Journal of Theoretical and Applied Information Technology
31st March 2017. Vol.95. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DEVELOPMENT OF A SUPPORT SYSTEM FOR MANAGING THE CYBER PROTECTION OF AN INFORMATION OBJECT

[1]LAKHNO V.A., [2]KRAVCHUK P. U, [3]MEKHED D.B., [4]MOHYLNYI H.A, [5]DONCHENKO V.U.

[1,2] Department of Managing Information Security, European University, Ukraine
[3] Department cybersecurity and mathematical simulation, Chernihiv National University of Technology, Ukraine
[4,5] Department of Information Technologies and Systems, Luhansk Taras Shevchenko National University, Ukraine
E-mail: [1]lva964@gmail.com, [2]p.kr@ukr.net, [3]d.mekhed@gmail.com, [4]g.mogilniy@gmail.com, [5]donchenko79@mail.ru

ABSTRACT

The architecture of the information object security management system and the intelligent decision support subsystem regarding cyber security operational management is offered particularly in conditions of uncertainty, inconsistency and lack of knowledge about the object security status. 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. 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 (IDSS). It will 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". A program set for IDSS in circuits of organizational-technical and operational management of the information object security system is developed. It is proven that using the developed IDSS allows us to reduce the cost of developing an information security system and to shorten the time for informing some responsible individual about information security incidents.

Keywords: *Information Safety; Information Security Management; Decision Support System; Morphological Approach.*

1. INTRODUCTION

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

For the successful usage of modern ICS it is necessary not only to know how to manage all the functional resources but to create an effective information security management system (ISMS). As management objects – ISMS are difficult organizational-technical structures (OTS), which function in conditions of uncertainty. Effective management of such systems has to be based on innovative information technologies aided by decision support which considers both IS and CS.

The lack of a unified approach to the formation of an effective system of managing cybersecurity IO, in particular information systems, information and communication systems, automated control systems etc., was the motivation for the research towards operational management of IO protection, which in many cases work under uncertainty, inconsistency and incompleteness of knowledge about the IO security state.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

One of the variants of this solution is the usage of a decision support system (DSS) in CS on the basis of intelligent information technologies (IIT). Research into improving existing and the development of new methods, models, algorithms and software (SW) for operational management of information protection (IP) in IO, particularly in conditions of uncertainty, inconsistency and lack of knowledge about ICS status becomes highly relevant.

2. LITERATURE DATA ANALYSIS AND PROBLEM STATEMENT

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 cyber-attack systems [1–4], and also DSS [5, 6] and expert systems (ES) [7–9] in this field. But these studies are basically presented only as formal mathematical models and are not implemented in currently active software. 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]. Unfortunately, the practical experience of such DSC (decision support systems) use is not shown.

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]. In the works [17, 18] all the disadvantages of many DSS and ES systems in the field of IS are shown: lack of highly qualified experts; difficulties that appear in the process of ISMS methods and models adapting to the needs of any particular organization; impossibility of certain ISMS efficiency assessing protection; and demanding true statistics of IS and CS incidents.

It is shown in the works [17, 19, 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. Proposed models are not sufficiently formalized and are difficult for algorithmic submission and program implementation.

On the opinion of some authors [12–14, 17–20], existing standards in the field of IS management don't form effective methods of cyber-security management.

In such a way, according to the disputes in publications [8, 10, 17], dedicated to the potential of using integrated DSS [5, 6] or ES [7, 9, 16] in ISMS, which realize a precautionary strategy of IO cyber-security [15, 20], the task of developing methods, models and applied software 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 and also of IP management in conditions of uncertainty of potential cyberterrorists influences became relevant.

3. FORMULATION OF THE RESEARCH PROBLEMS

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.

It is necessary to solve the following tasks to reach the goal of the research:

1. To develop a model of operational management (OM) of CS IO which allows us to increase IS management efficiency in conditions of information environment status uncertainty, and efficiency of the ISS rational structure planning process.
2. To develop the intelligent decision support system (IDSS) program of IO cyber-security management and to investigate the efficiency of the offered model.

4. INFORMATION SECURITY MANAGEMENT SYSTEM ARCHITECTURE

A model of a problematic situation in the field of CS consists of the three interacting systems: firstly, ISS which potentially can lead to problems with IS; secondly, controlling system (CS) with IS and CS (cyber-security), which is being developed for solving IP problems; thirdly, the environment in which ISS operates. In this case the environment is understood to be a huge number of potential threats for IS and CS.

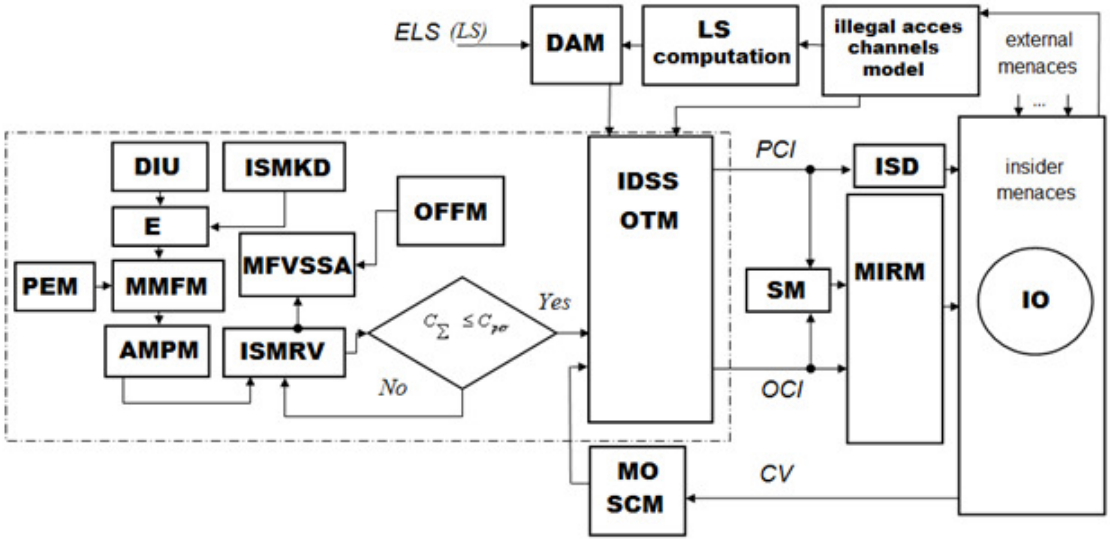
There is one main problem creating the CS – development of the threat model [7, 15, 21], which is connected to the specification of a management object interaction – ISS IO with the environment. IDSS, which develops a threat model building method, is based on a qualified scheme of goal-oriented destructive influences on IS and CS IO [22–24].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A generalized architecture of ISMS and CS is offered according to the results of the control strategy in conditions of uncertainty analysis, fig. 1. Level of safety *(LS)* 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.

Mechanisms of IP control are created in the circuit with organizational-technical control (OTC) governing changing business applications, data array (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. Command information is formed in the process of a goal-oriented choice of an information security method complex rational structure (ISMC).

Operational command information is formed in the CS and IS IO operational management (OM) circuit. This information is distributed to the management object by a security manager or automatically with the help of managing influences realization methods.



key: AMPM – additional matrices processing module; CV – controlled variable; DAM – deviation assessment module; DIU – data insertion unit; E – experts; ELS – entry level of safety; IDSS – intelligent decision of information security operational management (OM) support system; ISD – information security department; ISMKD – information security methods knowledge database; ISMRV – information security methods rational variants; MFVSSA – realization module of compliant firmware full variant set sorting algorithm; MIRM – managing influences realization methods on managing modules in ISM; MMFM – morphological matrices forming module; MO SCM – management object status control module; OCI – operational command information; OFFM – objective function forming module; PCI – planned command information; PEM – pairwise equation matrices; SM – security manager.

Fig. 1. Organizational-technical IP management IDSS structure

Effective solutions are chosen and decided according to the technical features of IP (ISM) as well as according to the IO controlled space status analysis.

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].

Because of the fact that possible ICS topologies can be unequal for the offered ISMS architecture it is appropriate to use a model of a structural-technological reserve (STR) optimization for critically important DA and infrastructure components according to the criterion of minimum probability of a task solving impossibility.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5. INFORMATION OBJECT CYBER-SECURITY OPERATIONAL MANAGEMENT MODEL

The safety level of *i*- IO crosspoint (EIS, ACS and other) is determined by the following formula:

$$LS_i = 1 - IMI_{cis_i}, \quad (1)$$

where IMI_{cis_i} – IS incident importance in *i*- IO crosspoint.

Incident importance IMI_{cis_i} is determined by the following:

$$IMI_{cis_i} = C_{ICR} \cdot At_i \cdot As_i \cdot TL_i \cdot LS_i, \quad (2)$$

where At_i – IS breach level in *i*- IO crosspoint; As_i – data asset (DA) criticality in *i*- IO crosspoint; TL_i – trust level of a device, which reports about IS breaches in *i*- IO crosspoint; LS_i – security measures level in *i*- IO crosspoint; C_{ICR} – coefficient that allows to represent a result in a range [0; 1].

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

$$LS_{CIS} = \prod_{i=1}^{n} (1 - C_{ICR} \cdot At_i \cdot As_i \cdot TL_i \cdot LS_i), \quad (3)$$

where *n* – quantity of crosspoints in IO structure.

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

$$RCA = \langle EST, CE, SS_{ne}, SS_h, PP, O(NN) \rangle, \quad (4)$$

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

where RCA – remote attack against IO; $ICA_{l(m)}$ – internal attack against IA with *k*-level of criticality, which are being processed in NN_m crosspoint, when an attacker has a user account with an access permission to a data, of which level of criticality is not higher than (*k*-1), and he is trying to increase his level of privileges; EST – external source of threat; IST_l^{k-1} – insider source of threat; CE – communication equipment in an information channel; SS_{ne}, SS_h – security services against the method of an attack spreading (networked and host; PP – protocols and packets; O – access object; NN_m^k – IO crosspoint, on which information with the highest level of criticality (*k*) is processed; *l, m* – numbers of crosspoints.

It is proven in works [4, 10, 21–26] 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 cyber-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:

$$\zeta_a \subseteq WCA \times IND = \left\{ \begin{array}{l} (wca_i, ind_j): \\ wca_i \in WCA \ \wedge \\ \wedge\, ind_j \in IND \end{array} \right\}, \quad (5)$$

where $IND = \{ind_j, ind_j\}$ – a network or IO perimeter indicator; WCA – possible spreading ways of cyber-attacks against IO crosspoints; $\zeta_a(wca_i)$ – crossing that determines an indicators set which reacts against the attack on the recent method.

For solving a task in conditions of uncertainty, inconsistency and lack of knowledge about the information environment status under attack, mechanisms of fuzzy inference are activated in IDSS because of the fact that the MO system has some time limits for processing and analysing command information. Incoming information for a fuzzy inference module is the quantity and information value of unusual system events [16, 18, 21]. Information that is formed getting out of a fuzzy inference system corresponds to an outcome variable which is the probability of the fact that a group of unusual events in a network is an attack.

There are some linguistic variables added to IDSS: «number of unusual events in network against the spreading of attack», «number of unusual events in the host», «number of unusual events in IO perimeter», «probability of the fact that found unusual activity is an attack». Following fuzzy sets A, B, C, D with membership functions $\upsilon_{\tilde{A}}, \upsilon_{\tilde{B}}, \upsilon_{\tilde{C}}, \upsilon_{\tilde{D}}$ are added to IDSS:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$A = \{\upsilon_{\tilde{A}}(x) \mid x : \upsilon_{\tilde{A}}(x) \in [0,1],\ x \in X\},$$
$$B = \{\upsilon_{\tilde{B}}(x) \mid x : \upsilon_{\tilde{B}}(x) \in [0,1],\ x \in X\},$$
$$C = \{\upsilon_{\tilde{C}}(x) \mid x : \upsilon_{\tilde{C}}(x) \in [0,1], x \in X\}. \quad (6)$$
$$D = \{\upsilon_{\tilde{D}}(p) \mid p : \upsilon_{\tilde{D}}(p) \in [0,1], p \in [0,1]\},$$

where X – IS events indicators numeric evaluation.

Membership functions of linguistic variables for input and output variables and also for production memory are formed on the basis of expert estimate and results of modeling [6, 8].

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:

$$\langle RO_i, RE_j, DA(RE_j), P_{CA}, P(z_l), OF, RO^{rat}(P_{CA})\rangle, \quad (7)$$

where RO_i – a reaction variant ; RE_j – a result; DA_j – a damage assessment; z – environment status uncertainty characteristic; $P(z_l)$ – l environment status probability; OF – object function of choice; $RO^{rat}(P_{CA})$ – rational variant of reaction; P_{CA} – attack probability.

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 cyber-attack: 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:

$$OF(RO_i, z) = \sum_{l=1}^{s} DA_j(RE_j(RO_i, z_l)) \cdot p(z_l), \quad (8)$$

where $p(z_l) = \prod_{i=1}^{I} p_{ij}(RE_j(RO_i), P_{CA})$.

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

$$p_{ij} = p_{ij}(RE_j(RO_i), P_{CA}),$$
$$\forall i : \sum_j p_{ij} = 1. \quad (9)$$

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

$$RO^{rat}(P_{CA}) = RO(\arg\min_i (OF(RO_i, z))). \quad (10)$$

Threat counteraction methods are developed by an ISS analyst taking into account the possible cases of their spreading. They are developed on the basis of IDSS decision making method choice that is adapted to the reaction optimal variant choice: distant invasion through free-to-join networks, local network invasion, through a radio channel using a wireless hot spot or other [4, 8, 9, 12, 15].

IP operational management intelligent support system is implemented in ISMS to negotiate difficulties with ill-defined situations and for increasing OM quality level.

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

Models [4, 15] consist of five perimeters for decentralized architecture of IO are considered in the research because of a necessity of maximal IDSS structuring.

6. RESULTS OF TESTING THE SOFTWARE SYSTEM «DECISION SUPPORT SYSTEM OF MANAGEMENT PROTECTION OF INFORMATION – DMSSCIS»

The software package "Decision Support System of Management protection of information –

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DMSSCIS» fig. 2, 3, designed for reasoned choice of a rational set of information security in the process of designing information security systems of information objects. DMSSCIS was also used in the modernization of existing information security systems in data centers of transport companies in Chernihiv (2016 p.), Dnipro (2014 p.), Poltava (2013–2014 p.) and several industrial enterprises in Kyiv (Ukraine).

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

Table 1: The results of testing the software system "Decision Support System of Management protection of information - DMSSCIS»

Class of cyber attacks	Options for responding to the current settings information of environment of information object	
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 via Wi Fi or Wi Max	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

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 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

.

Journal of Theoretical and Applied Information Technology
31st March 2017. Vol.95. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

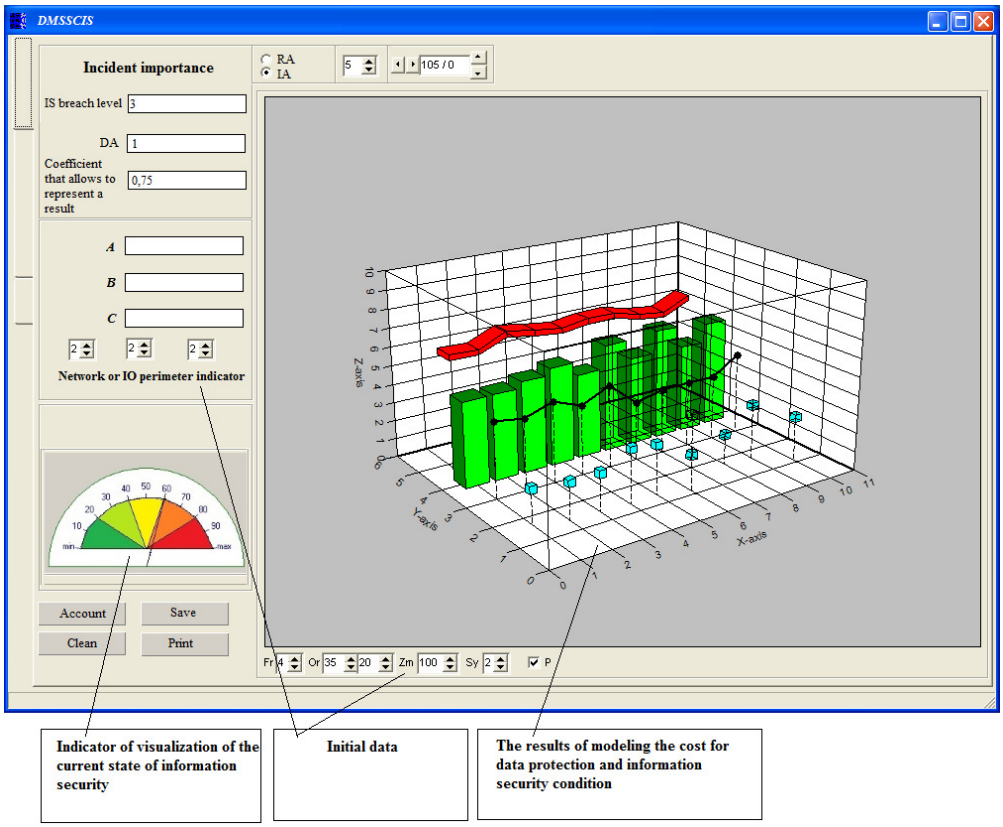
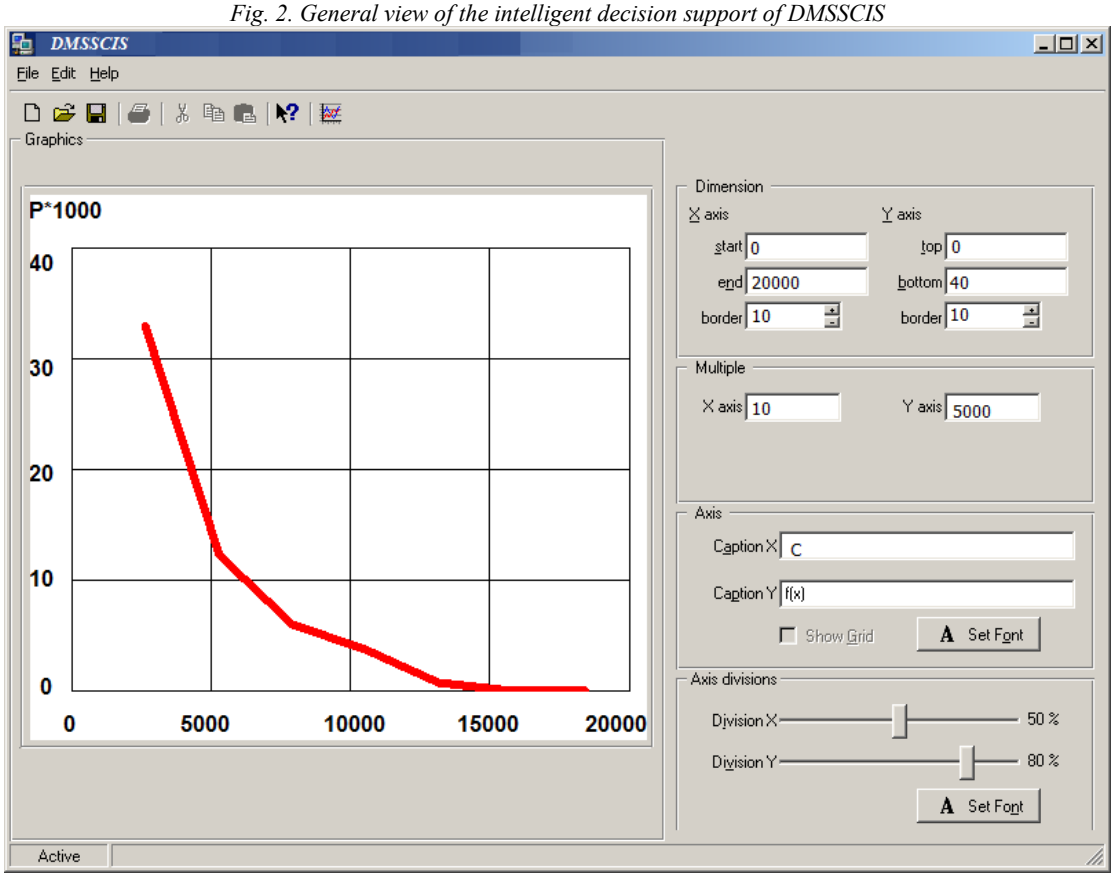


Fig. 2. General view of the intelligent decision support of DMSSCIS



ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

*Fig. 3. S*imulation results module with used DMSSCIS rational set of information security

Fig. 3 shows examples of simulation results by using DMSSCIS rational sets of information security. On Fig. 3 are common simulation results, which show that with the increase in the provision for information security of information objects, the probability of attackers' success of all goals is greatly reduced.

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 information security facility and reduces the time to inform those responsible for information security incidents by 6,9–7,2 times.

7. DISCUSSION OF TEST RESULTS AND PROSPECTS FOR FUTURE RESEARCH

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, 26].

The system of intelligent decision support «DMSSCIS» has the following advantages in comparison with similar systems of decision-making [5, 6]: allows evaluation of the level of information security at the protection facility comprising a plurality of nodes in which information is processed in different levels of criticality; allows specification of the source data on the number of units and segments the information object, given the level of criticality of information resources; ensure prompt evaluation kits of information security; shows a comparative analysis of different systems of information security in risk management; takes into account the specifics of the operation of a specific information object and real threats for key resources.

On a comparative analysis of similar software products [8, 9, 13, 14, 17], the developed decision support system considers various information systems specifics, such as transport, industry, banking and others. This ensures cost reduction for planning the joint hardware and software data protection performance.

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.

Further development of this work may be improving the interaction of traditional mechanisms of information security information objects, which, in particular, are working on primary information system modules and intelligent decision support «DMSSCIS».

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.

8. CONCLUSIONS

1. The model of operational management information and cyber security object forms a rational set of remedies based on morphological approach. 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 information security.

2. A developed software suite was made for intelligent decision support circuits organizational, technical and operational management of information system protection facilities. It confirmed the adequacy of the proposed models and algorithms. 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%.

REFERENCES:

[1] Y. Zhang, L. Wang, W. Sun, R.C. Green, M. Alam, "Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids", IEEE

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Transactions on Smart Grid, Vol. 2, No. 4, 2011 pp. 796–808.

[2] O. Al-Jarrah, A. Arafat, A. "Network Intrusion Detection System using attack behavior classification", *Information and Communication Systems (ICICS), 2014 5th International Conference 2014*, pp. 1–6.

[3] P. Louvieris, N. Clewley, X. Liu, "Effects-based feature identification for network intrusion detection", *Neurocomputing*, Vol. 121, Iss. 9, 2013, pp. 265–273.

[4] V. Lakhno, "Creation of the adaptive cyber threat detection system on the basis of fuzzy feature clustering", *Eastern–European Journal of Enterprise Technologies*, Vol. 2, No 9(80), 2016, pp. 18–25.

[5] E. Panaousis, A. Fielder, P. Malacaria, C. Hankin, F. Smeraldi, "Cybersecurity Games and Investments: A Decision Support Approach", *Chapter Decision and Game Theory for Security of the series Lecture Notes in Computer Science*, Vol. 8840, 2014, pp. 266–286.

[6] H. Cavusoglu, R. Srinivasan, T.Y. Wei, "Decision-theoretic and game-theoretic approaches to IT security investment", *Journal of Management Information Systems (ACySe)*, Vol. 25(2), 2008, 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 (iFUZZY),* 2013, pp. 346 – 351.

[8] L. Atymtayeva, K. Kozhakhmet, G. Bortsova, "Building a Knowledge Base for Expert System in Information Security", *Chapter Soft Computing in Artificial Intelligence of the series Advances in Intelligent Systems and Computing*, Vol. 270, 2014, pp. 57–76.

[9] M. Kanatov, L. Atymtayeva, B. Yagaliyeva, "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.

[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 Science*s, Vol. 232, 2013, pp. 482–500. http://dx.doi.org/10.1016/j.ins.2011.09.012

[11] W. Kearney, H. Kruger, H. "Theorising on risk homeostasis in the context of information security behavior", *Information and Computer Security*, Vol. 24 Iss: 5., 2015. pp. 496 – 513.

[12] O. Linda, M. Manic, T. Vollmer, J. Wright, "Fuzzy logic based anomaly detection for embedded network security cyber sensor", *Computational Intelligence in Cyber Security (CICS),* IEEE Symposium on 11–15 April 2011, pp. 202–209.

[13] L. Demetz, D. Bachlechner, "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.

[14] A. Oglaza, R. Laborde, P. Zarate, "Authorization Policies: Using Decision Support System for Context-Aware Protection of User's Private Data, Trust", *Security and Privacy in Computing and Communications (TrustCom), 2013*, 12th IEEE International Conference on 16–18 July 2013, pp. 1639-1644.

[15] V. Lakhno, S. Kazmirchuk, Y. Kovalenko, L. Myrutenko, T. Zhmurko, "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*, No 3/9 (81), 2016, pp. 30–38.

[16] M.M. Gamal, B. Hasan, A. F. Hegazy, "A Security Analysis Framework Powered by an Expert System", *International Journal of Computer Science and Security (IJCSS)*, Vol. 4, No. 6, 2011, P. 505–527.

[17] K. Goztepe, "Designing Fuzzy Rule Based Expert System for Cyber Security", *International Journal of Information Security Science*, 2012, Vol. 1, No 1, pp.13–19.

[18] R.S. Gutzwiller, S. M. Hunt, D. 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)*, 2016 IEEE International Multi-Disciplinary Conference on 21–25 March 2016. pp. 1.

[19] L. P. Reesa, J.K. Deanea, T. R. Rakesa, W. H. Bakerb, "Decision support for Cybersecurity risk planning", *Decision Support Systems*, Vol. 51, Iss. 3, 2011, pp. 493–505.

[20] S. Paliwal, R. Gupta, "Denial-of-Service, Probing & Remote to User (R2L) Attack Detection using Genetic Algorithm",

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

International Journal of Computer Applications, Vol. 60, No.19, 2012, pp. 57–62.

[21] N. Ben–Asher, C. Gonzalez, "Effects of cyber security knowledge on attack detection", *Computers in Human Behavior*, Vol. 48, 2015, pp. 51–61.

[22] R. Verma, M. Kantarcioglu, D. Marchette, E. Leiss, T. Solorio, "Security Analytics: Essential Data Analytics Knowledge for Cybersecurity Professionals and Students", *IEEE Security & Privacy*, Vol. 13, Iss. 6, 2015, pp. 60–65.

[23] J. Valenzuela, J. Wang, N. Bissinger, "Real-Time Intrusion Detection in Power System Operations", *IEEE Transactions on Power Systems*, Vol. 28, No. 2, 2013, pp. 1052–1062.

[24] O. Al-Jarrah, A. Arafat, "Network Intrusion Detection System using attack behavior classification", *Information and Communication Systems (ICICS)*, 2014 5th International Conference, pp. 1–6.

[25] K. Kritikos, P. Massonet, "Security-Based Adaptation of Multi-Cloud Applications", *Chapter Data Privacy Management, and Security Assurance of the series Lecture Notes in Computer Science*, Vol. 9481, 2016, pp. 47–64.

[26] O.I. Garasymchuk, Y. M. Kostiv, "Assessment of the effectiveness systems protection of information", *Vestnik KNU imeni Mikhaila Ostrogradskogo*, Vol. 1, Iss. 66, 2011, pp. 16–20.