amount of levels of less large and easier solvable small tasks. Each of these small tasks decides by means of one network level.

In the system of intellectual support of operative management it is suggested to use intellectual technologies: mechanism of unclear inferencing for the numeral estimation of probability of attack; organized organization of information about events in the base of knowledge; models of counteraction to the threats; making decision on the choice of rational variant of reacting on the events of safety.

References

1. Burachok V. L., Toliupa S.V., Anosov A.O. “System analysis and decision making in information security”. - Kyiv : State University of telecommunications, 2015. – P. 345.
2. Andreyev V.I, Goncharenko, Diviznuk M.M., Pavlov I.N., Horosko V.O. Designing of systems of technical protection information / – Sevastopol.: Изд. Центр СНУЯЭиП, 2011. – P. 235.
3. Toliupa S.V. Designing of systems of support decision-making in the recovery process and ensure comprehensive protect information systems. // Scientific and technical journal “Modern information security ”.– Kyiv, 2012. - №4. – P. 69-74.
4. Toliupa S.V., Pavlov I.N. Analysis of modeling approaches in decision-making processes when designing systems of information protection // Scientific and technical journal “Modern information security” – Kyiv, 2014. - №2. – P. 96-104.