UDC 004.056

Lakhno V. A.

Dr. Sc. Associate Professor, Head of Complex Information Security Organization Department, European University, Kyiv, Ukraine

DEVELOPMENT OF A SUPPORT SYSTEM FOR MANAGING THE CYBER SECURITY

Context. In this paper the urgent problem of development of software of decision making support systems in information security is solved. Approach is based on a choice of rational options of response to events taking into account operational state-of-health data of a subject to protection.

Objective. Goal of the research is developing a cyber-threats counterwork model using decision support system, choosing rational variants of reactions on the occurrences in cybersecurity, and taking into account current operational data.

Method. The information object cyber security operational management system and the formation of the protection methods rational sets model which is based on a morphological approach is developed. It is proposed to find an optimal variant of the information security perimeter sets using an object function that maximizes the correlation of a consolidated figure of "information security" to consolidated figure "costs".

Results. A model for the operational management of cyber security-critical computer systems was developed. This model allows us to generate different variants of protection sets that are compliant with a computer system taking into account morphological matrices for each security perimeter prepared with the intelligent decision support system. It is proved that the use of the developed decision support systems can significantly reduce the costs planned for the complex means of cyber defense, as well as reduce the time to inform decision-makers on how to counter the identified information security incidents.

Conclusions. Scientific novelty of research consists that the model of operational management of cyber security of an information objects and formation of a rational complex of security features based on morphological approach is for the first time offered. The practical value of the developed methods and instruments is that they allow: to reduce time of development of systems of cyber security, to increase efficiency of planning of rational modular composition of security features due to creation of information and software environment in case of design; to increase validity of the made decisions on operational and to organizational technical control by protection.

Keywords: information safety, information security management, decision support system, morphological approach.

NOMENCLATURE

ACS – automated control systems;
AEIS – audit of CS events;
AVP – antivirus protection;
B – backup;
CIIO – critically important information object;
CONTS – controlling system;
CA – cyber-attacks;
CS – cybersecurity;
DA – data array;
DIC – data integrity control;
DSS – decision support system;
ES – expert systems;
ICS – information-communicative systems;
IDSS – intelligent decision of information security OM support system;
IO – information objects;
IPM – information protection means;
IPR – information protection;
IS – informational security;
ISMC – information security method complex rational structure;
ISMS – information security management system;
ISS – information security systems;
MACS – monitoring and analysis of CS;
MIP – means of information protection;
NLAC – network-level access control;
OM – operational management;
OPIO (V) – the outer perimeter of information object;
PCOI (II) – perimeter of control of information object;
PIS (I) – the perimeter of the information system;
PNE (IV) – the perimeter of the network equipment;
PSIO – physical security of IO;
SDCA – subsystem of detection of CA;
UAC – User Access Control;
UAP (III) – User Access Perimeter;
A – linguistic variable "number of unusual events in network against the spreading of CA";
AL – the number of alternative variants
As_i – DA criticality in i-IO crosspoint;
At_i – IS breach level in i-IO crosspoint;
B – linguistic variable «number of unusual events in the host»;
C – linguistic variable «number of unusual events in IO perimeter»;
CE – communication equipment in an information channel;
C_{ICR} – coefficient that allows to represent a result in a range [0; 1];
DA_j – damage assessment;
DPT_{lm} – security tool for the realization of functional subsystem of l;
EST – external source of threat;
$ICA_{l(m)}$ – internal CA against IA with k-level of criticality;
IMI_{cis_i} – IS incident importance in i-IO crosspoint;
IND – network or IO perimeter indicator;
IST_l^{k-1} – insider source of threat;
l, m – numbers of crosspoints;
L – number of functional subsystems for the perimeter of the IS;

DOI 10.15588/1607-3274-2017-2-12

LS_i – security measures level in i-IO crosspoint;

MA_{in_l} – indicator of "expenses" for functional subsystem l;

$MA^{ST_{li}}_{K^l_{in}}$ – indicator value "expenses" for security tools ST_{lm};

$MA^{ST_{li}}_{K^l_{LS}}$ – indicator value "security";

MA_l – data for the choice of rational variants;

$MALS_l$ – indicator of "information security";

n – quantity of crosspoints in IO structure;

NN^k_m – IO crosspoint, on which information with the highest level of criticality (k);

O – access object;

OF – object function of choice;

P_{CA} – CA probability;

$P(z_l)$ – (l) environment status probability;

PP – protocols and packets;

PUR – purpose of decision making;

RCA – remote CA against IO;

RE_j – result;

RO_i – reaction variant;

$RO^{rat}(P_{CA})$ – rational variant of reaction;

RSV – range of synthetic variants of setup;

RUL – model of decision making regarding the choice of the optimal variant of CS tools

SFS – range of functional sub-systems for perimeter IS;

SS_{ne}, SS_h – security services against the method of an CA spreading (networked and host);

ST_{lm} – security tool for the realization of functional subsystem of l;

TL_i – trust level of a device, which reports about IS breaches in i-IO crosspoint;

WCA – possible spreading ways of CA against IO crosspoints;

X – IS events indicators numeric evaluation;

z – environment status uncertainty characteristic;

$\tau_a(p_i)$ – crossing;

$\zeta_a(wca_i)$ – crossing that determines an indicators set which reacts against the CA.

INTRODUCTION

It is impossible to imagine modern attitudes and perspectives of further ICS development in different fields of human activity without the increased attention of questions regarding IS and CS particularly because of the increasing number of CA and the destructive influence on IO. The rapid increase of incidents in the field of IS has shown that existing ISS, which are built on the basis of known threats and emerging attacks, are not always effective in cases of new CA which are created against the widespread enterprise information system, ACS in electronics, industry, transport, the banking system etc.

Goal of the research – developing a cyber-threats counterwork model using DSS, choosing rational variants of reactions on the occurrences in CS, and taking into account current operational IO data.

1 PROBLEM STATEMENT

Suppose that in the process of organizational and technical cyber security management of the CIIO, the protection methods rational sets model planning stage (information protection means) is considered as a process of sequential removal of uncertainty of ISS structure and composition. Thus, the planning of rational compatible software and hardware sets IPM is a consideration of alternatives AL: $PL = SFS \to CS_{al}$. Then the decision selection by the IDSS is regarded as forming a subset of the best options set $CS' \subseteq CS$.

In the study, the problem of comparing sets of IPM options is examined using morphological matrix sets in terms of "information security" in the perimeter ISS CIIO and "costs" for l functional subsystem ISS, which operate in conditions of uncertainty, inconsistency and lack of knowledge about the state of the object which is protected.

2 REVIEW OF THE LITERATURE

The increasing number of IS and CS threats has given rise to the surge of research in the field of development of uncovering and preventing CA systems [1–4], and also DSS [5, 6] and ES [7–9] in this field. Publication analysis [10, 11], allows us to uncover the increasing popularity of ISS risk assessment automated methods [12] and program sets of IS and CS risk management [13]. It was mentioned in the works [14, 15] that ISMS, in which intelligent technologies of cyber-threat identification and reacting to occurrences of IS breaches are realized, are products of private companies, and that a customer in general doesn't have any information about methods and models of leading effects forming in systems [16]. It is shown in the works [17–20] that it is appropriate to equip existing DSS and ES in field of IS (excluding tasks of cyber-security management) with functional models that allow us to increase efficiency of enumeration and investigation of illegitimate interferences to the work of ICS crimes.

In such a way, according to the disputes in publications [5, 6, 8, 10, 16, 17], dedicated to the potential of using integrated DSS or ES in ISMS, the task of developing methods, models for using them in practice in intelligent support of ISS rational structure planning and the task of assessment and prediction of IS and CS risks became relevant.

3 MATERIALS AND METHODS

There is one main problem creating the CONTS – development of the threat model [7, 15, 21], which is connected to the specification of a management object interaction – ISS IO with the environment. IDSS, which develops a threat model building method, is based on a qualified scheme of goal-oriented destructive influences on IS and CS IO [22–24]. A generalized architecture of ISMS and CS is offered according to the results of the control strategy in conditions of uncertainty analysis [4, 15, 24].

Level of safety is used in the capacity of an operated variable. The *LS* value depends on the maximum level of information urgency which is being updated according to recent changes in ICS. Models [4, 15] consist of five perimeters for decentralized architecture of IO, fig. 1.

Mechanisms of IPR control are created in the circuit with organizational-technical control governing changing business applications, DA processing plans, infrastructure, and all the corresponding requests to the information safety level. The circuit contains: IDSS in regards to choosing a security strategy and a system of safety level assessment. Managing influence in the circuit is realized by the staff of the IS department. The task of ISMC rational structure choice for IO is made according to the following criteria [4, 9, 7, 15]: minimum probability of achieving goals by an attacker; minimum of IO losses should the attacker's goals be achieved; maximum probability of successful ISMC counteraction to the actions of an attacker; minimum "cost-risk" integrated index value [4, 9].

Quantity assessment of IO safety can be found the following way:

$$LS_{CIS} = \prod_{i=1}^{n} (1 - C_{ICR} \cdot At_i \cdot As_i \cdot TL_i \cdot DPT_{lm_i}). \quad (1)$$

Quantity of insider and external CA against IO are given in the form of tuples:

$$RCA = \langle EST, CE, SS_{ne}, SS_h, PP, O(NN) \rangle, \quad (2)$$

$$ICA_{l(m)} = \langle IST_l^{k-1}, CE, SS_{ne}, SS_h, PP, O^k(NN_m^k) \rangle. \quad (3)$$

It is proven in works [4, 10, 12, 20] that the only effective way to identify an attack is in the analysis of a combination of unusual events. That is why in IDSS, an attack spreading *WCA* possible ways, quantity is compared to a quantity of indicators IND. The probability of the fact that suspicious action is a attack is assessed with the indicators quantity which reacted against the attack spreading method. Crossing $\tau_a(p_i)$ determines an indicators set. We get the following expression:

$$\zeta_a \subseteq WCA \times IND = \{(wca_i, ind_j) : wca_i \in WCA \wedge ind_j \in IND\} \quad (4)$$

In conditions when the status of the information environment is unknown, the threat counteraction model is enabled in IDSS, which has an opportunity to choose a controlling influence that better corresponds to the management object status. A process of choosing an optimal safety events reaction variant are given in a form of a tuple:

$$\langle RO_i, RE_j, DA(RE_j), P_{CA}, P(z_l), OF, RO^{rat}(P_{CA}) \rangle. \quad (5)$$

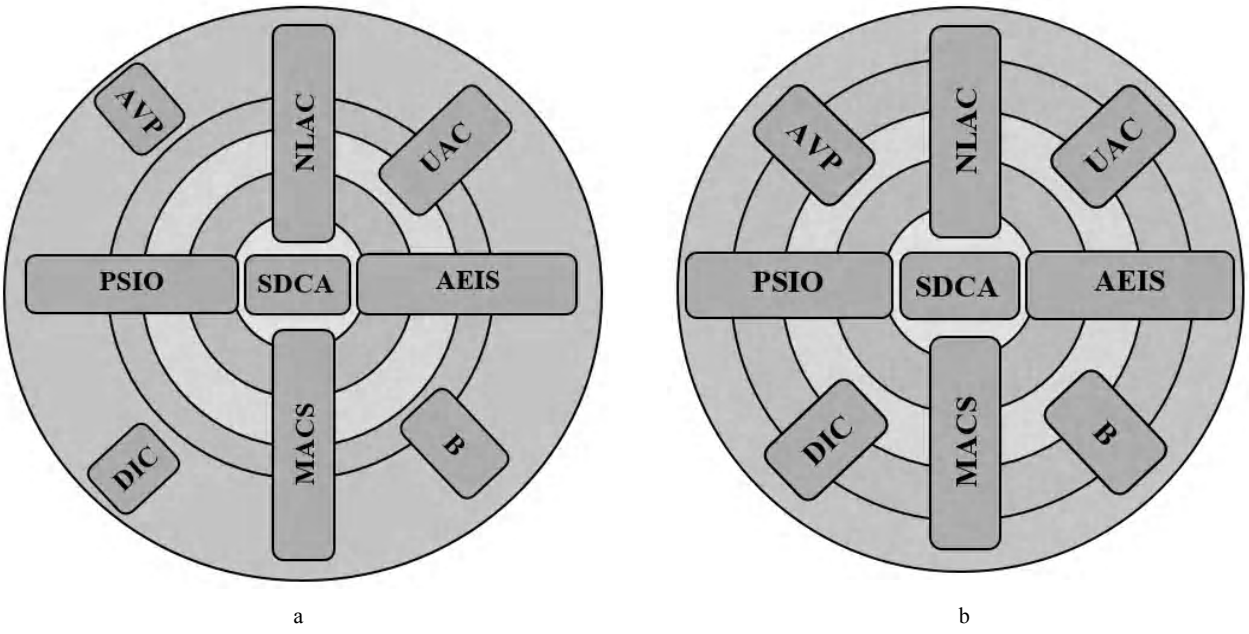
Safety events [4, 6, 9] reaction variants probability analysis $\{RO_i\}$ has shown that the number of control influences for each situation is limited $i \in [1,3]$. An alternative advantages evaluation with a damage assessment model is used in IDSS – $\{RE_j\}, j \in [1,4]$ taking into account that the IS events reaction variants choice is made in conditions of a potential CA: no harm, losses for a certain user, losses for a group of users, loss for all ICS from attack realization.

Define a function with which we choose an optimal reaction variant:

$$OF(RO_i, z) = \sum_{l=1}^{s} DA_j(RE_j(RO_i, z_l)) \cdot \prod_{i=1}^{I} p_{ij}(RE_j(RO_i), P_{CA}). \quad (6)$$

The probability p_{ij} of getting every *j*-result choosing every *i*-reaction variant is determined the following way:

$$p_{ij} = p_{ij}(RE_j(RO_i), P_{CA}), \ \forall i : \sum_j p_{ij} = 1. \quad (7)$$



a b

Figure 1 – IS subsystems:
a – Centralized IO variant; b – Decentralized IO variant

Control influence rational variant $RO^{rat}(P_{CA})$ is determined this way:

$$RO^{rat}(P_{CA}) = RO\left(\arg\min_{i}\left(OF(RO_i, z)\right)\right). \quad (8)$$

An IS OM intelligent support subsystem contains: a fuzzy inference mechanism for CA probability numeric evaluation; organized structure information about knowledge database events; threat recognition and counteraction models [4, 5, 9]; algorithm for making a decision regarding choosing an optimal safety events reaction variant [8].

During the organizational-technical management process, the stage of planning of storage for information security tools, and the process of gradual removal of uncertainty about the structure and the storage of information security tools in the information security system is being considered. The process of planning PL rational sets *MIP* is described with the formula:

$$PL = SFS \to RSV_{al}. \quad (9)$$

With the help of the system for intelligent support, the process of choosing optimal variant of *MIP* setup for perimeters of CS is considered as the formation of a sub-range for the best variants of setup $RSV' \subseteq RSV$. The range of the setup variants is described as

$$RSV = \{RSV_1, \ldots, RSV_{AL}\}. \quad (10)$$

For the choice of the optimal variant of CS tools the objective function *OF* is used:

$$RSV_{al} = OF(RSV). \quad (11)$$

The population of data, which make it possible to compare variants of setups, includes two sub-ranges:

$$MA_{LS_l} \subset MA_l \quad \& \quad MA_{in_l} \subset MA_l. \quad (12)$$

Usage a morphological approach, the model of decision making regarding the choice of the optimal variant of CS tools, is presented in the form of the sequence:

$$RUL: \langle PUR, SFS, RUL_s, RSV, MA_l, OF, RSV_r(RSV')\rangle. \quad (13)$$

The starting data for the synthesis of variants of CS tools sets: $SFS = \{SFS_1, \ldots, SFS_L\}$. Accepted:

$$RSV = SFS_1 \times \ldots \times SFS_L \quad \& \quad SFS_l = \{ST_{l1}, \ldots, ST_{lK_l}\}. \quad (14)$$

The choice of the rational variants of information security tools setups is realized on the basis of experts' knowledge in the field of CS. The process of formation of a rational structure of information security tools is divided into five stages: 1) The variants of *MIP* setup are put under development. The range of possible variants of the solution is set with the help of the morphological matrix. For the considered perimeters of information security, the morphological matrices of CS tools are developed; 2) The intermediary matrices are filled in, which indicate compatibility with the firmware. For each couple of CS tools for different functional subsystems their compatibility is defined. The result is filled in the table. If *MIP* are consistent, then the function of compatibility is $s(ST_{lm}, ST_{pr}) = 1$, in other case $s(ST_{lm}, ST_{pr}) = 0$; 3) The range of decisions concerning the choice of variants of setup *MIP* is generated. The range of tool setups is reduced to the sub-range which is known to be compatible with each other. The range $RSV = \{RSV_1, \ldots, RSV_R\}$, which consists of all possible variants of formulation of setup *MIP* for the considered perimeter, is the Descartes's production of setups of alternatives (morphological matrix ranges).

The element of the range is presented as follows:

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

The generation of the range of decisions concerning the choice of the variants, which consists of compatibility with each other *MIP*, is done in the following way. The iterated synthesis of variants of setup is made, which consists of compatibility *MIP*: on the first step the variants of CS tools for the first sub-system are consequently enumerated, after the choice of the alternative ST_{li} the transition to the second stage is made. On the second stage the consequent enumeration of variants of CS tools for the second subsystem is made, but the choice is made only for those alternatives ST_{2j}, for which the compatibility function is $s(ST_{1i}, ST_{2j}) = 1$ etc. For the choice of alternatives for l subsystem, the choice is made only from those alternatives ST_{lm}, for which the compatibility function is equal to one: $s(ST_{l-1,m}, ST_{lm}) = 1, \ldots, s(ST_{li}, ST_{lm}) = 1$.

Hence, the choice of *MIP* from each set of morphological matrix (one from each range) for the formation of a variant of setup is made only from compatibility with each other's firmware.

The further reduction of the *CS* range in the system of intelligent support for decision making is made in the form of a full enumeration with the given objective function. As the objective function for the choice of the setup variant, $CS_r = \{ST_{1i}, ST_{2j}, \ldots, ST_{lm}, \ldots, ST_{Ln}\}$ the function is used

$$OF = \max_r \frac{MA_{K_{LS}^l}^{ST_{1i}} + \ldots + MA_{K_{LS}^l}^{ST_{Ln}}}{MA_{K_{in}^l}^{ST_{1i}} + \ldots + MA_{K_{in}^l}^{ST_{Ln}}}. \quad (16)$$

The criteria of the quality of information "security" indicator is divided into two groups: the indicators of the effectiveness of the operative methods of the security and the indicators of the functional fitness.

4 EXPERIMENTS

The software package ("Decision Support System of Management protection of information – DMSSCIS") was developed for check of working capacity and practical applicability of the offered model of operational management of cyber security [4, 15]. In the course of the experimental

check of SP reaction options (RO_i) decision making support systems on different classes of CA for the current parameters of probability of implementation of the attack of P_a were researched. Also sets of instruments of information protection $CS' \subseteq CS$ for the purpose of a choice of rational option were researched. Restrictions on the cost of a set are accepted and minimum probabilities of successful implementation attacking all are more whole than CA for the selected set. DMSSCIS was also used in the modernization of existing information security systems in data centers of transport companies in Dnipro (2014) and several industrial enterprises in Kyiv.

5 RESULTS

On the software "DMSSCIS", that particular selection method implemented an efficient option for responding to security events. The results are shown in Table 1.

During the research the possibility was taken into account of an attack that implements remote intrusion through the perimeter, the availability of internal and external users, and abusers that have high privileges and violate the safety of information. After the formation of efficient information security in enterprises which took part in the study, with the help of intelligent decision support "DMSSCIS" the predicted value was P_a =1,78–1,91% risk that there was an average value of 5,9–6,2 times less risk to information security systems compared to before.

The amount of expenditure by the organization on information security for critical nodes of information objects order from 5200–5500 $. The likelihood of the offender achieving all their goals is 10^{-2}. The increase in appropriations for the organization of information security above a certain level (above 13,000 $.) is inappropriate because it does not lead to a significant increase in the efficiency of information security.

During the research it was shown that the implementation of the intelligent decision support "DMSSCIS" allows an increased level of automation and centralized monitoring of CS facility and reduces the time to inform those responsible for information security incidents by 6,9–7,2 times.

6 DISCUSSION

The approach of building a comprehensive information security system for the information object makes it possible to reduce the cost of data protection by 32–35% compared to alternative methods [6–9, 12, 13]. A certain lack of intelligent systems of decision support of "DMSSCIS", required the involvement in the initial study of several independent experts to build membership functions of production and assembly rules. At the current stage of research for this instrument, the fuzzy logic Fuzzy Toolbox (Matlab) was employed, which calculated "security information" MIP parameters for everyone involved in perimeter protection.

Overall, based on the studies, we can ascertain the effectiveness of the proposed models and software for information security management (information systems and automated control system) in examined enterprises.

CONCLUSIONS

In this paper the urgent problem of development of software of decision making support systems in CS of OI.

Scientific novelty of research consists that the model of operational management of CS of an OI and formation of a rational complex of security features based on morphological approach is for the first time offered. Unlike existing solutions, the model prepared on the basis of intelligent decision support, a morphological matrix for each facility's perimeters of information protection, and can generate a set of options for remedies which take into account the compatibility of software and hardware. The choice of the optimal option set for that perimeter protection of information, implements an objective function that maximizes the ratio of the sum "security information" to the total rate "cost". It provides a range of remedies for a given class of certified security, and satisfies the requirements for eligible costs for implementation of CS.

The practical value of the developed methods and instruments is that they allow: to reduce time of development of systems of CS, to increase efficiency of planning of rational modular composition of security features due to

Table 1 – The results of testing the software system "DMSSCIS"

Class of CA	Options for responding to the current settings information of environment of information object RO_i		
U2R	A=2, B=3, P_a = 0,54	A=1, B=1, P_a = 0,242	
	The end of session attack source node	Sending a warning message to the user	
R2L	A=1, B=3, P_a = 0,43	A=1, B=1, P_a = 0,192	
	The end of session attack source node	Sending a warning message to the user	
DOS/DDOS	A=2, B=3, P_a = 0,62	A=1, C=2, P_a = 0,4	
	The end of session attack source node	Sending a warning message to the user	
The external attack (Wi Fi)	A=3, C=3, P_a = 0,678	A=1, C=2, P_a = 0,4	A=1, C=1, P_a = 0,3
	Blocking access point	DOS-attack on stations	The lack of response
A remote attack via lines on the perimeter	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 the server in the network	Reconfiguration of security services to block IP	Sending a warning message to the user
Cost of a rational set of means of information protection $CS' \subseteq CS$ for OI			
Experts		"DMSSCIS"	
1000–11000 $		7000–8000 $	

creation of information and software environment in case of design; to increase validity of the made decisions on operational and to organizational technical control by protection. By using the developed system of intelligent decision support, networks of enterprises using DMSSCIS reduced the projected cost of the planned system of protection to 35 %. Further development of this work may be improving the interaction of traditional mechanisms of information security IO, which, in particular, are working on primary information system modules and intelligent decision support "DMSSCIS".

ACKNOWLEDGEMENTS

The work is supported by the state budget scientific research project of Dnipropetrovsk National University of Railway Transport named after academician V. Lazaryan "Automation of processes of complex technical systems in conditions of uncertainty" (state registration number 0104U005401).

REFERENCES

1. Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids / [Y. Zhang, L. Wang, W. Sun, R. C. Green II at al] // IEEE Transactions on Smart Grid. – 2011. – Vol. 2, No. 4. – P. 796–808. DOI:10.1109/TSG.2011.2159818
2. Al-Jarrah O. Network Intrusion Detection System using attack behavior classification / O. Al-Jarrah, A. Arafat // 5th International Conference Information and Communication Systems (ICICS). – 2014. – P. 1–6. DOI: 10.1109/IACS.2014.6841978
3. Louvieris P. Effects-based feature identification for network intrusion detection / P. Louvieris, N. Clewley, X. Liu // Neurocomputing. – 2013. – Vol. 121, Iss. 9. – P. 265–273. DOI:10.1016/j.neucom.2013.04.038
4. Lakhno V. Creation of the adaptive cyber threat detection system on the basis of fuzzy feature clustering / V. Lakhno // Eastern-European Journal of Enterprise Technologies. – 2016. – Vol. 2, No 9(80). – P. 18–25. DOI: 10.15587/1729-4061.2016.66015
5. Cybersecurity Games and Investments: A Decision Support Approach / [E. Panaousis, A. Fielder, P. Malacaria, C. Hankin et al] // Chapter Decision and Game Theory for Security. – 2014. – Vol. 8840. – P. 266–286. DOI: 10.1007/978-3-319-12601-2_15
6. Cavusoglu H. Decision-theoretic and game-theoretic approaches to IT security investment / H. Cavusoglu, R. Srinivasan, T. Y. Wei // Journal of Management Information Systems. – 2008. – Vol. 25(2). – P. 281–304.
7. Li-Yun Chang. Applying fuzzy expert system to information security risk Assessment – A case study on an attendance system / Li-Yun Chang, Zne–Jung Lee // 2013 International Conference on Fuzzy Theory and Its Applications. – P. 346–351. DOI: 10.1109/iFuzzy.2013.6825462
8. Atymtayeva L. Building a Knowledge Base for Expert System in Information Security / L. Atymtayeva, K. Kozhakhmet, G. Bortsova // Chapter Soft Computing in Artificial Intelligence. – 2014. – Vol. 270. – P. 57–76. DOI:10.1007/978-3-319-05515-2_7
9. Kanatov M. Expert systems for information security management and audit / M. Kanatov, L. Atymtayeva, B. Yagaliyeva // Implementation phase issues, Soft Computing and Intelligent Systems, Joint 7th International Conference on and Advanced Intelligent Systems (ISIS), 15th International Symposium on 3–6 Dec. 2014. – P. 896–900. DOI:10.1109/SCIS-ISIS.2014.7044702
10. Yanga Y.-P. Ou. A VIKOR technique based on DEMATEL and ANP for information security risk control assessment / Y.-P. O. Yanga, H. Shieha, G. Tzeng // Information Sciences. – 2013. – Vol. 232. – P. 482–500. http://dx.doi.org/10.1016/j.ins.2011.09.012
11. Bulgurcu B. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness / B. Bulgurcu, H. Cavusoglu, I. Benbasat // MIS Quarterly. – 2010. – No. 34(3). – P. 523–548.
12. Fuzzy logic based anomaly detection for embedded network security cyber sensor / [O. Linda, M. Manic, T. Vollmer, J. Wright] // Computational Intelligence in Cyber Security (CICS), IEEE Symposium on 11–15 April 2011. – P. 202–209. DOI: 10.1109/CICYBS.2011.5949392
13. Demetz L. To Invest or Not to Invest? Assessing the Economic Viability of a Policy and Security Configuration Management Tool / L. Demetz, D. Bachlechner // The Economics of Information Security and Privacy, Springer, 2013. – P. 25–47. DOI:10.1007/978-3-642-39498-0_2
14. Oglaza A. Authorization Policies: Using Decision Support System for Context-Aware Protection of User's Private Data, Trust, Security and Privacy in Computing and Communications (TrustCom) / A. Oglaza, R. Laborde, P. Zarate // 2013 12th IEEE International Conference on 16–18 July 2013, Melbourne, VIC Australia. – P. 1639–164. DOI: 10.1109/TrustCom.2013.202.
15. LakhnoDesign of adaptive system of detection of cyber-attacks, based on the model of logical procedures and the coverage matrices of features / [V. Lakhno, S. Kazmirchuk, Y. Kovalenko, L. Myrutenko et al] // Eastern-European Journal of Enterprise Technologies. – 2016. – No. 3/9 (81). – P. 30–38. DOI: 10.15587/1729-4061.2016.71769
16. Gamal M. M. A Security Analysis Framework Powered by an Expert System / M. M. Gamal, B. Hasan, A. F. Hegazy // International Journal of Computer Science and Security. – 2011. – Vol. 4, No. 6. – P. 505–527.
17. Goztepe K. Designing Fuzzy Rule Based Expert System for Cyber Security / K. Goztepe // International Journal of Information Security Science. – 2012. – Vol. 1, No. 1. – P. 13–19.
18. Gutzwiller R. S. A task analysis toward characterizing cyber-cognitive situation awareness (CCSA) in cyber defense analysts / R. S. Gutzwiller, S. M. Hunt, D. S. Lange // 2016 IEEE International Multi-Disciplinary Conference on 21–25 March 2016, DOI: 10.1109/COGSIMA.2016.7497780.
19. Decision support for Cybersecurity risk planning / [L. P. Reesa, J. K. Deanea, T. R. Rakesa, W. H. Bakerb] // Decision Support Systems. – 2011. – Vol. 51, Iss. 3. – P. 493–505. DOI.org/10.1016/j.dss.2011.02.013
20. Paliwal S. Denial-of-Service, Probing & Remote to User (R2L) Attack Detection using Genetic Algorithm / S. Paliwal, R. Gupta // International Journal of Computer Applications. – 2012. – Vol. 60, No.19. – P. 57–62.
21. Ben-Asher N. Effects of cyber security knowledge on attack detection / N. Ben-Asher, C. Gonzalez // Computers in Human Behavior. – 2015. – Vol. 48. – P. 51–61. DOI: 10.1016/j.chb.2015.01.039
22. Buryachok V. L. Algoritm ocinyuvannya stupenya zaxishhenosti special'nix informacijno-telekomunikacijnix sistem // Zaxist informacії. – 2011. – No. 3. – P. 19–27.
23. Valenzuela J. Real-Time Intrusion Detection in Power System Operations / J. Valenzuela, J. Wang, N. Bissinger // IEEE Transactions on Power Systems, 2013. – Vol. 28, No. 2. – P. 1052–1062. DOI:10.1109/TPWRS.2012.2224144
24. Потій О. В. Дослідження методів оцінки ризиків безпеці інформації та розробка пропозицій з їх вдосконалення на основі системного підходу / О. В. Потій, А. В. Лєншин [Текст] // Збірник наукових праць Харківського університету Повітряних Сил. – 2010. – Вип. 2(24). – С. 85–91.

Article was submitted 16.12.2016.
After revision 28.12.2016.

Лахно В. А.
Д-р техн. наук, доцент, зав. кафедри організації комплексного захисту інформації, Європейський університет, Київ, Україна

РОЗРОБКА СИСТЕМИ ПІДТРИМКИ РІШЕНЬ З УПРАВЛІННЯ КІБЕРЗАХИСТОМ

Актуальність. В роботі вирішена актуальна задача розвитку математичного забезпечення систем підтримки прийняття рішень з кібербезпеки на основі вибору оптимізованих варіантів реагування на інциденти. При цьому враховуються експлуатаційні параметри об'єкта захисту.

Мета. Розробка моделі протидії кіберзагрозам на основі застосування системи підтримки рішень по вибору оптимізованих варіантів реагування на інциденти кібербезпеки з урахуванням поточної інформації, яка стосується об'єктів захисту.

Метод. Розроблено модель оперативного менеджменту кібербезпекою критично важливих комп'ютерних систем і синтезу раціональних комплексів засобів захисту. Модель базується на морфологічній парадигмі. Запропоновано здійснювати вибір оптимізованих варіантів комплексів для периметрів кіберзахисту за допомогою цільової функції, яка максимізує відношення узагальненого індексу «захищеність інформації» до підсумкового показника «витрати».

Результати. Розроблено модель оперативного менеджменту кібербезпекою критично важливих комп'ютерних систем. Модель дозволяє з урахуванням сукупності морфологічних матриць, підготовлених в ході роботи системи підтримки прийняття рішень для кожного з розглянутих в роботі периметрів, згенерувати варіативні набори комплексів захисту, в яких врахована їх апаратно-програмна сумісність. Розроблено програмний комплекс для інтелектуальної підтримки прийняття рішень в задачах управління кібербезпекою об'єкта інформатизації. Доведено, що використання розробленої системи підтримки рішень дозволяє істотно зменшити плановані витрати на комплекси засобів кіберзахисту, а також скоротити час інформування відповідальних осіб про способи протидії виявленим інцидентам з інформаційної безпеки.

Висновки. Наукова новизна досліджень полягає в тому, що вперше запропонована модель оперативного менеджменту кібербезпекою критично важливих комп'ютерних систем і синтезу оптимізованих комплексів засобів захисту, що базується на морфологічній парадигмі. Практична цінність розроблених методів і засобів полягає в тому, що вони забезпечують: економію часу на етапі побудови комплексних систем кібербезпеки об'єктів інформатизації; підвищення ефективності вибору оптимізованих модульних систем кіберзахисту; аргументованість прийнятих рішень в процесі стратегічного, оперативного та організаційного менеджменту захистом об'єктів інформатизації.

Ключові слова: інформаційна безпека, управління захистом інформації, система підтримки рішення, раціональний набір засобів захисту.

Лахно В. А.
Д-р техн. наук, доцент, зав. кафедры организации комплексной защиты информации, Европейский университет, Киев, Украина

РАЗРАБОТКА СИСТЕМЫ ПОДДЕРЖКИ РЕШЕНИЙ ПО УПРАВЛЕНИЮ КИБЕРЗАЩИТОЙ

Актуальность. В работе решена актуальная задача развития математического обеспечения систем поддержки принятия решений по кибербезопасности на основе выбора оптимизированных вариантов реагирования на инциденты с учетом эксплуатационных параметров объекта защиты.

Цель. Разработка модели противодействия киберугрозам на основе применения системы поддержки решений по выбору оптимизированных вариантов реагирования на инциденты кибербезопасности с учетом текущей информации, касающейся объектов защиты.

Метод. Разработана модель оперативного менеджмента кибербезопасностью критически важных компьютерных систем и синтеза рациональных комплексов средств защиты. Модель базируется на морфологической парадигме. Предложено осуществлять выбор оптимизированных вариантов комплексов для периметров киберзащиты с помощью целевой функции, которая максимизирует отношение обобщенного индекса «защищенность информации» к итоговому показателю «затраты».

Результаты. Разработана модель оперативного менеджмента кибербезопасностью критически важных компьютерных систем. Модель позволяет с учетом совокупности морфологических матриц, подготавливаемых в ходе работы системы поддержки принятия решений для каждого из рассматриваемых в работе периметров, сгенерировать вариативные наборы комплексов защиты, в которых учтена их аппаратно-программная совместимость. Разработан программный комплекс для интеллектуальной поддержки принятия решений в задачах управления кибербезопасностью объекта информатизации. Доказано, что использование разработанной системы поддержки решений позволяет существенно уменьшить планируемые расходы на комплексы средств киберзащиты, а также сократить время информирования ответственных лиц о способах противодействия выявленным инцидентам информационной безопасности.

Выводы. Научная новизна исследований состоит в том, что впервые предложена модель оперативного менеджмента кибербезопасностью критически важных компьютерных систем и синтеза оптимизированных комплексов средств защиты, базирующаяся на морфологической парадигме. Практическая ценность разработанных методов и средств заключается в том, что они обеспечивают: экономию времени на этапе построения комплексных систем кибербезопасности объектов информатизации; повышение эффективности выбора оптимизированных модульных систем киберзащиты; аргументированность принимаемых решений в процессе стратегического, оперативного и организационного менеджмента защитой объектов информатизации.

Ключевые слова: информационная безопасность, управление защитой информации, система поддержки решения, рациональный набор средств защиты.

REFERENCES

1. Zhang Y., Wang L., Sun W., Green R. C., Alam M. Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids, *IEEE Transactions on Smart Grid,* 2011, Vol. 2, No. 4, pp. 796–808. DOI:10.1109/TSG.2011.2159818
2. Al-Jarrah O., Arafat A. Network Intrusion Detection System using attack behavior classification, *Information and Communication Systems (ICICS), 2014 5th International Conference*, 2014, pp. 1–6. DOI: 10.1109/IACS.2014.6841978
3. Louvieris P., Clewley N., Liu X. Effects-based feature identification for network intrusion detection, *Neurocomputing,* 2013, Vol. 121, Iss. 9, P. 265–273. DOI:10.1016/j.neucom.2013.04.038
4. Lakhno V. Creation of the adaptive cyber threat detection system on the basis of fuzzy feature clustering, Eastern-European Journal of Enterprise Technologies, 2016, Vol. 2, No. 9(80): Information and controlling system, pp. 18–25. DOI: 10.15587/1729-4061.2016.66015
5. Panaousis E., Fielder A., Malacaria P., Hankin C., Smeraldi F. Cybersecurity Games and Investments: A Decision Support Approach, Chapter Decision and Game Theory for Security of

the series Lecture Notes in Computer Science, 2014, Vol. 8840, pp. 266–286. DOI: 10.1007/978-3-319-12601-2_15
6. Cavusoglu H., Srinivasan R., Wei T. Y. Decision-theoretic and game-theoretic approaches to IT security investment, *Journal of Management Information Systems*, 2008, Vol. 25(2), pp. 281–304.
7. Li-Yun, Chang, Zne-Jung Lee Applying fuzzy expert system to information security risk Assessment – A case study on an attendance system, *2013 International Conference on Fuzzy Theory and Its Applications,* 2013, pp. 346–351. DOI: 10.1109/iFuzzy.2013.6825462
8. Atymtayeva L., Kozhakhmet K., Bortsova G. Building a Knowledge Base for Expert System in Information Security, *Chapter Soft Computing in Artificial Intelligence,* 2014, Vol. 270, pp. 57–76. DOI:10.1007/978-3-319-05515-2_7
9. Kanatov M., Atymtayeva L., Yagaliyeva, B. Expert systems for information security management and audit. Implementation phase issues, Soft Computing and Intelligent Systems (SCIS), *Joint 7th International Conference on and Advanced Intelligent Systems (ISIS), 15th International Symposium on 3–6 Dec. 2014,* pp. 896–900. DOI:10.1109/SCIS-ISIS.2014.7044702
10. Yu-Ping Ou Yanga, How-Ming Shieha, Gwo-Hshiung Tzeng A VIKOR technique based on DEMATEL and ANP for information security risk control assessment, *Information Sciences,* 2013, Vol. 232, pp. 482–500. http://dx.doi.org/10.1016/j.ins.2011.09.012
11. Bulgurcu B., Cavusoglu H. and Benbasat I. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness, *MIS Quarterly,* 2010, No. 34(3), pp. 523–548.
12. Linda O., Manic M., Vollmer T., Wright J. Fuzzy logic based anomaly detection for embedded network security cyber sensor, *Computational Intelligence in Cyber Security (CICS), IEEE Symposium on 11–15 April 2011,* 2011, pp. 202–209. DOI: 10.1109/CICYBS.2011.5949392
13. Demetz L., Bachlechner D. To Invest or Not to Invest? Assessing the Economic Viability of a Policy and Security Configuration Management Tool, *The Economics of Information Security and Privacy*, Springer, Heidelberg, 2013, pp. 25–47. DOI:10.1007/978-3-642-39498-0_2
14. Oglaza A., Laborde R., Zarate P. Authorization Policies: Using Decision Support System for Context-Aware Protection of User's Private Data, Trust, Security and Privacy in Computing and Communications (TrustCom), *12th IEEE International Conference on 16–18 July 2013,* 2013, pp. 1639–164. DOI: 10.1109/TrustCom.2013.202.
15. Lakhno V., Kazmirchuk S., Kovalenko Y., Myrutenko L., Zhmurko T. Design of adaptive system of detection of cyber-attacks, based on the model of logical procedures and the coverage matrices of features, *Eastern-European Journal of Enterprise Technologies,* 2016, No. 3/9 (81), pp. 30–38. DOI: 10.15587/1729-4061.2016.71769
16. Gamal, M. M., Hasan, B., Hegazy, A.F. A Security Analysis Framework Powered by an Expert System, International Journal of Computer Science and Security, 2011, Vol. 4, No. 6, pp. 505–527.
17. Goztepe, K. Designing Fuzzy Rule Based Expert System for Cyber Security, International Journal of Information Security Science, 2012, Vol. 1, No. 1, pp. 13–19.
18. Robert S. Gutzwiller, Sarah M. Hunt, Douglas S. Lange A task analysis toward characterizing cyber-cognitive situation awareness (CCSA) in cyber defense analysts, Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), *IEEE International Multi-Disciplinary Conference on 21–25 March 2016,* 2016. DOI: 10.1109/COGSIMA.2016.7497780.
19. Loren Paul Reesa, Jason K. Deanea, Terry R. Rakesa, Wade H. Bakerb Decision support for Cybersecurity risk planning, *Decision Support Systems,* 2011, Vol. 51, Iss. 3, pp. 493–505. DOI.org/10.1016/j.dss.2011.02.013
20. Paliwal, S., Gupta, R. Denial-of-Service, Probing & Remote to User (R2L) Attack Detection using Genetic Algorithm, International Journal of Computer Applications, 2012, Vol. 60, No. 19, pp. 57–62.
21. Ben-Asher N., Gonzalez C. Effects of cyber security knowledge on attack detection, Computers in Human Behavior, 2015, Vol. 48, pp. 51–61. DOI: 10.1016/j.chb.2015.01.039
22. Burachok, V. Algorithm for evaluating the degree of protection of special information and telecommunication systems, *Information Security,* 2011, No. 3, pp. 19–27.
23. Valenzuela J., Wang J., Bissinger N. Real-Time Intrusion Detection in Power System Operations, *IEEE Transactions on Power Systems,* 2013, Vol. 28, No. 2, pp. 1052–1062. DOI:10.1109/TPWRS.2012.2224144
24. Potij O. V., Ljenshyn A. V. Doslidzhennja metodiv ocinky ryzykiv bezpeci informacii' ta rozrobka propozycij z i'h vdoskonalennja na osnovi systemnogo pidhodu, *Zbirnyk naukovyh prac' Harkivs'kogo universytetu Povitrjanyh Syl*, 2010, Vyp. 2(24), pp. 85–91.