Розроблені метод та модель управління кіберзахистом об'єкта інформатизації, які базуються на комплексному впровадженні системи підтримки прийняття рішень у завданнях захисту інформації. Система дозволяє аналітикам працювати в режимі он-лайн. Це істотно скорочує часові та експертні ресурси в процесі прийняття управлінських рішень з інформаційної безпеки. Наведено результати тестування програмного комплексу «Система підтримки прийняття рішень по керуванню кібербезпекою підприємства»

Ключові слова: кібербезпека, об'єкт інформатизації, система підтримки рішень, експертна оцінка, метод Дельфі

Разработаны метод и модель управления киберзащитой объекта информатизации, базирующиеся на комплексной имплементации системы поддержки принятия решений в задачи защиты информации. Система позволяет аналитикам работать в режиме on-line, что существенно сокращает временные и экспертные ресурсы в процессе принятия управленческих решений по информационной безопасности. Приведены результаты тестирования программного комплекса «Система поддержки принятия решений по управлению кибербезопасностью предприятия»

Ключевые слова: кибербезопасность, объект информатизации, система поддержки решений, экспертная оценка, метод Дельфи

UDC 004.056
DOI: 10.15587/1729-4061.2017.111081

MANAGEMENT OF INFORMATION PROTECTION BASED ON THE INTEGRATED IMPLEMENTATION OF DECISION SUPPORT SYSTEMS

V. Lakhno
Doctor of Technical Science, Professor
Department of Managing Information Security
European University
Akademika Vernadskoho blvd., 16 V, Kyiv, Ukraine, 03115
E-mail: lva964@gmail.com
V. Kozlovskyi
Doctor of Technical Sciences, Professor
Department of Technical Information Security Tools*
E-mail: vvkzeos@gmail.com
Y. Boiko
PhD, Associate Professor
Department of Information Technology Security*
E-mail: julia_boyko2010@ukr.net
A. Mishchenko
Doctor of Technical Science, Professor
Department of Information Security Protection*
E-mail: partpravo@i.ua
I. Opirskyy
PhD, Associate Professor
Department of Information Security
Lviv Polytechnic National University
Stepana Bandery str., 12, Lviv, Ukraine, 79013
E-mail: iopirsky@gmail.com
*National Aviation University
Kosmonavta Komarova ave., 1, Kyiv, Ukraine, 0305

1. Introduction

Current stage of development of the postindustrial society has been accompanied by a rise in the number and complexity of cyberattacks against various IO – information-communication system (ICS), automated control systems, etc. More and more funds are allocated every year on cybersecurity (CS) and information protection (IP) is appropriated more funds [1]. Global practice, however, has demonstrated vividly that a simple increase in the number of means and activities on IP does not always produce a tangible effect [2], while in certain situations [3] it only adds up to the workload of stuff of companies and in organizations. Thus, a new promising alternative direction emerges for providing IO CS based on employing intelligent information technologies of cyber defense. Such technologies include decision support systems (DSS) for IP and CS [4]. The relevance of present study is determined, above all, by the state of problems in IP and the management level of CS under conditions of growing number and complexity of intentional destructive attacks on the enterprises' ICS.

The research relevance is predetermined by the need for further development of the methodological apparatus, which allows implementation of the new intelligent DSS into management tasks on information protection and cybersecurity at various objects of informatization.

2. Literature review and problem statement

An increase in the intensity and complexity of cyberattacks, primarily targeted at ICS, has sparked interest in the

development of intelligentized systems of IP and management of cyber safety [5, 6]. The need for operational decision-making related to the management of IP has rendered promising the studies into development of decision support systems (DSS) [7] and expert systems (ES) [8] in this field. Appropriately developed are the new methods, models, algorithms, and application software (SW) within the framework of creation of intelligentized DSS and ES.

In papers [9, 10], authors analyzed models for estimating risks for CS at the objects of informatization by using ES. The studies have failed to introduce any application software to the market.

Articles [11, 12] describe a decision-making procedure in the ICS IP situations that are not structured sufficiently enough. The research [12] did not result in any hardware/software implementation.

The practice of employing DSS and ES for the tasks on managing IP and CS at separate enterprises was outlined in [13, 14]. As shown in [15, 16], the existing commercial DSS and ES for the information (IS) and cybersecurity are of closed character, and their acquisition by individual enterprises implies significant financial costs. At the same time, the existing non-profit DSS and ES for information protection lack functionality.

As shown in [17], the problem of the integrated implementation of DSS and ES was not systematically addressed in the context of management tasks for IS.

Given the conclusions drawn by authors of [7, 8, 12], there is still an unresolved problem on the systemic implementation of intelligentized DSS and ES into the management tasks on IP. Support for a decision-making procedure and quality expert assessment allow solving the tasks of IS and CS in the most efficient way. A decision can be based on the models that take into account different expert interval estimates of the degree of IO protection. Thus, conceptually innovative approaches can be based on the paradigm of integrated implementation of DSS for the tasks of IP and for providing cybersecurity.

3. The aim and objectives of the study

The aim of present work is to develop a method and a model for managing cybersecurity at the objects of informatization based on the automation of a procedure of coordination of expert opinions in a DSS.

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

– to develop a method and a model for managing IS based on the systemic DSS implementation into tasks on managing cybersecurity of IO;

– to design and test IO cyber security management DSS based on the application of the Delphi method, which would as well as take into account the IS interval estimates and metrics for different classes of threats, anomalies, and cyber-attacks.

4. A method and a model for managing protection of an informatization object based on the systemic DSS implementation

In the process of project implementation, a critical part of development as a whole is the correct definition of the problem – management of protection of informatization objects on the basis of integrated implementation of decision support systems on cybersecurity. The approaches, analyzed in [1–5], aimed at providing cybersecurity of IO, which imply extensive build-up of means and activities on IP, do not always guarantee reliable protection. Expert systems, including adaptive [4, 8, 14], and DSS do not eliminate the need for antivirus software, intrusion detection systems, etc. However, in the complex situations on IO cyber security in which the outcome of the task depends on subjective knowledge, the effect of their implementation into integrated IPS is sufficiently high.

The proposed method for the IO protection management includes the following stages:

Stage 1. Analysts perform division of the tasks on IO protection. For example, category 1: formation of requirements and a comprehensive information protection system (IPS) and objects of protection, based on the characteristics of OI; category 2: systematization and updating of information arrays on IPS and IO protection objects; category 3: analytics, control and analysis of effectiveness of the mechanisms of IO cyber security; category 4: working out (correction) of decisions on IO protection management.

Stage 2. The formalization of requirements to the IS management processes for IO is performed. Logical rules for DSS on IS are created.

Stage 3. Knowledge base (KB) is compiled for DSS with the participation of analysts (experts).

The implementation of a systemic approach to the tasks on managing protection of IO employing a DSS, in particular under on-line mode, is represented by the formalization of a support process in the form of program modules for the situation center (SC) on cybersecurity, Fig. 1. Support of the process of interviewing experts (analysts) in DSS under on-line mode predetermined the choice of an interactive- dialog mode of system operation. Emphasis is placed on the tasks of evaluating parameters of IO protection, as well as a predictive estimate of situation transformation during detection of threats, anomalies or targeted cyber-attacks. External experts who evaluate different parameters of IO protection can, by using their own portal (shown in green in Fig. 1), employing a DSS or independently, give a necessary assessment of the situation.

When registered on the portal related to DSS, the user account is created on the server. This allows the analyst to participate in subsequent surveys and studies, including expert evaluation of the situation.

For example, experts, independently or with the help of a DSS, are encouraged to identify parameters of interaction between the sources of threats and their destructive influences on IO.

Experts, independently or in collaboration with a DSS, fill in questionnaires in the form of matrix:

$$e_i = \begin{bmatrix} 11 & \dots & MI \\ \vdots & \ddots & \vdots \\ N1 & \dots & NMI \end{bmatrix}, \quad (1)$$

where N is the number of sources of threats for the analyzed IO; MI is the number of techniques to implement each threat. i is the number of experts working with a DSS.

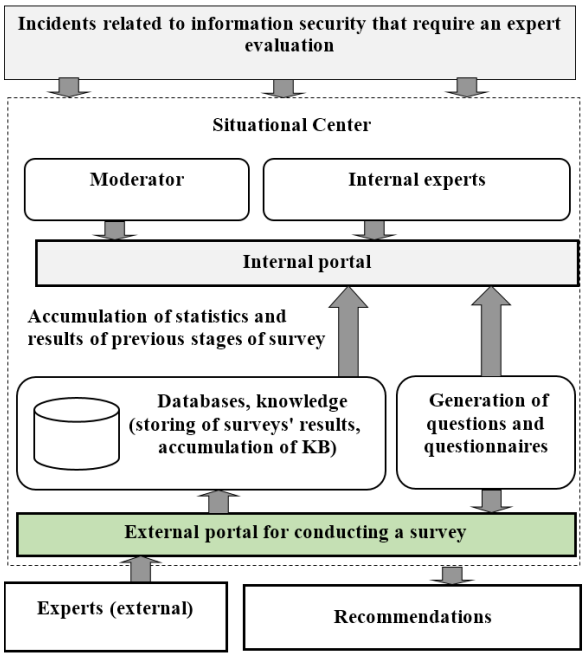

Fig. 1. Structural diagram of the platform for expert estimation of the informatization object protection using a DSS under on-line mode

Prior to the stage of coordination of the experts' opinions (e) at round (r) and reaching a consensus, the summary matrix takes the form:

$$e_r = \sum_{i=1}^{n} \begin{bmatrix} 11 & \dots & MI \\ \vdots & \ddots & \vdots \\ N1 & \dots & NMI \end{bmatrix}. \quad (2)$$

Processing of experts' opinions in a DSS is based on the Delphi method. A distinctive feature of the designed system is the capability to dynamically generate questionnaire forms using the frames in each round of the survey under on-line mode.

Upon completion of filling the questionnaire forms, the Web page that is connected to the DSS dynamically displays tabular and graphical results.

Stage 4. Systematization of the obtained data is performed by the minimally significant components of the object of protection. A procedure is implemented of assigning a category to the determined classifiers – threats to IO; state of ICS for IO; the recommended methods and tools to protect information, etc. As a result, the metadata for KB are created and the principles of formation of new knowledge or rules for the DSS are synthesized.

Stage 5. Given the dynamics of emergence of new types of destructive influence on IO [18, 19], a degree of adjustment of classifiers is determined. The models of their interaction are refined [20, 21]. At this stage, the logical rules are formed for a dynamical change in the expert assessments for possible classifiers.

Reaching a consensus among experts in the process of DSS operation under on-line mode is based on the application of the Delphi method [22–24]. The method proposed, taking into account results of [7, 14], is supplemented by a model of expert assessments coordination, which considers different interval estimations and metrics of IS [25, 26] for the known threats, anomalies and cyber-attacks [14, 27, 28].

Interval estimates of the situation transformation related to the assessment of IO protection are described as follows:

$$\overline{ER}_{ps} = \left\{ \overline{ER}_{pse} \mid e = \overline{1, E_{ps}} \right\}; \quad (3)$$

$$\overline{ER}_{pse} = \left\{ \left[\overline{ER}^{-}_{psew}; \overline{ER}^{+}_{psew} \right] \mid w = \overline{1, W} \right\}, \quad (4)$$

where ER_{pse} is the expert estimate for the w-th level [8, 22, 23], the e-th expert, relative to the s-th indicator for estimated parameter p.

Interval estimates are correlated with the metrics of IS [14, 25, 26].

In accordance with [14, 25, 26], for the interval estimates of IO protection (similarly for other parameters), the IS metrics are assigned:

$$me_{g_{pse_i w}, g_{pse_j w}} = \left(1/W \right) \cdot \sum_{w=1}^{W} me_{g_{pse_i e_j w}}, \quad (5)$$

where

$$g_{psew} = \left[g^{-}_{psew}; g^{+}_{psew} \right].$$

Significance of the opinion of the e-th expert was evaluated as follows:

$$op_{pse} = \left(1 - me\left(\overline{ER}_{pse}, \tilde{ER} \right) \right) \cdot C_{pse}, \quad (6)$$

where C_{pse} is the competence of the expert relative to the analyzed metric of IP.

Expression (6) allows us to analyze the results when one group of experts employed DSS while another did not. In this case, the results being compared differ [23, 24].

The average interval estimate is calculated as follows:

$$\overline{ES}^{-}_{psw} = \left(1/E \right) \cdot \sum_{e=1}^{E_{ps}} \overline{ER}^{-}_{psew}; \quad (7)$$

$$\overline{ES}^{+}_{psw} = \left(1/E \right) \cdot \sum_{e=1}^{E_{ps}} \overline{ER}^{+}_{psew}. \quad (8)$$

Integral expert estimate in DSS:

$$\overline{\overline{ER}}^{-}_{psw} = \arg\min_{\overline{ER}^{-}_{psew}} \left(\left| \overline{ER}_{psew} - \overline{ES}^{-}_{psew} \right| \right); \quad (9)$$

$$\overline{\overline{ER}}^{+}_{psw} = \arg\min_{\overline{ER}^{+}_{psew}} \left(\left| \overline{ER}_{psew} - \overline{ES}^{+}_{psew} \right| \right). \quad (10)$$

In the analytical module of DSS, confidence interval of the first round of expert estimate of the situation was determined as follows:

$$\overline{ER}_{pse} \in T_{ps}, then\ \overline{ER}_{pse} = \arg\min_{\overline{ER}_{pse}} \left(\widetilde{me}_{pse} \right), \quad (11)$$

where T is the time of situation's transformation related to the assessment of IS parameter – p.

For the first round of experts' survey using DSS, the resulting confidence interval determines the radius of the set of expert estimates:

$$RA^{(T_{ss})} = \max_{\overline{ER}_{pse}} \left(\widetilde{me} \right). \quad (12)$$

Confidence interval in the subsequent rounds was determined as follows:

$$\overline{ER}_{pse} \in T_{ps}, then \ \widetilde{me} < RA^{(T_{ps})}. \quad (13)$$

Summary expert assessment in DSS was determined as follows:

$$\widehat{ER}_{ps} = 0{,}5 \cdot \left(ES^{+}_{psw\left(\widehat{ER}_{ps}\right)} + ES^{-}_{psw\left(\widehat{ER}_{ps}\right)} \right). \quad (14)$$

Thus, the model that enables coordination of expert opinions and takes into account interval estimates and IS metrics, makes it possible to fill DSS KB. Correction of KB is also possible in the case of detecting new knowledge or discrepancies between expert estimates.

Stage 6. The rules are worked out for the evaluation of compliance of the selected comprehensive IPS with IS requirements. Thanks to the developed DSS, there is the possibility of correcting the decisions based on operative assessment of the current state of IO protection.

Stage 7. Basic management concepts are generated, as well as rules and guidelines on response and timely application of preventive, governing, correcting and other influences on events related to IS incidents at IO.

Stage 8. Long-term plans are devised for the development of integrated IPS for IO.

If necessary, stages 1–8 can be repeated with regard to correction of ES and DSS KB.

5. Software complex "Decision support system for managing cyber security of an enterprise – DMSSCSE"

In order to implement DSS in software, we chose MySQL, HTML, CSS, which allowed us to develop an intuitive interface, Fig. 2. To implement modules for the information and graphic representation of results, we used the programming language Python.

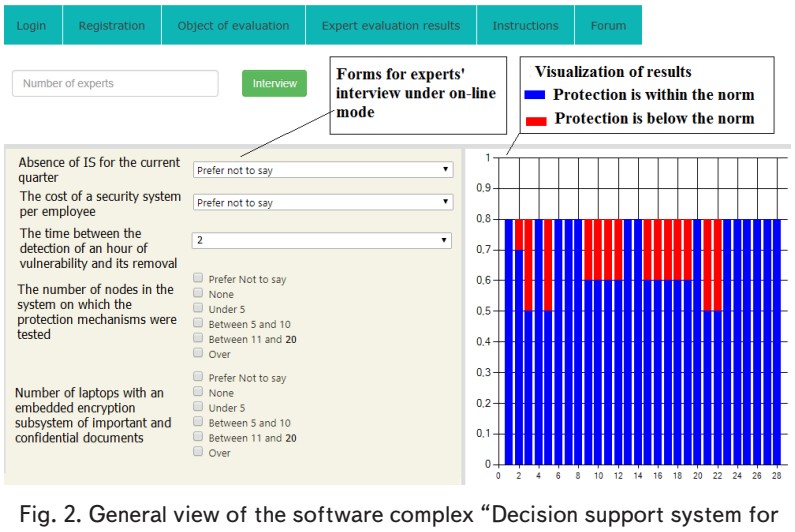

Fig. 2. General view of the software complex "Decision support system for managing cyber security of enterprises – DMSSCSE" (for the work of experts on-line)

DSS "DMSSCSE" was tested during modernization of IPS in computer centers at enterprises in Kyiv, Lviv, Chernihiv and others (Ukraine).

Fig. 3, 4 show comparative results obtained during interviewing the experts, independently and using the DSS "DMSSCSE". From 7 to 11 experts were involved for the enterprises participating in the testing of DSS. We invited experts with experience in the field of information protection not less than 5 years. Without the DSS "DMSSCSE", the experts filled in questionnaires evaluating ICS protection parameters of the analyzed enterprises. At the second stage of the study, the experts were asked to perform the evaluation using the DSS "DMSSCSE".

Fig. 3 shows results of the evaluation of experts of vulnerability of the analyzed enterprise, independently and using the DSS "DMSSCSE" [13, 14]. Figure 4 shows results of the evaluation of the enterprises' web-sites. Reference value of the estimated parameters (p) was accepted equal to 1 [3, 14, 17]. If the parameter's estimate is equal to 0 – protection is missing.

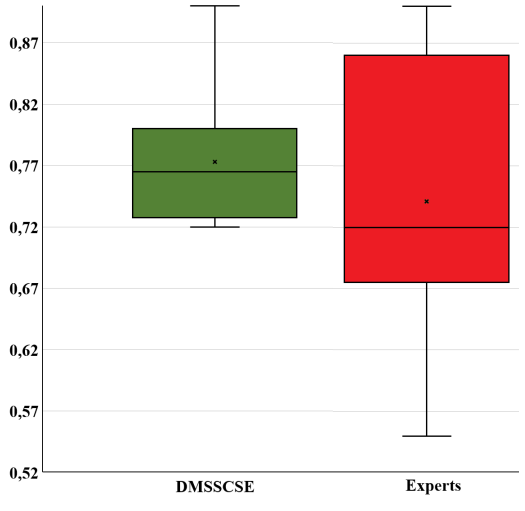

Fig. 3. Results of experts' evaluation of the degree of ICS vulnerability, independently and using the interface of "DMSSCSE"

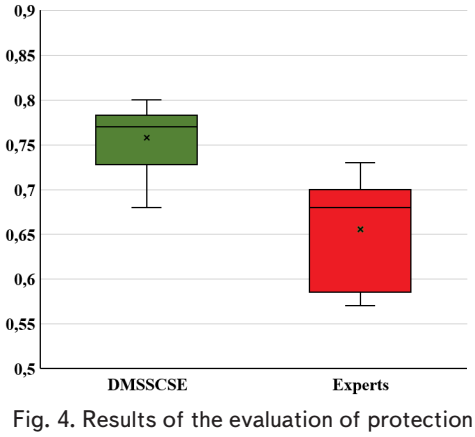

Fig. 4. Results of the evaluation of protection of the enterprises' web-sites

Fig. 3, 4 show that a divergence in the opinion of experts who employed "DMSSCSE" is about 15–18 % less than for the variant of evaluation without using the DSS.

Fig. 5 shows results of the experts' evaluation of vulnerability of the enterprises' computing centers [3, 14], independently (red bars) and using the DSS "DMSSCSE" (green bars).

The results obtained show that when not using the DSS "DMSSCSE" experts estimate protection of ICS more optimistically. However, the follow-up audit of IS of the analyzed enterprises did not always confirm the assessment of experts and the received estimations were more consistent with the variant that employed the DSS "DMSSCSE". In this case, the IS audit was conducted by analysts with an experience in the field of information protection of not less than 10 years.

Fig. 6 shows comparison histogram of time (in minutes) spent by the experts, independently (red bars) and using the interface of "DMSSCSE" (green bars), to evaluate signs of unauthorized access to the information system of an enterprise's computing center.

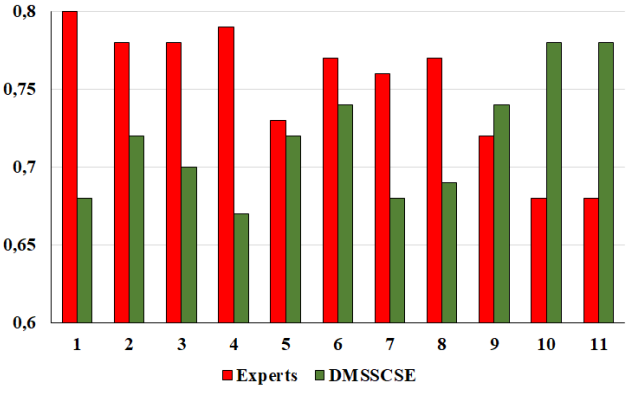

Fig. 5. Results of the experts' evaluation, independently and using the interface of "DMSSCSE", of the degree of protection of enterprises' computing centers

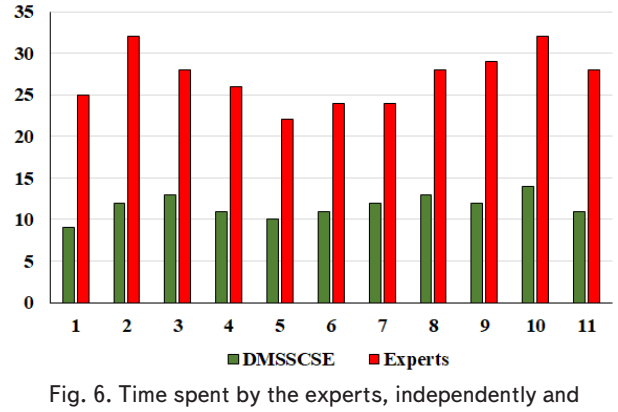

Fig. 6. Time spent by the experts, independently and using the interface of "DMSSCSE", to evaluate signs of unauthorized access to the information system of an enterprise

Fig. 7 shows comparison histogram of the time taken to assess protection of an enterprise's web-site.

The time spent by experts for data processing using "DMSSCSE" is 35–50 % less compared to an independent analysis by the analysts. In addition, the number of rules involved in the process of logical output of "DMSSCSE" is 1.5 times larger. The result of the use of the interface of DSS "DMSSCSE" in computing centers at the enterprises in Kyiv, Chernihiv, Lviv is a reduction in costs for the organization of cyber protection by 32 35 %. Reducing the time needed for the evaluation (using the DSS) and response to cyber incidents by 11–14 % allows us to argue about improvements in the effectiveness of IS management system. In the course of testing the DSS, we also verified mechanisms of the interaction between experts and "DMSSCSE" in the synthesis of governing rules for the tasks on managing protection of IO.

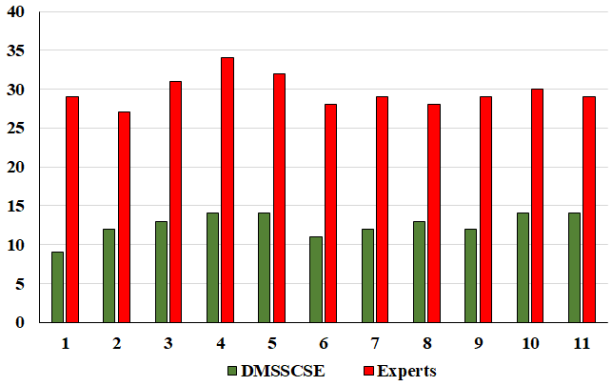

Fig. 7. Time spent to estimate protection of an enterprise's web-site

6. Discussion of results of testing DSS and the prospects for further research

The method and the model proposed form a set of basic rules and establish relations between the subclasses of cyberattacks and IS incident categories. Expert assessment (using the DSS "DMSSCSE") of action against IS of the object of protection, as well as coordination of judgments by experts, make it possible to predict the categories of CS incidents for the existing and new classes of cyberattacks. In the course of testing, the time needed to assess threats to IO was reduced by 11–12 %. The application of DSS "DMSSCSE" decreased the cost of organizing integrated IPS by 12–15 % (compared with alternative techniques [2, 6, 10, 25]).

It was established that the application of DSS "DMSSCSE" makes it possible to reduce expenses for the organization of integrated IPS by 12–15 % compared with alternative methods [2, 6, 10, 25]. The described solutions complement existing studies [4, 8, 11, 17], in the context of solving tasks on managing protection of IO based on the implementation into comprehensive IPS of DSS on cybersecurity. The results obtained allowed us to recommend the DSS "DMSSCSE" for the implementation into integrated IPS at a number of enterprises in the cities of Kyiv and Dnipro.

When compared to similar solutions reviewed in papers [8, 11, 17], ES and DSS "DMSSCSE" has the following advantages:

– it is possible to integrate the developed software into existing comprehensive IPS;

– the efficiency of decision-making in the tasks on managing information protection of IO improves;

– a flexible adjustment of the DSS is possible with regard to the specificity of IO protection.

The shortcoming of DSS "DMSSCSE", identified in the process of testing, is the need to engage, at an early stage of the formation of knowledge base, independent experts familiar with the characteristics of protection of a particular IO.

A promising direction for development of the present work is to fill the knowledge base and the database of logical rules for DSS taking into account the expansion of test information and the results of approbation of "DMSSCSE".

7. Conclusions

1. We developed the method and the model for managing protection of the objects of informatization, based on the integrated implementation of decision support systems for the tasks on cybersecurity. The proposed solutions differ from those that already exist by the possibility to automate the procedure of generating variants for controlling actions using the DSS. The described model, based on the Delphi method, makes it possible to conduct the survey and coordinate expert opinions, including taking into account various interval estimations of the degree of protection, as well as the information safety metrics at different objects of informatization.

2. We designed and tested under actual conditions at the enterprises of Ukraine a software complex "Decision support system for managing cyber security of enterprises – DMSSCSE". The DSS is adapted for the work of experts on-line. It was established that DSS "DMSSCSE" makes it possible to improve effectiveness of the applied organizational and technical measures to protect objects of informatization, as well as to reduce the cost of organizing comprehensive information security systems by 12–15 % compared with the existing solutions.

References

1. Radziwill, M. Cybersecurity Cost of Quality: Managing the Costs of Cybersecurity Risk Management [Electronic resource] / M. Radziwill, M. C. Benton // arXiv. – 2017. – Available at: https://arxiv.org/ftp/arxiv/papers/1707/1707.02653.pdf
2. Jalali, M. S. Decision Making and Biases in Cybersecurity Capability Development: Evidence from a Simulation Game Experiment [Electronic resource] / M. S. Jalali, M. Siegel, S. Madnick // arXiv. – 2017. – Available at: https://arxiv.org/ftp/arxiv/papers/1707/1707.01031.pdf
3. Gordon, L. A. Investing in Cybersecurity: Insights from the Gordon-Loeb Model [Text] / L. A. Gordon, M. P. Loeb, L. Zhou // Journal of Information Security. – 2016. – Vol. 07, Issue 02. – P. 49–59. doi: 10.4236/jis.2016.72004
4. 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
5. Kim, K. National cyber security enhancement scheme for intelligent surveillance capacity with public IoT environment [Text] / K. Kim, I. Kim, J. Lim // The Journal of Supercomputing. – 2016. – Vol. 73, Issue 3. – P. 1140–1151. doi: 10.1007/s11227-016-1855-z
6. Li, S. Securing the Internet of Things [Text] / S. Li, L. D. Xu. – Syngress, 2017. – 154 p.
7. 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
8. 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
9. Medhat, K. Security in Mission Critical Communication Systems [Text] / K. Medhat, R. A. Ramadan, I. Talkhan // Advances in Wireless Technologies and Telecommunication. – 2017. – P. 270–291. doi: 10.4018/978-1-5225-2113-6.ch012
10. Mai, B. Neuroscience Foundations for Human Decision Making in Information Security: A General Framework and Experiment Design [Text] / B. Mai, T. Parsons, V. Prybutok, K. Namuduri // Lecture Notes in Information Systems and Organisation. – 2016. – P. 91–98. doi: 10.1007/978-3-319-41402-7_12
11. Elnajjar, A. E. A. DES-Tutor: An Intelligent Tutoring System for Teaching DES Information Security Algorithm [Text] / A. E. A. Elnajjar, S. S. A. Naser // International Journal of Advanced Research and Development. – 2017. – Vol. 2, Issue 1. – P. 69–73.
12. 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
13. Farhangi, H. Cyber-Security Vulnerabilities: An Impediment Against Further Development of Smart Grid [Text] / H. Farhangi // Power Systems. – 2016. – P. 77–93. doi: 10.1007/978-3-319-28077-6_6
14. Lakhno, V. Development of adaptive expert system of information security using a procedure of clustering the attributes of anomalies and cyber attacks [Text] / V. Lakhno, Y. Tkach, T. Petrenko, S. Zaitsev, V. Bazylevych // Eastern-European Journal of Enterprise Technologies. – 2016. – Vol. 6, Issue 9 (84). – P. 32–44. doi: 10.15587/1729-4061.2016.85600
15. 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.
16. Garae, J. Visualization and Data Provenance Trends in Decision Support for Cybersecurity [Text] / J. Garae, R. K. L. Ko // Data Analytics. – 2017. – P. 243–270. doi: 10.1007/978-3-319-59439-2_9
17. Lakhno, V. Development of the intelligent decision-making support system to manage cyber protection at the object of informatization [Text] / V. Lakhno, Y. Boiko, A. Mishchenko, V. Kozlovskii, O. Pupchenko // Eastern-European Journal of Enterprise Technologies. – 2017. – Vol. 2, Issue 9 (86). – P. 53–61. doi: 10.15587/1729-4061.2017.96662

18. Page, J. Directors' liability survey: Cyber attacks and data loss–a growing concern [Text] / J. Page, M. Kaur, E. Waters // Journal of Data Protection & Privacy. – 2017. – Vol. 1, Issue 2. – P. 173–182.
19. Guo, J. Cyber-Physical Power System (CPPS) reliability assessment considering cyber attacks against monitoring functions [Text] / J. Guo, Y. Wang, C. Guo, S. Dong, B. Wen // 2016 IEEE Power and Energy Society General Meeting (PESGM). – 2016. doi: 10.1109/pesgm.2016.7741899
20. Computational Intelligence, Cyber Security and Computational Models [Text] / G. S. S. Krishnan, R. Anitha, R. S. Lekshmi, M. S. Kumar, A. Bonato, M. Graña (Eds.). – Springer Science & Business Media, 2014. – 416 p. doi: 10.1007/978-81-322-1680-3
21. Liu, X. Trilevel modeling of cyber attacks on transmission lines [Text] / X. Liu, Z. Li // IEEE Transactions on Smart Grid. – 2017. – Vol. 8, Issue 2. – P. 720–729. doi: 10.1109/tsg.2015.2475701
22. Nugraha, Y. An Adaptive Wideband Delphi Method to Study State Cyber-Defence Requirements [Text] / Y. Nugraha, I. Brown, A. S. Sastrosubroto // IEEE Transactions on Emerging Topics in Computing. – 2016. – Vol. 4, Issue 1. – P. 47–59. doi: 10.1109/tetc.2015.2389661
23. Johnson, A. M. Business and Security Executives Views of Information Security Investment Drivers: Results from a Delphi Study [Text] / A. M. Johnson // Journal of Information Privacy and Security. – 2009. – Vol. 5, Issue 1. – P. 3–27. doi: 10.1080/15536548.2009.10855855
24. Pruitt-Mentle, D. A Delphi Study of Research Priorities in Cyberawareness [Electronic resource] / D. Pruitt-Mentle // Educational Technology Policy, Research and Outreach-CyberWatch. – 2011. – Available at: http://www.c3schools.org/etpro/Documents/2011/CISSE/Delphi_study_CISSE_2011_short_paper.pdf
25. Savola, R. M. Towards a taxonomy for information security metrics [Text] / R. M. Savola // Proceedings of the 2007 ACM workshop on Quality of protection – QoP '07. – 2007. – P. 28–30. doi: 10.1145/1314257.1314266
26. Rostami, M. A Primer on Hardware Security: Models, Methods, and Metrics [Text] / M. Rostami, F. Koushanfar, R. Karri // Proceedings of the IEEE. – 2014. – Vol. 102, Issue 8. – P. 1283–1295. doi: 10.1109/jproc.2014.2335155
27. Aggarwal, P. Cyber-Security: Role of Deception in Cyber-Attack Detection [Text] / P. Aggarwal, C. Gonzalez, V. Dutt // Advances in Intelligent Systems and Computing. – 2016. – P. 85–96. doi: 10.1007/978-3-319-41932-9_8
28. Dang, Y. Anomaly Detection for Data Streams in Large-Scale Distributed Heterogeneous Computing Environments [Text] / Y. Dang, B. Wang, R. Brant, Z. Zhang, M. Alqallaf, Z. Wu // ICMLG2017 5th International Conference on Management Leadership and Governance. – 2017. – P. 121.
29. 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
30. Liang, G. The 2015 Ukraine Blackout: Implications for False Data Injection Attacks [Text] / G. Liang, S. R. Weller, J. Zhao, F. Luo, Z. Y. Dong // IEEE Transactions on Power Systems. – 2017. – Vol. 32, Issue 4. – P. 3317–3318. doi: 10.1109/tpwrs.2016.2631891