УДК 004.415.056.5

С. В. Толюпа, І. І. Пархоменко
Київський національний університет ім. Тараса Шевченка

ЗАХИСТ ІНФОРМАЦІЇ З ІНТЕЛЕКТУАЛЬНОЮ ПІДТРИМКОЮ ОРГАНІЗАЦІЙНО-ТЕХНІЧНОГО Й ОПЕРАТИВНОГО УПРАВЛІННЯ

Для успішного використання сучасних інформаційних технологій необхідно ефективно управляти не тільки мережею, але і її системою захисту інформації (СЗІ), при цьому на рівні інформаційної системи автономно повинна працювати система, яка реалізує управління складом подій інформаційної безпеки, планування модульного складу СЗІ й аудиту. З огляду на те, що СЗІ є доволі складною організаційно-технічною системою, що функціонує в умовах невизначеності, суперечливості та неповноти знань про стан інформаційного середовища, управління такою системою має ґрунтуватися на застосуванні методів теорії прийняття рішень і необхідності застосування інтелектуальних технологій.

Ключові слова: захист, системний аналіз, система, інформація, інформаційна безпека, загроза, локальна мережа, урівень захищеності.

S. Toliupa, I. Parkhomenko
Taras Shevchenko National University of Kyiv

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

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. 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. 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. Formed operational command information that is communicated to the security administrator control object or automatically by means of implementing control actions on the built-in protection circuit control modules in the operational management. 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. 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.

Key words: protection, system analysis, system, information, information security, threat, local network, security level

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. This system must have at least four security zones: the outer covering the entire territory on which the buildings; Belt structures, facilities or devices in the system; belt system components (hardware, software, database elements) and a belt process data processing (Input / Output, internal processing, etc.). 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.

On the basis of principles analysis in conditions of uncertainty is offered generalized architecture security management information system in a local information system. Analyzes the basic management functions, the expediency of construction of system options, including two functional subsystems: subsystem of organizational and technical management and subsystem operational management in real time. In accordance with the requirement to quantify the characteristics of the systems, systems engineering put forward in the index is introduced as a controlled variable - The level of protection required depends on the value of the maximum level of criticality of processed information in a given period of time.

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.

Formed operational command information that is communicated to the security administrator control object or automatically by means of implementing control actions on the built-in protection circuit control modules in the operational management.

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].

On the basis of improving information security management capabilities through the use of new methods for solving management problems and reduce the control cycle time developed a functional model of the control system allows you to visualize and effectively display the IS management mechanism, identify processes for the implementation of which requires the development of automated intelligent control system of support.

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 developing the principles of organizational and technical and operational management of IS, which ensures retention of the required level of data protection in the operation of ISS in the framework of the existing plan in a situation of destructive information impacts.

On the basis of the set-theoretic approach proposed formalized description of the information system using a model that maps the semantics of the subject area. A description of the set of attacks in the form of tuples

$$U^{vnesh} = \langle S^{\text{int}ernal}, A, 3_{network}, 3_{hosts}, \Pi, O(C_m) \rangle \tag{1}$$

$$U^{vnesh}_{l(m)} = \langle S_1^{k-1}, A, 3_{network}, 3_{hosts}, \Pi, O^k(C_m^k) \rangle,$$

where U^{vnesh} – Attacks against information assets of the local information system; $U^{vnesh}_{l(m)}$ –Internal attacks on critical information assets k level processed in segments C_m, when the offender has an account as a user with the right to access to information, the level of which no more critical *(k* -1), and attempts to exceed their privileges; S^{internal} – external threats; S_1^{k-1} – the internal source of the threat; A - communication equipment in the communication channel; $3_{network}, 3_{hosts}$ – security services in the path of the attack, network and host; P – protocols, packets; *O* – object access; C_m^k – a segment in which information is processed, the highest level of criticality is equal to *k; l, m* - numbers of the local network.

An estimate of the number of pathways attacks, analyzed the ability to identify attacks on indicators of abnormal events on the propagation path. With the characteristic of the predicate introduced set of indicators

$$I = \{ i_j : \ i_j - yndykator\ the\ network, hostov, perymetr \}. \tag{2}$$

Since the only effective way to identify the attack is to analyze combinations of abnormal events, we are invited to compare a variety of possible ways to spread *P* attacks the set of indicators

$$\tau_a \subseteq P \times I = \{ (p_i, i_j) : p_i \in P \ \ \wedge \ \ i_j \in I \}, \tag{3}$$

and the probability that the suspicious activity is an attack, to evaluate the number of indicators on the propagation path. The cross section of conformity $\tau_a(p_i)$ defines a set of indicators corresponding to the implementation of the attacks in this way.

Since the operational management system is required to be the time the command information computation, the solution should be used for the fuzzy inference engine control tasks in conditions of incomplete, contradictory, and uncertainty about the state of the data information environment. Information that is input to the fuzzy inference system are the input variables - the number of signs of abnormal events. These variables correspond to the actual processes on the network. The information that is generated at the output of the fuzzy inference system, corresponds to the output variable, which is the probability that the set of abnormal events on the network is an attack (the probability of an attack).

Introduced linguistic variables “number of abnormal events on the network pathway attack”, “number of abnormal events on the host”, “number of abnormal events on the perimeter”, “the probability that suspicious activity is network attack”" In consideration of the input fuzzy sets *A, B, C, D* with accessory functions $\mu_{\tilde{A}}, \mu_{\tilde{B}}, \mu_{\tilde{C}}, \mu_{\tilde{D}}$:

$$\begin{gathered} A = \{ \mu_{\tilde{A}}(x) \mid x : \mu_{\tilde{A}}(x) \in [0,1], x \in X \}, \\ B = \{ \mu_{\tilde{B}}(x) \mid x : \mu_{\tilde{B}}(x) \in [0,1], x \in X \}, \\ C = \{ \mu_{\tilde{C}}(x) \mid x : \mu_{\tilde{C}}(x) \in [0,1], x \in X \}. \\ D = \{ \mu_{\tilde{D}}(p) \mid p : \mu_{\tilde{D}}(p) \in [0,1], p \in [0,1] \}, \end{gathered} \tag{4}$$

where *X* – the set of numbers of information security events indicators.

Membership functions of linguistic variables for input and output variables, the base of production rules are formed on the basis of expert data and modeling results.

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 process of selecting management options for responding to security events described by the tuple

$$\langle U_i, V_j, C_j(V_j), P_{\text{a}}, P(z_l), J, U^*(P_{\text{a}}) \rangle, \tag{5}$$

where U_i – Version of the response; V_j – the outcome; C_j – damage assessment; *the z* – parameter uncertainty of the state of the environment; $P(z_l)$ – the probability of the state of the environment; *J* – target selection function; $U^*(P_{\text{a}})$, –rational response option; P_{a} – the probability of an attack.

Model selection rational option is proposed not only to form a connection graph options respond to security events and outcomes, but also realize the function using a tabular form.

Analysis of possible response options $\{U_i\}$ to security events showed that the number of control actions for each situation is limited, $i \in [1,3]$. Since the selection is carried out under conditions of a possible implementation of the attack, it is proposed to connect the system to the assessment of alternatives preferences of damage: no damage, damage to a single user, damage to a group of users, the damage caused by the implementation of the attacks ($\{V_j\}, j \in [1,4]$).

Sets functionality, by which the selection of management options to respond:

$$J(U_i, z) = \sum_{l=1}^{s} C_j\left(V_j\left(U_i, z_l\right)\right) \cdot p\left(z_l\right), \tag{6}$$

$$p\left(z_l\right) = \prod_{i=1}^{I} p_{ij}\left(V_j\left(U_i\right), P_a\right).$$

where probability p_{ij} occurrence of each j outcome when selecting the response options offered to count as a function of the probability of attacks

$$p_{ij} = p_{ij}\left(V_j\left(U_i\right), P_{\text{a}}\right), \qquad \forall i : \sum_j p_{ij} = 1. \tag{7}$$

Rational control action $U^*\left(P_a\right)$ is defined as

$$U^*\left(P_{\text{a}}\right) = U\left(\arg \min_i \left(J\left(U_i, z\right)\right)\right). \tag{8}$$

On the basis of the adapted to the choice of a rational variant response decision making method developed to counter threats to the model taking into account the possible pathways of them: local network intrusion, over the air via a wireless access point, remote invasion through open access network.

Model counter threats in the case of potentially allow remote intrusion through the perimeter on the communication lines are presented in graph form and function realization shown respectively in Figure 1 and Table 1. In the development of models to counter threats to the principle of insufficient reason to Bernoulli, which is applicable in conditions of uncertainty.

Response options:

- U 1 – blocking access to the service on the network;
- U 2 – reconfiguration of security services with the aim of blocking the interaction of a specific IP-address;
- U 3 – sending alerts to the remote user and administrator awareness of increased activity.

For the developed models the results of numerical calculations for the three values of probability of attack.

To overcome the difficulties in weakly formalized situations higher quality level of operational management includes ensuring the necessary and sufficient intellectual support.

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.

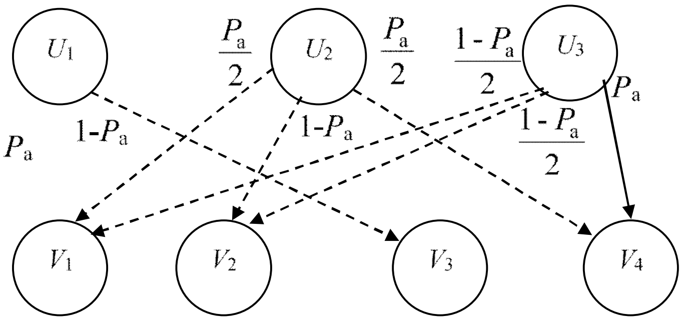

Fig. 1. Graph of response options and outcomes

Table 1

Implementation of the function

U	Z																	
	z_1	z_2	z_3	z_4	z_5	z_6	z_7	z_8	z_9	z_{10}	z_{11}	z_{12}	z_{13}	z_{14}	z_{15}	z_{16}	z_{17}	z_{18}
U_1	C_1	C_3	C_1	C_3	C_1	C_3	C_1	C_3	C_1	C_3	C_1	C_3	C_1	C_3	C_1	C_3	C_1	C_3
U_2	C_1	C_1	C_2	C_2	C_4	C_4	C_1	C_1	C_2	C_2	C_4	C_4	C_1	C_1	C_2	C_2	C_4	C_4
U_3	C_1	C_1	C_1	C_1	C_1	C_1	C_2	C_2	C_2	C_2	C_2	C_2	C_4	C_4	C_4	C_4	C_4	C_4

Let’s represent the separated level LIS like a nonlinear object with huge amount of entrance variables $\{x_i\}, i=\overline{1,n}$ and one outcome variable y.

$$y = f_y\left(x_1, x_2, \ldots x_n\right) \tag{9}$$

As input variables select sources sign of abnormal events. Output variable is an indicator of the degree of possibility of the state of the local information network.

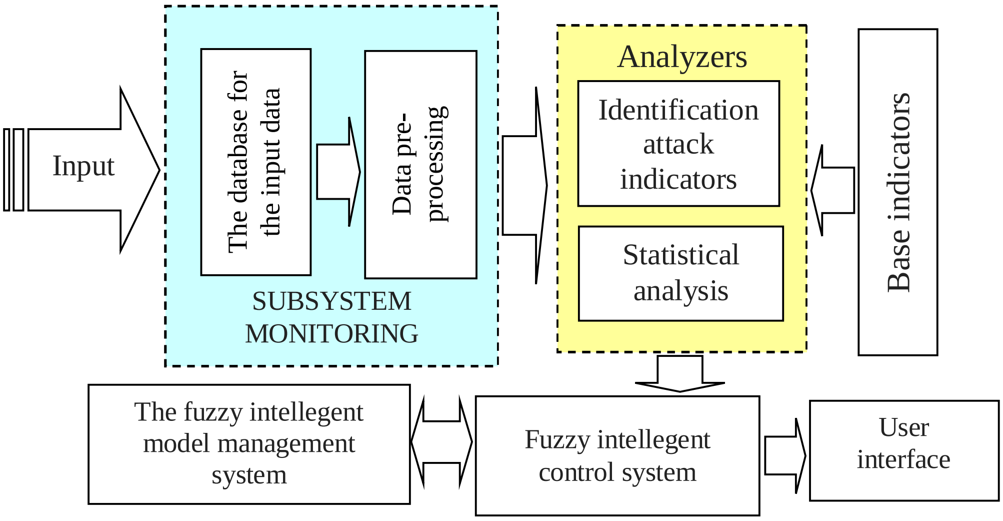
Input
The database for the input data
Data pre-processing
SUBSYSTEM MONITORING
Analyzers
Identification attack indicators
Statistical analysis
Base indicators
The fuzzy intellegent model management system
Fuzzy intellegent control system
User interface

Fig. 2. Structure of information system decision to detect attacks in the forest

In the model, the following assumptions and limitations:

- input variables $\{x_i\}$ within one level independent;
- at each level of the network isolated individual network functions.
- Integrated intelligent decision support system (IIDSS) for intrusion detection provides a set of functional components that allow to automate and speed up the production of actions that govern when changing situation in the forest. The structure IIDSS (Fig. 2) are:
- monitoring subsystem that executes the collection of primary information on the network equipment and software. Sources of information: event logs, database information, routers, control, switches, firewalls and other telecommunications equipment;
- power indicator and statistical analysis [5].

When analyzing identify indicators attacks were carried out to detect the AP data entering, by finding appropriate anomalous behavior indicators contained in the regularly updated database. Fuzzy intelligent system receives information about AP, AP analyzes the sources and develop proposals and actions that control, to eliminate them. The structure of fuzzy intelligent system (NIS) is shown in Fig. 3. The NIS program includes 12 units, 7 of whom are actually intelligent, and others - NIS development environment.

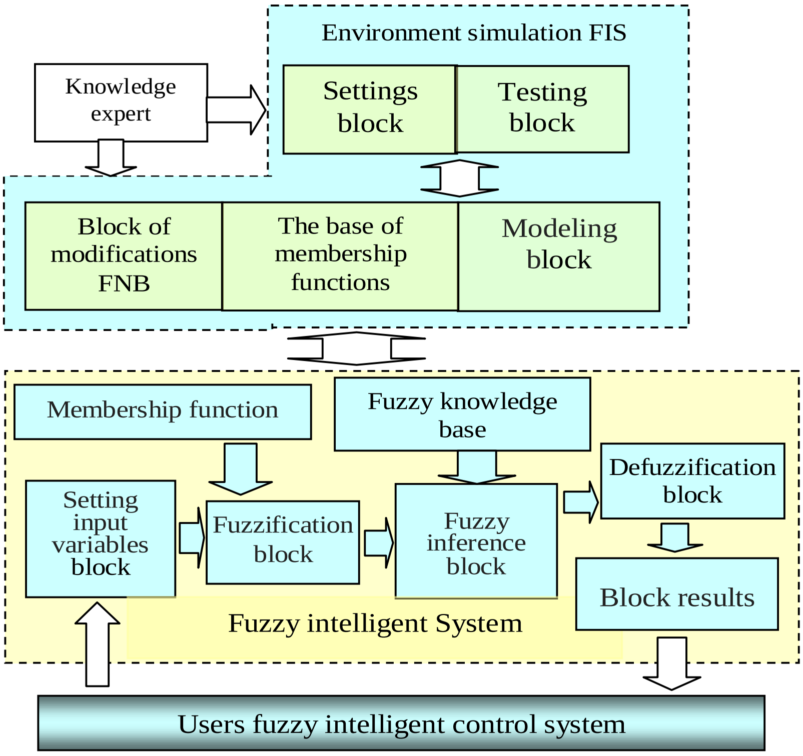

Fig. 3. Structure intellectual fuzzy control system GIS

The process of building the NIS is performed on the following algorithm:

- determine the characteristics of the system - defined input and output linguistic variables and their terms;
- definition of membership functions of linguistic terms;
- formation NS describing the behavior of the object;
- setting decision by NIS optimization problems using instructive sample.

As a result of fuzzy inference obtained membership function output variable each class solutions. During the simulation engineer on expert knowledge and can observe the behavior of the object in different areas of input variables. Setting model from experimental data can increase the normal work of NIS.

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. (2015), System analysis and decision making in information security, State University of telecommunications, Kyiv. 2. Andreyev V. I, Goncharenko, Diviznuk M. M., Pavlov I. N., Horosko V. O. (2011), Designing of systems of technical protection information, Sevastopol National University of Nuclear Energy and Industry Publishing center, Sevastopol. 3. Toliupa S.V. (2012), “Designing of systems of support decision-making in the recovery *process and ensure comprehensive protect information systems", Scientific and technical journal "Modern information security ", no. 4, pp. 69–74. 4. Toliupa S. V., Pavlov I. N. (2014) "Analysis of modeling approaches in decision-making processes when designing systems of information protection", Scientific and technical journal "Modern information security" no. 2, pp. 96–104. 5. Krivutca V. G., Berkman L. N., Toliupa S. V. (2012), Information and communication new generation network, State University of telecommunication, Kyiv.*

References

1. Бурячок В. Л., Толюпа С. В., Аносов А. О. Системний аналіз та прийняття рішень в інформаційній безпеці. Київ: ДУТ, 2015. С. 345. 2. Андреев В. И., Гончаренко Ю. Ю., Дивизинюк М. М., Павлов И. Н., Хорошко В. А. Проектирование систем технической защиты информации. Севастополь: Изд. Центр СНУЯЭиП, 2011. 235 с. 3. Толюпа С. В. Проектирование систем поддержки принятия решений в процессе восстановления и обеспечения комплексной защитыв информационных системах // Науково-технічний журнал "Сучасний захист інформації". 2012. № 4. С. 69–74. 4. Толюпа С. В., Павлов І. М. Аналіз підходів моделювання процесів прийняття рішень при проектуванні систем захисту інформації // Науково-технічний журнал "Сучасний захист інформації". 2014. № 2. С. 96–104. 5. Кривуца В. Г., Беркман Л. Н., Толюпа С. В. Інфокомунікаційні мережі нового покоління: монографія. Київ: ДУІКТ, 2012. 286 с.