Запропоновано архітектуру системи управління захистом об'єкта інформатизації з підсистемою інтелектуальної підтримки прийняття рішень з оперативного менеджменту кіберзахистом, зокрема в умовах неповноти знань про стан об'єкту захисту. Розроблено модель оперативного управління кібербезпекою об'єкта інформатизації та формування раціонального комплексу засобів захисту, заснована на морфологічному підході

Ключові слова: інформаційна безпека, управління захистом інформації, морфологічний підхід, система підтримки прийняття рішення

Предложена архитектура системы управления защитой объекта информатизации с подсистемой интеллектуальной поддержки принятия решений по оперативному менеджменту киберзащитой, в частности в условиях неполноты знаний о состоянии защищаемого объекта. Разработана модель оперативного управления кибербезопасностью объекта информатизации и формирования рационального комплекса средств защиты, основанная на морфологическом подходе

Ключевые слова: информационная безопасность, управление защитой информации, морфологический подход, система поддержки решения

UDC 004.056
DOI: 10.15587/1729-4061.2017.96662

DEVELOPMENT OF THE INTELLIGENT DECISION-MAKING SUPPORT SYSTEM TO MANAGE CYBER PROTECTION AT THE OBJECT OF INFORMATIZATION

V. Lakhno
Doctor of Technical Sciences, Associate Professor
Department of Managing Information Security*
E-mail: lva964@gmail.com
Y. Boiko
PhD, Associate Professor
Department of IT-Security**
E-mail: julia_boyko2010@ukr.net
A. Mishchenko
Doctor of Technical Sciences, Professor
Department of technical information security tools**
E-mail: partpravo@i.ua
V. Kozlovskii
Doctor of Technical Sciences, Professor
Department of technical information security tools**
E-mail: vvkzeos@gmail.com
O. Pupchenko
Postgraduate student
Department of Information Systems and Mathematical Sciences*
E-mail: oleksandr.pupchenko@gmail.com
*European University
Akademika Vernadskoho blvd., 16 V, Kyiv, Ukraine, 03115
**National Aviation University
Kosmonavta Komarova ave., 1, Kyiv, Ukraine, 03058

1. Introduction

Current level and further prospects for the development of information– communication systems (ICS) in different areas of human activity cannot be imagined without special attention paid to the issues of information (IS) and cybersecurity (CS). This is, in part, due to the growing number of cyber threats and destructive impacts on the objects of informatization (OBI).

That is why, in order to successfully use modern ICS, it is necessary not only to effectively manage their functional resources but also to create efficient information protection control systems (IPCS). Since the objects of control, IPCS, are rather complex organizational-technical structures (OTS) that operate under conditions of uncertainty, effective management of such systems should be based on the innovative information technologies of decision making support that relate to IS and CS.

One of the variants to solve this problem is the use of decision support systems (DSS) to manage CS based on intelligent information technologies (IIT).

This, in turn, makes it absolutely relevant to examine how to improve existing and develop new methods, models and software (SW) for the operational control over protection of OBI, in particular under conditions of incompleteness of knowledge about the state of ICS.

2. Literature review and problem statement

Growing number of cyberthreats to OBI caused a surge of research in the field of development of mathematical models for DSS [1, 2] and expert systems (ES) [3, 4] on the issues of information security and information protection (IP). But these studies are mainly represented only by formal mathematical models and are not brought to employable software products.

A separate direction of research into development of DSS [5] of intelligent decision-making support systems (IDMSS) [6] and ES with IS is the papers dedicated to the development of means of automated risk assessment of OBI [7] and program complexes of risk management of IS and CS [8]. Instead, articles [9, 10] note that IPCS, which realized intelligent technologies for responding to the events related to violation of IS, are the product of privately-owned companies; in this case, the customer in most cases is not aware of the information on the methods and models for the formation of controlling influences in the systems [11].

Papers [12, 13] pointed out the following shortcomings of many DSS and ES in the field of IS:

– required presence of experts with high qualification;

– difficulties arising in the adaptation of methods and models of IPCS to the needs of a particular organization;

– inability to evaluate the effectiveness of a particular IPCS at the object of protection;

– the requirement of availability of reliable statistics about the incidents in IS and CS.

Articles [14, 15] demonstrate that the existing DSS and ES in the field of IS, in addition to the tasks on managing cyberprotection, are advisable to equip with functional modules that allow improving the efficiency of planning of rational composition of the OBI IP systems (IPS). At the same time, no information about practical experience of applying such modules in DSS is provided by the authors.

Papers [16, 17] indicated that the existing standards in the field of IS management do not form specific approaches to managing the cyberptotection of OBI, and it complicates procedures of designing the employable software products that would allow adequate assessment of the degree of OBI.

Therefore, given the potential of application of DSS in IPCS, which implement preventive strategy of OBI cyberprotection [18, 19], it appears a relevant problem to develop the methods, models and applied SW applicable to the practical implementation in IDMSS. In particular, these studies are topical in the area of intelligent decision-making support for planning the rational structure of IPS, assessment and prediction of risk of violating the IS and CS, as well as management of IP under conditions of uncertainty in the potential impacts from cybercriminals.

3. The aim and tasks of the study

The aim of present study is to develop a model for counteracting the cyberattacks based on the application of IDMSS to select rational variants of response to the CS events with regard to operational data on the state of OBI.

To achieve the set aim, the following tasks have to be solved:

– to design an architecture for the information protection control system of OBI with a centralized and a decentralized variant of processing;

– to improve an operational control model (OC) of OBI CS, which makes it possible to increase the efficiency of IS management under condition of uncertainty in the state of OBI, as well as to improve the process of planning the rational structure of IPS;

– to develop a software complex of IDMSS to manage the OBI cyberprotection and to explore effectiveness of the proposed model.

4. Architecture of information protection control system

The main problem in the construction of IPCS, in particular control system (CoS) with CS, is the choice of the model of threats [20, 21]:

$$OI=\left\{\bigcup_{j=1}^{w}B^j,\bigcup_{j=1}^{w}INF^j,\bigcup_{j=1}^{w}RES^j,\bigcup_{j=1}^{w}VUL^j,\bigcup_{j=1}^{w}U^j,\bigcup_{j=1}^{w}COM^j,D_r^j\right\},\quad(1)$$

where B^j are the business processes of an enterprise; INF^j is the set of types of information arrays (IM); RES^j are the resources of OBI ICS; VUL^j is the set of vulnerabilities of OBI; U^j is the set of OBI ICS users; COM^j is the set of information flows of OBI; D_r^j is the set of states of OBI; $j=1,2,...,w$.

Based on the principles of control under conditions of uncertainty [5, 9, 16, 17] and the selected model of threats (1), we propose a generalized architecture of IPCS and CS, Fig. 1.

As a controlled variable, we use an indicator – the level of security (LS) [5, 9, 12, 17]. LS value depends on the maximal level of criticality of information processed in ICS.

In the circuit of organizational-technical management (OTM), we set up control mechanisms of IP during a change in appropriate business processes, for example, in the content of information arrays (IM), infrastructure, etc. An OTM circuit, given the results presentes in [6, 9], was improved by the implementation of block that allows controlling the assigned parameters of OBI CS. In the block of controlled parameters (CP), we implemented the algorithm for partition of space of attributes of anomalies and cyberattacks into clusters [12, 19] in the course of implementation of the procedure for the recognition of destructive influences. An improved architecture of IPCS differs from existing solutions by the possibility of simultaneous optimization when computing control tolerances for anomalies and cyberattacks. In this case, analysis of the level of OBI protection is performed in real time. The circuit includes: IDMSS for choosing a strategy of protection, a system for security level estimation (risk). Controlling influence in the circuit is executed by employees of the department (service) of IS. The command information is formed in the course of a purposeful selection of the rational structure of a complex of information protection means (CIPM).

In the OC circuit, operational command information is formed, which is delivered to the object of control by a security administrator or automatically by means of the realization of controlling influences.

The following abbreviations are adopted: SA – security administrator; DIB – data input block; KBIPM – knowledge base of information protection means; ISD – information security department; E – experts; MRCI – means of realization of controlling influences on the controlling modules embedded to IPM; CP – controlled parameters; MIESO – module for the implementation of exhaustive search algorithm of options from compatible software and hardware means; OC MCS – module of control over the state of object of control; MDA – module of deviation assessment; MPAM – module for processing additional matrices; MPC – matrices of pairwise comparisons; MFMM – module for the formation of morphological matrices; MFOF –module for the formation of objective function; OCI – operational command information; PLP – primary level of protection; SCI – scheduled command information; ROIPM – rational options for the information protection means; IDMSS – intelligent decision making support system over operational control (OC) of information protection.

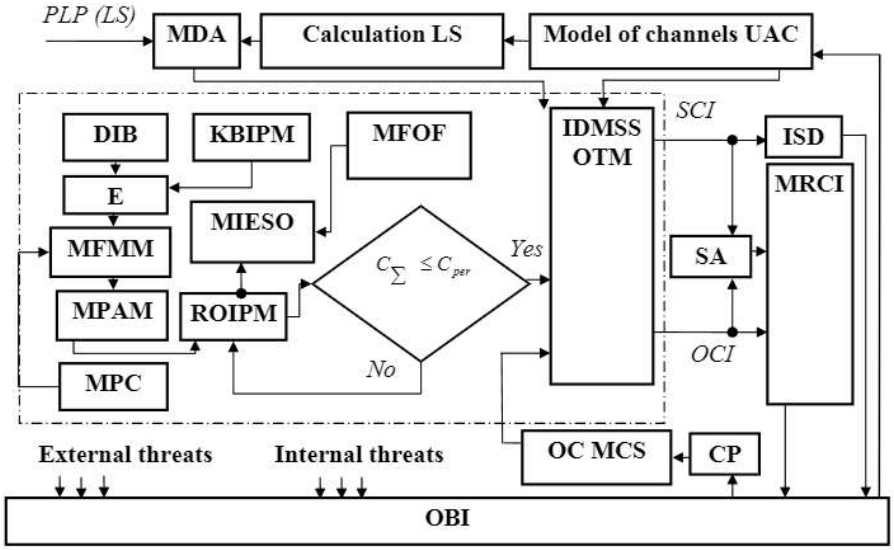

Fig. 1. Structure of IDMSS for the organizational-technical management of IP

In Fig. 2, The following designations are adopted: AVP – antivirus protection; DIC – data integrity control; AEIS – audit of events of information security; PSIO – physical security of information object; B – backup; UAC – user access control; SDCA – subsystem of detection of cyber attacks; MACS – monitoring and analysis of cyber security; NLAC – Network-level access control.

Perimeters of OBI protection: PIS (I) – the perimeter of the information system; PCOI (II) – perimeter of control of object of informatization; UAP (III) – User Access Perimeter; PNE (IV) – the perimeter of the network equipment; OPIO (V) – the outer perimeter of information object.

The IDMSS developed for the tasks on IP is expedient to consider for the subsystems of CS, which consist of five perimeters for centralized and decentralized architecture of OBI, Fig. 2 [22]. In Fig. 2, *a*, perimeters of IS are denoted as conditional boundaries that separate zones with different (required) security levels. In Fig. 2, *b*, perimeters of IP are formed based on possible threats to OBI SC. Corresponding methods for the means of IP are marked in green.

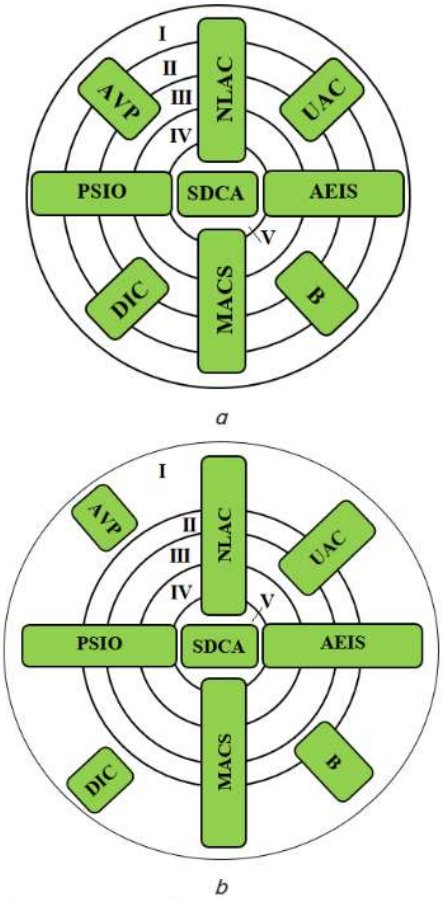

Fig. 2. Subsystems of IS: *a* – centralised option of OBI; *b* – decentralised option of OBI

The task on choosing the rational structure of CIPM for OBI is carried out according to the following criteria [22, 23]: minimal probability of the intruder accomplishing all goals; minimum of average level of losses at OBI from the intruder accomplishing all goals; maximum probability of success in the counteraction by CIPM of the intruder accomplishing all goals; minimum value of the integral indicator "cost – risk". For the proposed architecture of IPCS, we used the model of optimization of structural-technological resource (STR) for mission-critical IM and OBI infrastructure components by the criterion of minimum probability of failure to solve the task [18, 22].

In other words, according to the set task, it is necessary to find such values $x_{nm}^{um^*}$, which are

$$\min_{\left\{X_{unum}^{um^*}\right\}} \prod_{un=1}^{N} \prod_{um=1}^{M_{inf}} \left[\prod_{um^*}^{M_{inf}} \phi_{unum}^{um^*} \prod_{un=1}^{N_{po}} \prod_{um=1}^{M_{inf}} \prod_{um_1=1}^{M_{inf}^*} \prod_{um_2=1}^{M_{inf}^*} P_{um_1^* um_2^*}^{unumun\,um^*} \right], \quad (2)$$

where um* is node in OBI; M_{inf} is the number of IM; N_{po} is the number of program modules of OBI; ϕ_{unum}^{un} is the distribution of tasks on the nodes of OBI; $P_{um_1^* um_2^*}^{unumun\,um^*}$ is the probability of resolving all tasks on the nodes of OBI,

– with restrictions:

– on structural duplication of modules $X_{unum}^{um_1^*} X_{un\,um}^{um_2^*} = 0$ for $\forall un, um, un', um', um_1^*, um_2^*$, for which the conditions are satisfied $C_{um_1^* um_2^*} = 0$, $\phi_{unum}^{un\,um} \neq 0$;

– on the distribution of separate modules of OBI and others by separate nodes $X_{unum}^{um^*} = 1$, for the selected unum operating modules and um*-x nodes;

– on the longest possible time when solving the task

$$\sum_{un=1}^{N_{po}} \max_{\left\{um^*\right\}} \left[X_{unum}^{um^*} \theta_{unum} \lambda_{unum} \right] +$$

$$\sum_{un=1}^{N_{po}} \sum_{un'}^{N_{po}} \sum_{um=1}^{M_{inf}} \sum_{um'=1}^{M_{inf}} \max_{\left\{um_1^*, um_2^*\right\}} \left[X_{unum}^{um_1^*} X_{un'um'}^{um_2^*} \phi_{unum}^{un'um'} \frac{1}{C_{um_1^* um_2^*}} \right] \le T^*, \quad (3)$$

where T^* is the maximum possible time for solving the task; θ_{unum} is the number of requests in OBI for the processing of information; λ_{unum} is the intensity of solving the tasks;

$$\sum_{un=1}^{N_{pe}}\sum_{um=1}^{M_{inf}} x_{umun}^{um^*} f_{unum} \le V_{um^*},$$

$\forall um^*$, $um^* = \overline{1, M_{inf}}$. – on the maximum volume of external memory in the OBI nodes.

Based on the analysis of possibilities to improve IPCS of OBI, we propose the model for operational control over IDMSS with IS, which allows increasing the quality in planning the structure of IPS.

5. Model for the operational control over cyberprotection of object of informatization

Quantitative assessment of OBI protection can be obtained

$$LS_{CIS} = \prod_{i=1}^{n}(1 - C_{ICR} \cdot At_i \cdot As_i \cdot TL_i \cdot LS_i), \quad (4)$$

where C_{ICR} is the coefficient that allows representing the obtained result in the range [0; 1]; At_i is the level of violation of IS in the *i*th node; As_i is the criticality of information assets (IA) in the *i*th node; TL_i is the level of confidence in the device that reports IS violations in the ith node; LS_i is the level of protective measures in the ith node; the level of protection of the *i*th node; n is the number of nodes in OBI.

Sets of internal and external attacks against OBI will be represented in the form of tuples:

$$RCA = \langle EST, CE, SS_{ne}, SS_h, PP, O(NN)\rangle, \quad (5)$$

$$ICA_{l(m)} = \langle IST_l^{k-1}, CE, SS_{ne}, SS_h, PP, O^k(NN_m^k)\rangle, \quad (6)$$

where RCA is the remote attack on OBI; $ICA_{l(m)}$ is the internal attack on IA at the criticality level k, which are processed in node NN_m when the intruder has an account as a user with the right to access the information whose criticality level does not exceed (k-1) and tries to expand his privileges; EST is the external source of threat; IST_l^{k-1} is the internal source of threat; CE is the communication equipment; SS_{ne}, SS_h are the security services in the path of growing attack, network and hosting; PP are the protocols, packets; O is the object of access; NN_m^k is the OBI node, which processes information with the highest level of criticality (k); l, m are the numbers of nodes.

Articles [9, 17, 19, 24] proved that the only effective way to identify attack is the analysis of combinations of anomalous events. That is why IDMSS matches the set of possible ways WCA of spreading the attacks with the set of indicators IND. The number of indicators that were enabled along its progress assesses a probability that a suspicious activity is a cyberattack. The intersection $\tau_a(p_i)$ defines the set of indicators. Then we receive the following expression:

$$\zeta_a \subseteq WCA \times IND = \{(wca_i, ind_j): wca_i \in WCA \wedge ind_j \in IND\}, \quad (7)$$

where IND={ind_j:ind_l} is the indicator of a network or a perimeter of OBI; WCA are the possible ways of spreading the cyberattack against the nodes of OBI; $\zeta_a(wca_i)$ is the intersection, which defines the set of indicators that correspond to the realization of an attack along a given path.

In order to solve the tasks of IP under conditions of controversy or incompleteness of data on the state of OBI during the attack, IDMSS employs the mechanisms of fuzzy inference. The input information for the module of fuzzy inference is the number and informativeness of the attributes of anomalous events in the system [6, 17, 22]. The information that is formed at the output of fuzzy inference system corresponds to the original variable, which is the probability that the combination of anomalous events in the network is actually the attack.

Under condition of missing information on the state of OBI, IDMSS employs a model to counteract the threats, which enables a possibility to select the controlling influence that to the largest extent corresponds to the state of an object of control. The process of selecting the optimal option to respond to the security events will be represented in the form of a tuple:

$$\langle RV_i, RE_j, RUL, DA(RE_j), P_{CA}, P(z_l), OF, RV^{rat}(P_{CA})\rangle, \quad (8)$$

where RV_i is the variant of response; RE_j is the result; RUL are the decisive rules in IDMSS; DA_j is the loss assessment; z is the parameter of uncertainty in the state of environment; $P(z_l)$ is the probability of state $_l$ of the environment; OF is the objective function of selection; $RV^{rat}(P_{CA})$ is the rational option of response; P_{CA} is the probability of attack.

An analysis of possible reaction variants {RO_i} for the security events [9, 17, 22] revealed that the number of controlling influences for each situation is limited, i∈[1, 3].

Since the selection of options to respond to the IS events is carried out under conditions of a potential cyber attack, IDMSS applies a model for assessing the alternative benefits with the estimation of loss – {RE_i}, j∈[1, 4]: no damage, loss to a particular user, damage to a group of users, damage from the attack for the entire ICS.

We set the functional, according to which a selection of optimal variant of response is carried out:

$$OF(RV_i, z) = \sum_{l=1}^{s} DA_j\left(RE_j(RV_i, z_l)\right) \cdot p(z_l), \quad (9)$$

where

$$p(z_l) = \prod_{i=1}^{l} p_{ij}\left(RE_j(RV_i), P_{CA}\right).$$

Probability p_{ij} of the occurrence of each jth result when choosing the ith option of response is calculated as follows:

$$p_{ij} = p_{ij}\left(RE_j(RV_i), P_{CA}\right), \quad \forall i: \sum_j p_{ij} = 1. \quad (10)$$

Rational variant of controlling influence $RV^{rat}(P_{CA})$ is determined as:

$$RV^{rat}(P_{CA}) = RV\left(\arg \min_i\left(OF(RV_i, z)\right)\right). \quad (11)$$

In order to overcome difficulties in weakly-formalized situations, and for an improved qualitative level of OU, IPCS is equipped with a system of intelligent support of operational control over IP. In the process of organizational-technical management, at the stage of planning the composition of IP means (IPM), there is a consideration of the process of sequential removal of uncertainty concerning the structure and composition of IPM in IPS. The planning process PL

of rational combinations (sets) of MIP is described by expression

$$PL=SFS\rightarrow CS_{al}, \quad (12)$$

where SFS is the set of functional subsystems for the perimeter of IP; CS is the chosen set of IPM.

A process of decision-making by means of IDMSS on selecting the optimal variant of MIP for respective IP perimeters is regarded as the formation of a subset of the best options $CS'\subseteq CS$. The set of options set is represented as

$$CS=\{CS_1,..., CS_{AL}\}, \quad (13)$$

where AL is the number of variants of alternative combinations, based on which the choice is made.

In order to select the optimal variant of a IPM set, objective function OF is used: $CS_{al}=OF(CS)$.

The set of data that allow comparing the IPM variant includes two subsets:

$$MA_{LS_l}\subset MA_l \,\&\, MA_{in_l}\subset MA_l,$$

where MA_{LS_l} is the IPM indicator "protection of information"; MA_{in_l} is the IPM indicator "expenses" for the lth functional subsystems.

Using a morphological approach, decision-making model for choosing the optimal variant of IPM is represented as a tuple:

$$RUL:\langle PUR,SFS,RUL_s,CS,\ MA_l,OF,CS_r(CS')\rangle, \quad (14)$$

where PUR is the aim of making a decision; SFS are the initial data for the synthesis of IPM variants: $SFS=\{SFS_1,..., SFS_L\}$; RUL_s is the generation rule of variants of a set, which can be represented in analytical form as a vector product of sets

$$CS=SFS_1\times...\times SFS_L,$$

where SFS_l is the set, consisting of IPM of the lth functional subsystem

$$SFS_l=\left\{CM_{l1},...,CM_{lm}...,CM_{lK_l}\right\}.$$

CS is the set of synthesized variants of a set; MA_l are the data for the selection of rational variants; OF is the objective function to select the rational choice of IPM (selection rule); CS_r is the rational set of IPM, CM_{lm} is the protection means for the realization of the lth functional subsystem.

The selection of rational variants of IPM is implemented based on processing the knowledge of experts in the field of IS. The process of forming the rational complex of IPM is divided into five stages:

1. One develops variants of combinations of MIP. The set of possible variants to solve the task on selection is assigned by a morphological matrix. For the examined perimeters of IP, we developed morphological matrices of IPM.

2. One fills in auxiliary matrices in which one defines software-hardware means compatible with one another (SHM). Auxiliary matrix of compatible solutions is filled as follows. For each pair of IPM from different functional subsystems, one determines whether they are compatible. The result obtained is entered into KBIPM. If MIP are compatible, then compatibility function $s(CM_{lm},CM_{pr})=1$, otherwise $s(CM_{lm},CM_{pr})=0$.

3. One generates a set of decisions on the choice of options for MIP. One performs a truncation of this set to a subset of the options of a set from SHM compatible with each other. The set $CS=\{CS_1,..., CS_R\}$, consisting of all the possible options for constructing MIP for the IP perimeter, is a Cartesian product of sets of alternatives (rows of a morphological matrix).

Element of the set is represented as follows:

$$CS_r=$$
$$=\left\{\left(CM_{1i},CM_{2j},...,CM_{lm},...CM_{Ln}\right): CM_{lm}\in SFS_l, \forall l=\overline{1,L}\right\}, \quad (15)$$

where L is the number of functional subsystems for the perimeter of OBI IPS.

The generation of a set of decisions on the choice of options of the set, which consists of MIP compatible with each other, is carried out as follows. One runs an iterative synthesis of options which consist of compatible MIP: at the first step, variants of IPM for the first subsystem is sequentially checked, after selecting the alternatives CM_{1i}, a transition to the second stage takes place. At the second step, one performs a sequential check of options for IPM of the second subsystem, but the choice is made only for such alternatives CM_{2j}, for which compatibility function $s(CM_{1i},CM_{2j})=1$ and so on. When selecting the alternatives from the first subsystem, the choice is made only out of such alternatives CM_{lm}, for which the compatibility functions are equal to unity:

$$s(CM_{l-1,m}, CM_{lm})=1,...,s(CM_{2j}, CM_{lm})=1,$$

$$s(CM_{li,} CM_{lm})=1.$$

Thus, the choice of MIP from each row of the matrix to form the option set is performed only from SHM compatible compatible with each other.

4. Further truncation of set CS in IDMSS is performed by exhaustive search by the assigned objective function:

$$OF=\max_r\left(\frac{MA_{K^1_{LS}}^{CM_{li}}+...+MA_{K^1_{LS}}^{CM_{lm}}+...+MA_{K^1_{LS}}^{CM_{Ln}}}{MA_{K^1_{in}}^{CM_{li}}+...+MA_{K^1_{in}}^{CM_{lm}}+...+MA_{K^1_{in}}^{CM_{Ln}}}\right), \quad (16)$$

where $MA_{K^1_{LS}}^{CM_{li}}$ is the value of indicator "protection"; $MA_{K^1_{in}}^{CM_{li}}$ is the value of indicator "expenditures" on the protection means CM_{lm}.

The criteria of quality of IPM by the indicator "protection" are divided into two groups: indicators of effectiveness of operational methods of protection and indicators of functional applicability. Criteria of quality by the indicator "expenditures" are also divided into two groups: the cost of appropriate IPM and functional expenditures (for example, decrease in the performance of OBI modules when using the given IPM).

Using the T. Saaty method [17, 25], DSS carries out estimation of IPM and related criteria [9, 22]. It also calculates normalized values of the natural vector of IPM by all criteria to the indicators "protection" CR^1_{LS} and "expenditures" CR^1_{in} based on the processing of all the matrices of pairwise comparisons with regard to the links between criteria.

After selecting the rational combinations of IPM for the appropriate perimeters of protection, we receive a rational modular composition of holistic CIPM of OBI, which satisfies the requirement OF→max.

1. One estimates if the formed complex of IPM satisfies the requirement

$$C_{\Sigma} \le C_{per}, \tag{17}$$

where C_{Σ} is the total cost for the implementation of the MIR complex; C_{per} are the financial resources allocated for the implementation of the complex.

Indicator C_{Σ} is calculated using the following expression:

$$C_{\Sigma} = C_{P} + \sum_{S}\left(\sum_{i_S} C^{B}_{i_S} + \sum_{j_S} C^{M}_{j_S} + \sum_{k_S} C^{H}_{i_S} + C_{scg_S}\right), \tag{18}$$

where, accordinly, the cost of the set: C_p are the IPM of perimeter; $C^{B}_{i_S}$ are the IPM, which process information of the base level of criticality (CL); $C^{M}_{j_S}$ are the IPM, which process information of the medium CL; $C^{H}_{i_S}$ are the IPM, which process information of the high CL; C_{scg_S} are the IPM on the boundary of the sth segment of OBI; S is the number of segments of OBI.

The choice of a complex of IPM is realized by approaching the rational structure in the process of iterations. Such approach satisfies the requirements of the acceptable expenditures for the implementation of IPS.

In the process of analysis and assessment of risks, IDMSS defines a degree of adequacy of the planned IPM sets to the existing threats. Since the impact on information by different destructive factors is largely at random, then as a quantitative measure of vulnerability, IDMSS employs a probability of security violation of information.

It is accepted that the value of indicator of the mth MIP security information P_{blm} is a subjective probability of detection and blocking by IPM of unauthorized actions, that is, theoretically expected efficiency of the barrier.

It is obvious that the probability of violation of P^{n}_{blm} protection complements P_{blm} to unity, that is

$$P^{n}_{blm} = 1 - P_{blm}, \tag{19}$$

where P^{n}_{blm} is the probability of information protection violation, or the probability of vulnerability of the mth MIP (the probability of overcoming the appropriate perimeter).

It is known that the level of protection and relative risk complement each other to unity. It is proposed to compute the level of protection LS by formula

$$LS = 1 - \overline{R} = 1 - \sum_{S}\frac{C_s}{C_{\Sigma}}\cdot P_s, \tag{20}$$

where $\overline{R}$ is the relative risk; C_s is the proportion of cost of information resources in segment s, which is subject to protection; s is the number of segment; S is the number of segments; P_s is the resultant probability of threats to the information environment of OBI segment; C_{Σ} is the total unacceptable loss; C_s/C_{Σ} is the coefficient of danger of the totality of threats in the sth segment, which is defined as the proportion of cost of the object of protection, in particular, the information that is processed in the node.

Thus, to assess the level of protection, it is necessary to have a quantitative assessment of the probability of realization of the unauthorized access channels (UAC).

To assess the probability of violation of OBI IS by the subset of intruders {H} on a subset of possible channels for unauthorized obtaining of information (HOI) {CH} for a node of OBI, the following ratio is used

$$P_{S\{H\}\{CH\}} = 1 - \prod_{CH}\left(1 - P^{(b)}_{sjk}\right)\prod_{H}\left(1 - P^{(b)}_{sjk}\right), \tag{21}$$

under conditions

$$P^{(b)ex}_{sjk} \subset P^{(b)}_{sjk}, P^{(b)in}_{sjk} \subset P^{(b)}_{sjk},$$

where $P^{(b)in}_{sjk}$, $P^{(b)ex}_{sjk}$ is the probability of HOI that is processed in the sth segment, accordingly, by an internal (in) and an external (ex) intruder (attacker) for the object of protection that has gate points to the global network, external dedicated communication channels for which remote attacks through a perimeter is possible.

With regard to the proposed architecture and adopted model of protection $P^{(b)ex}_{sjk}$ is calculated as

$$P^{(b)ex}_{sjk} = 1 - \prod_{l=1}^{5}(1 - P^{ex}_{sjkl}), \tag{22}$$

where P^{ex}_{sjkl} is the probability of HOI that is processed in the sth node, by an attacker in case of overcoming the appropriate perimeter of protection l.

Probability of P^{ex}_{sjkl} depends on the following factors

$$P^{ex}_{sjkl} = P^{AS}_{skl}\cdot P^{H}_{sjkl}\cdot P^{TR}_{sjl}\cdot P^{IN}_{sjl}, \tag{23}$$

where accordingly, the probabilitis of: P^{AS}_{skl} – attempt of an internal attacker or external user – intruder to access the first perimeter of protection; P^{H}_{sjkl} – overcoming by attacker or external intruder of the first perimeter of protection; P^{TR}_{sjl} – the presence of traffic from the node (segment) s through the first perimeter; P^{IN}_{sjl} – the availability of information that is subject to protection in the node s when transmitting the traffic at the moment of overcoming by external intruder of the first perimeter.

An internal intruder in the course of the realization of UAC chanels must overcome at least three perimeters of protection. Then the probability of HOI that is processed in segment s by an internal intrder is calculated by formula:

$$P^{(b)in}_{sj} = 1 - \prod_{l=1}^{3}(1 - P^{in}_{sjl}), \tag{24}$$

where P^{in}_{sjl} is the probability of HOI (that is processed in the sth segment) by an internal intruder in case of overcoming the corresponding perimeter l.

Probability P^{H}_{sjkl} depends on the quality of IPM and the number of perimeters of protection at OBI. If an intruder must overcome M barriers in the appropriate perimeter, then the probability of his successful attack is defined as the product of

$$P^{H}_{sjkl} = \prod_{m=1}^{M} P^{H}_{blm} = \prod_{m=1}^{M}(1 - P_{blm}). \tag{25}$$

Based on the proposed model for risk assessment of the IS violation, we developed software packages (SP) for the automated system of intelligent support in the organizational-technical and operational management of OBI IP.

6. Software package "System of intellectual support for making decisions on the control of cybersecurity – DMSSCIS"

Software package "System of intellectual support for making decisions on the control of cybersecurity – DMSSCIS" (Fig. 3) is intended for a substantiated choice of rational complex of IPM when designing OBI IPS. DMSSCIS was also used in the course of modernization of existing IPS in computational centres at enterprises in Chernihiv (2016), Dnipro (2014), Poltava (2013–2014) and several industrial enterprises in Kyiv.

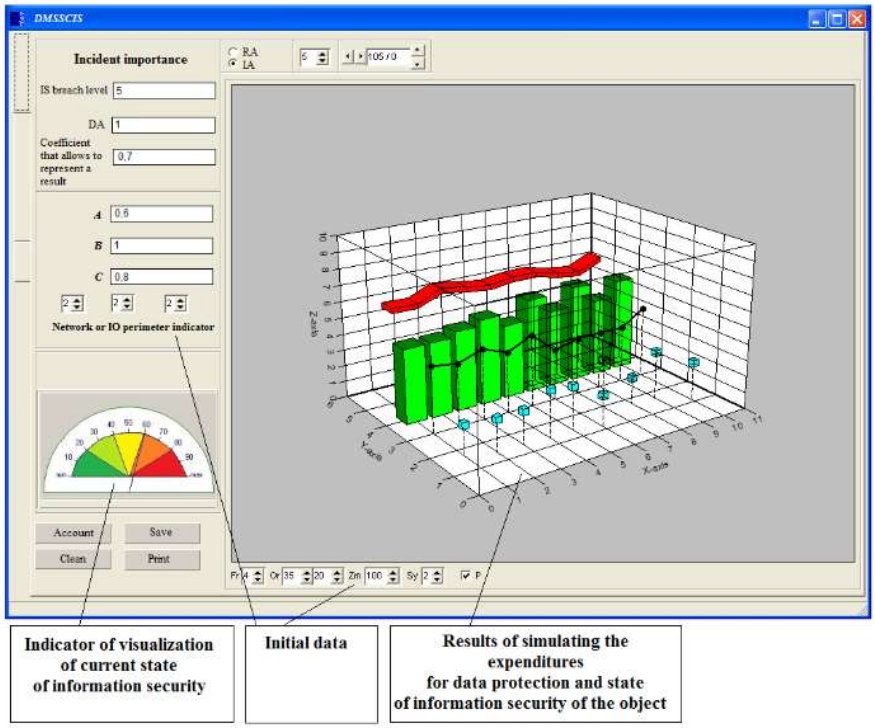

Fig. 3. Software package "System of intellectual support for making decisions on the control of cybersecurity – DMSSCIS"

Based on the software tool "DMSSCIS", which in particular implements the method of choosing the rational option of response to the security-related events, we obtained the following results, Table 1.

In the course of research we took into account a possibility of the existence of an attacker, who implements remote intrusion through the perimeters, the presence of external and internal users-intruders and an insider that has high privileges and violates security policy of OBI. After forming a rational composition of IPM at the enterprises where we carried out the study, a predicted value of risk, obtained by using the IDMSS "DMSSCIS", amounted to 1.78–1.91 %, which on average is 5.9–6.2 times lower than the value of risk for IPS that were previously used at the enterprises.

Fig. 4 shows examples of results of simulating the rational sets of IPM received using DMSSCIS.

Fig. 4, *a* show results of modeling the cost (C) of rational sets of OBI IPM. Fig. 4, *b* shows dependence of the integral indicator of overall expenses on IPS for OBI, related to the losses from the actions of intruder and the expenditures for the organization of a rational option of the IPM set. The resulting dependence has a clearly pronounced minimum. This indicates that, starting at this point, the level of spending on IPS begins to exceed the level of losses from the actions of intruder, which is why a major share in the value of integral indicator is the total cost of IPM.

Thus, at the overall cost to organize IPS along critical nodes [22] at OBI of the order of 5200–5500 units, the probability of an intruder reaching all aims is 10^{-2}.

Table 1

Results of testing the IDMSS "DMSSCIS"

Type of cyberattack	Options of response for the current parameters of OBI for the following linguistic variables: A is the number of anomalous network events along the way of spreading attack, B is the number of anomalous events on host, C is the number of anomalous events on the perimeter of OB, D is the probability that a detected anomalous activity in the network is actually the attack	
	Decision is made by ISA	Decision is made by ISA+ IDMSS (DMSSCIS)
DOS/DDOS	A=2; B=3; C=2; D=0,7; P_a=0,62	
	End of session with the node attack source	Sending out a warning
	Mean time of making a decision (MTMD), 15-20 min.	MTMD, 5–7 min.
U2R	A=2; B=3; C=2; P_a=0,54	
	End of session with the node attack source	Sending out a warning to the user
	MTMD, 3–7 min.	MTMD, 1–2 min.
R2L	A=1, B=3, P_a=0,432	
	End of session with the node attack source	Sending out a warning to the user
	MTMD, 6–8 min.	MTMD, 3–4 min.
Remote attack over the perimeter by the communication line	A=3, B=4, C=2, P_a=0,82; A=1, B=1, C=1, P_a=0,224 A=1, P_a=0,076	
	Blocking access to server in the network or Security services reconfiguration for the purpose of blocking IP	Sending out a warning or Security services reconfiguration for the purpose of blocking IP
	MTMD, 27–35 min.	MTMD, 2–3 min.

An increase in expenditures for the organisation of IPS above a certain level (exceeding 13000 units) is not expedient since it does not lead to a significant improvement in the efficiency of IPS.

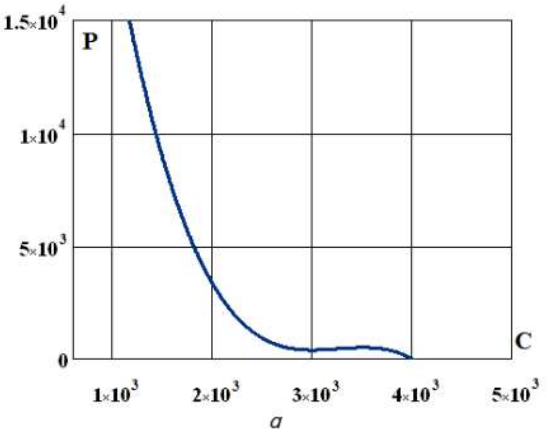

Fig. 4. Simulation results using DMSSCIS of the rational sets of IPM for OBI: *a* – dependence of the probability of realization of all the goals by intruder (**P**) on the cost of OBI IPS complexes (**C**, conditional units); *b* – integral indicator of overall expenditures on OBI IPS (**C**, conditional units) on the probability of successful counteraction by IPM of the actions of intruder (**P**)

In the course of research, it was demonstrated that the implementation of the IDMSS "DMSSCIS" makes it possible to enhance the level of automation and centralization in the monitoring of OBI protection, as well as reduce the time it takes to inform decision-makers about IS incidents by 6.9–7.2 times.

7. Discussion of results of IDMSS testing and prospects for further research

The proposed approach to constructing a comprehensive IPS for OBI allowed us to reduce expenditures for IPM by 32–35 % compared to alternative methods [2, 6, 10, 25].

The IDMSS "DMSSCIS" has the following advantages in comparison with similar DSS [8, 11, 17]:

– it allows assessing the level of OBI protection, which consists of a set of nodes that process information of the various criticality levels; allows assigning source data by the number of segments and nodes of OBI, taking into account the criticality levels of IA;

– provides efficiency in the evaluation of IPM sets; allows running a comparative analysis of various complexes of IPM during risk management;

– allows taking into account the specifics of functioning of a particular OBI and real threats to key resources.

A certain shortcoming of the IDMSS "DMSSCIS" is the requirement to engage at the initial stage of examination a few independent experts for the construction of memebership functions and compiling production rules. At the present stage of research, for this purpose we employed tools from the Fuzzy Toolbox (Matlab), which computes such indicators of MIP as "protection of information" for each involved perimeter of protection.

Further development of present work may include improving the interaction between traditional mechanisms of cybersecurity at OBI, which, in particular, process initial information by the modules of "DMSSCIS".

In general, based on the studies conducted, we can confirm effectiveness of the proposed models and software package for managing IS at the OBI of enterprises.

8. Conclusions

1. We proposed architecture of IPCS, in which the choice of optimal variant of the set of IP means for the respective perimeter is realized using an objective function that maximizes the ratio of the summary indicator "protection of information" to the summary indicator "expenditures". This makes it possible to obtain a complex of means of protection, certified for a given class of security. The requirements are also taken into account to the reasonable cost of the implementation of an information security system for a centralized and a decentralized variants of processing the information.

2. We improved a model for the operational maanagement of OBI CS and the formation of a balanced complex of means of protection. The model is based on the morphological approach. In contrast to the existing solutions, the model with regard to the morphological matrices for each of the perimeters of protection of OBI prepared by IDMSS allows us to generate variants of sets of means of protection, which take into account the compatibility of software and hardware tools.

3. We developed a software comples for IDMSS in the contours of managing the system of protection of OBI. The adequacy of the proposed model is confirmed. The use of the developed IDMSS in the networks of enterprises where the software package DMSSCIS was verified made it possible to reduce the planned spending on the construction of IPS by up to 35 %.

References

1. Panaousis, E. Cybersecurity Games and Investments: A Decision Support Approach [Text] / E. Panaousis, A. Fielder, P. Malacaria, C. Hankin, F. Smeraldi // Lecture Notes in Computer Science. – 2014. – P. 266–286. doi: 10.1007/978-3-319-12601-2_15

2. Fielder, A. Decision support approaches for cyber security investment [Text] / A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, F. Smeraldi // Decision Support Systems. – 2016. – Vol. 86. – P. 13–23. doi: 10.1016/j.dss.2016.02.012
3. Chang, L.-Y. Applying fuzzy expert system to information security risk Assessment – A case study on an attendance system [Text] / L.-Y. Chang, Z.-J. Lee // 2013 International Conference on Fuzzy Theory and Its Applications (iFUZZY). – 2013. doi: 10.1109/ifuzzy.2013.6825462
4. Atymtayeva, L. Building a Knowledge Base for Expert System in Information Security [Text] / L. Atymtayeva, K. Kozhakhmet, G. Bortsova // Advances in Intelligent Systems and Computing. – 2014. – P. 57–76. doi: 10.1007/978-3-319-05515-2_7
5. Grossklags, J. Secure or insure? [Text] / J. Grossklags, N. Christin, J. Chuang // Proceeding of the 17th international conference on World Wide Web – WWW '08. – 2008. doi: 10.1145/1367497.1367526
6. Kanatov, M. Expert systems for information security management and audit. Implementation phase issues [Text] / M. Kanatov, L. Atymtayeva, B. Yagaliyeva // 2014 Joint 7th International Conference on Soft Computing and Intelligent Systems (SCIS) and 15th International Symposium on Advanced Intelligent Systems (ISIS). – 2014. doi: 10.1109/scis-isis.2014.7044702
7. Korzhyk, D. Stackelberg vs. Nash in Security Games: An Extended Investigation of Interchangeability, Equivalence, and Uniqueness [Text] / D. Korzhyk, Z. Yin, C. Kiekintveld, V. Conitzer, M. Tambe // Journal of Artificial Intelligence Research. – 2011. – Vol. 41. – P. 297–327.
8. Rees, L. P. Decision support for Cybersecurity risk planning [Text] / L. P. Rees, J. K. Deane, T. R. Rakes, W. H. Baker // Decision Support Systems. – 2011. – Vol. 51, Issue 3. – P. 493–505. doi: 10.1016/j.dss.2011.02.013
9. Akhmetov, B. Designing a decision support system for the weakly formalized problems in the provision of cybersecurity [Text] / B. Akhmetov, V. Lakhno, Y. Boiko, A. Mishchenko // Eastern-European Journal of Enterprise Technologies. – 2017. – Vol. 1, Issue 2 (85). – P. 4–15. doi: 10.15587/1729-4061.2017.90506
10. Goztepe, K. Designing Fuzzy Rule Based Expert System for Cyber Security [Text] / K. Goztepe // International Journal of Information Security Science. – 2012. – Vol. 1, Issue 1. – P. 13–19.
11. Oglaza, A. Authorization Policies: Using Decision Support System for Context-Aware Protection of User's Private Data [Text] / A. Oglaza, R. Laborde, P. Zarate // 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. – 2013. doi: 10.1109/trustcom.2013.202
12. Lakhno, V. Design of adaptive system of detection of cyber-attacks, based on the model of logical procedures and the coverage matrices of features [Text] / V. Lakhno, S. Kazmirchuk, Y. Kovalenko, L. Myrutenko, T. Zhmurko // Eastern-European Journal of Enterprise Technologies. – 2016. – Vol. 3, Issue 9 (81). – P. 30–38. doi: 10.15587/1729-4061.2016.71769
13. Gamal, M. M. A Security Analysis Framework Powered by an Expert System [Text] / M. M. Gamal, B. Hasan, A. F. Hegazy // International Journal of Computer Science and Security (IJCSS). – 2011. – Vol. 4, Issue 6. – P. 505–527.
14. Ben-Asher, N. Effects of cyber security knowledge on attack detection [Text] / N. Ben-Asher, C. Gonzalez // Computers in Human Behavior. – 2015. – Vol. 48. – P. 51–61. doi: 10.1016/j.chb.2015.01.039
15. Ou Yang, Y.-P. A VIKOR technique based on DEMATEL and ANP for information security risk control assessment [Text] / Y.-P. Ou Yang, H.-M. Shieh, G.-H. Tzeng // Information Sciences. – 2013. – Vol. 232. – P. 482–500. doi: 10.1016/j.ins.2011.09.012
16. Linda, O. Fuzzy logic based anomaly detection for embedded network security cyber sensor [Text] / O. Linda, M. Manic, T. Vollmer, J. Wright // 2011 IEEE Symposium on Computational Intelligence in Cyber Security (CICS). – 2011. doi: 10.1109/cicybs.2011.5949392
17. Mashkina, I. V. Issues of information security control in virtualization segment of company information system [Text] / I. V. Mashkina, M. B. Guzairov, V. I. Vasilyev, L. R. Tuliganova, A. S. Konovalov // 2016 XIX IEEE International Conference on Soft Computing and Measurements (SCM). – 2016. doi: 10.1109/scm.2016.7519715
18. Gutzwiller, R. S. A task analysis toward characterizing cyber-cognitive situation awareness (CCSA) in cyber defense analysts [Text] / R. S. Gutzwiller, S. M. Hunt, D. S. Lange // 2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA). – 2016. doi: 10.1109/cogsima.2016.7497780
19. Lakhno, V. Creation of the adaptive cyber threat detection system on the basis of fuzzy feature clustering [Text] / V. Lakhno // Eastern-European Journal of Enterprise Technologies. – 2016. – Vol. 2, Issue 9 (80). – p. 18–25. doi: 10.15587/1729-4061.2016.66015
20. Burger, E. W. Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies [Text] / E. W. Burger, M. D. Goodman, P. Kampanakis, K. A. Zhu // Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security – WISCS '14. – 2014. doi: 10.1145/2663876.2663883
21. Al-Jarrah, O. Network Intrusion Detection System using attack behavior classification [Text] / O. Al-Jarrah, A. Arafat // 2014 5th International Conference on Information and Communication Systems (ICICS). – 2014. doi: 10.1109/iacs.2014.6841978
22. Lahno, V. Protection of information in critical application data processing systems [Text] / V. Lahno // MEST Journal. – 2014. – Vol. 2, Issue 2. – P. 102–112. doi: 10.12709/mest.02.02.02.11
23. Shin, J. Development of a cyber security risk model using Bayesian networks [Text] / J. Shin, H. Son, R. Khalil ur, G. Heo // Reliability Engineering & System Safety. – 2015. – Vol. 134. – P. 208–2017. doi: 10.1016/j.ress.2014.10.006
24. Tosh, D. An evolutionary game-theoretic framework for cyber-threat information sharing [Text] / D. Tosh, S. Sengupta, C. Kamhoua, K. Kwiat, A. Martin // 2015 IEEE International Conference on Communications (ICC). – 2015. doi: 10.1109/icc.2015.7249499
25. Hwang, J. Information Security Policy Decision Making: An Analytic Hierarchy Process Approach [Text] / J. Hwang, I. Syamsuddin // 2009 Third Asia International Conference on Modelling & Simulation. – 2009. doi: 10.1109/ams.2009.49