Journal of Theoretical and Applied Information Technology
31st July 2018. Vol.96. No 14

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

DEVELOPMENT OF A DECISION SUPPORT SYSTEM BASED ON EXPERT EVALUATION FOR THE SITUATION CENTER OF TRANSPORT CYBERSECURITY

[1] LAKHNO V., [2] AKHMETOV B., [3] KORCHENKO A., [4]ALIMSEITOVA Z. [5]GREBENUK V.

[1]Department of Cyber Security, European University, Ukraine
[2]Caspian state university of technologies and engineering named after Sh. Yesenov, Kazakhstan
[3]Department of Information technologies security, National Aviation University, Ukraine
[4]Department of information security, Satbayev University, Kazakhstan
[5]National academy of Security service of Ukraine, Ukraine

E-mail: [1]lva964@gmail.com, [2]berik.akhmetov@yu.edu.kz, [3]agkorchenko@gmail.com, [4]zhuldyz_al@mail.ru, [5]okzi@e-u.in.ua

ABSTRACT

The work is devoted to the development of the mathematical support of decision support systems (DSS) for information and cybersecurity of information and communication transport systems (ICTS). There was improved the algorithm on the basis of the Delphi method for carrying out a survey to assess the ICTS security using the DSS. The algorithm is adapted for on-line mode for solving the problems of situations development forecasting related to information security and to prevention of the destructive influence of cyber attacks on ICTS. There was proposed a model for structuring of heterogeneous information obtained by interviewing the experts and for forming a knowledge base of DSS.
One of the motivating reason for this research was the need to develop a fairly simple for algorithmic implementation, but effective tool for the experts work online, assessing the information security of a particular information object.
On the basis of the proposed model, there were developed and tested automated tools for depth ICTS security analysis in the on-line mode using the generation of questionnaires for the research conducting by Delphi method. There were presented the results of approbation of the developed tools for the practical tasks of ICTS cyber security ensuring. It is shown that the proposed solutions allow to reduce financial and time costs in the process of on-line expert evaluation organizing and contribute to its quality and effectiveness.

Keywords: *Information Security, Cybersecurity, Expert Evaluation, Decision Support System, Delphi Method.*

1. INTRODUCTION

Analysis of complex control objects on transport, in particular, integrated information security systems (IISS), as well as cybersecurity subsystems (CSS), has shown the need to create means for depth analysis of the subject area related to the security of information and communication transport systems (ICTS).

According to the experience of IISS use in ICST, it is possible to provide information and cybersecurity (IS and CS) with the help of their actively interaction with experts, for example, within the framework of specialized situational centers (SC), but without computer technology this work is very laborious. In order to confront to the complex targeted cyberattacks you can, in particular, use decision support systems (DSS) in ICTS security operational control (OC) tasks. For this purpose during the process of implementation of the procedure of the alternative scenarios formation for the solution of the OC IS ICTS tasks, it is necessary to apply expert evaluation, in particular, the Delphi method (DM) used in many DSS of IS and CS.

Therefore, the subject of the research devoted to the development of models and software on the basis of DM for DSS tasks of OC IS ICTS seems to be relevant.

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

2. ANALYSIS OF LITERARY DATA AND PROBLEM STATEMENT

In connection with the increasing number of complex targeted cyberattacks on critically important computer systems (CICS) in recent years, there is appeared a separate direction of the researches devoted to the development of DSS [1], [2] and expert systems (ES) [3], [4] in the field of IS and CS.

According to the authors' opinion [5], [6], without the interaction of experts and analysts of the IS and relevant DSS and ES it is problematic to describe not always formalized relations between threats and vulnerabilities in the conceptual and functional aspects of cybersecurity of CICS.

It is difficult to analyze and to support the decision-making related to IS of CICS weakly amenable for formalization and structuring the task of CS with the appearance of new classes of attacks [7].

In works [8], [9] it was shown that the disadvantages of many DSS and ES in the field of IS and CS are: the need for highly skilled experts at the formation of a structured knowledge base (KB); difficulties at mathematical ensuring adapting for solving the prediction problems [8] using the expert evaluation procedure (for example, on the basis of DM and of acceptable interval estimates and metrics); availability of reliable statistics on incidents of IS and CS. However, the authors confined themselves with a conceptual description of the model, without giving a detailed description of it.

In works [10], [11] it was shown that the main direction of DM application of the IISS formation tasks is the evaluation of medium-term and long-term problems associated with the violation of CS of CICS [11]. These works did not receive further development in the form of applied software products, and were limited only with theoretical calculations. In works [12], [13] it was noted that the main advantage of DM is the anonymity of the survey, as well as the possibility of feedback from experts. However, as it is shown in [14], [15], there are no means of automation at the stage of questionnaire generating. Despite the practical experience of DM usage [16], [17] in various subject areas, including the problems of information protection (IP) [18], [19], there is almost no mathematical formalization for existing DSS of IS and the system approach to the process of survey conducting in the on-line mode.

Taking into account the controversy in works [20], [21], it seems obvious that it is necessary to continue researches on practically implemented solutions for DSS, especially at the stage of confirmed estimates formation based on DM, as well as on fuzzy interval estimates and metrics in DSS of IS CICS. The performed analysis of the previous studies also revealed the need for formalization of the stage of confirmed reasoning formation of the analysts on CS and for creation of software tools in DSS of IS for information support of the expert evaluation process (in particular, in on-line mode), which determined the relevance of the work.

3. PURPOSE AND OBJECTIVES OF THE RESEARCH

The purpose of the research is the development of models and software for the DSS operational control tasks of IS CICS, to which, in particular, ICTS also belong to.

In order to achieve this purpose it is necessary to solve the following tasks:

- to develop a formalization model of the confirmed estimates formation stage during the evaluating the IS and reaching a consensus of experts' opinions in the process of DM implementing based on fuzzy interval estimates and metrics in the DSS;
- to develop software for the generation of questionnaires used during the expert evaluation of IS based on DM, and to test the software in real-time tasks of OC IS ICTS.

4. MODEL OF THE CONFIRMED ESTIMATES FORMATION DURING THE EXPERT EVALUATION OF THE CYBERSECURITY OF THE PROTECTION OBJECT

The basis for the intellectual solution of the problems of IP and CS with the help of DSS and ES is the principle of reproducing the knowledge of experienced experts and analysts of IS. The use of heuristics allows to achieve a significant reduction of alternatives at searching for a rational solution for non-standard tasks related to the evaluation of the existing and new anomalies, attacks and threats in the CICS.

The process of confirmed expert estimates formation and achieving consensus using the Delphi method [13], [16], [17], [22], [23], taking into account the results of [24], [25], [26], is suggested to be supplemented with interval estimates and IS metrics [27], [28], characteristic for different classes of threats, anomalies and

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

cyberattacks. At the same time, there were taken into consideration the results obtained by the formation of the corresponding DB of IS CICS [24], [25], [29], [30].

The procedure for structuring the situation, related to the task of solution support for the ensuring of IS CICS, was considered in the functional and structural context of the concept - the knowledge field (KF) of cybersecurity [25].

In the developed DSS [24], [25], [26] there were used cognitive maps (COGM) that reflect the subjective interpretation of the regularities of the CICS element functioning. To describe the COGM there were also used the methods for identifying the preferences of the expert (or the decision-maker - DM), analyzing scenarios for situations transforming related to the problems of the CS

As a result, there are generated a variety of interval situation estimates:

$$\overline{AS}_{os} = \left\{ \overline{AS}_{ose} | e=\overline{1,E_{OS}} \right\} \;\&\; \overline{AS}_{ose} =$$

$$= \left\{ \left[\overline{AS}^{-}_{osew} ; \overline{AS}^{+}_{osew} \right] | w=\overline{1,W} \right\}, \qquad (1)$$

where AS_{ose} – expert evaluation for w level [8], [22], [23] the e expert, relatively to s indicator for o object.

Interval estimates of the situation are also correlated with the IS metrics [27], [28].

Let assume that for the obtained interval estimates there are given the IS metrics

$$m_{g_{ose_i w}, g_{ose_j w}} =$$

$$= (1/W) \cdot \sum_{w=1}^{W} m_{g_{ose_i} e_j w}, \qquad (2)$$

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

the works [23], [27], [28] show that at the calculation of IS metrics with different compositions of expert groups, the results can differ substantially. Therefore, the importance of the e expert opinion is estimated by the value:

$$op_{ose} = \left(1 - m\left(\overline{AS}_{ose}, \tilde{AS} \right) \right) \cdot C_{ose}, \qquad (3)$$

where C_{ose} – expert's competence regarding the analyzed IS metrics.

The average interval estimate was calculated by the formulas:

$$\overline{ES}^{-}_{osw} = \left(1/E \right) \cdot \sum_{e=1}^{E_{OS}} \overline{AS}^{-}_{osew} \;\&$$

$$\overline{ES}^{+}_{osw} = \left(1/E \right) \cdot \sum_{e=1}^{E_{OS}} \overline{AS}^{+}_{osew}; \qquad (4)$$

The Integral expert estimate was calculated by the formulas:

$$\overline{\overline{AS}}^{-}_{osw} = \arg\min_{\overline{AS}^{-}_{osew}} \left(\Psi 0 \right) \;\&\; \overline{\overline{AS}}^{+}_{osw} =$$

$$= \arg\min_{\overline{AS}^{+}_{osew}} \left(\Psi 1 \right), \qquad (5)$$

where

$$\Psi 0 = \left| \overline{AS}_{osew} - \overline{ES}^{-}_{osew} \right|, \quad \Psi 1 = \left| \overline{AS}_{osew} - \overline{ES}^{+}_{osew} \right|.$$

The confidence interval of the first round of the expert evaluation of the situation is determined by the following dependence:

$$\overline{AS}_{ose} \in T_{os}, then \; \overline{AS}_{ose} = \arg\min_{\overline{AS}_{ose}} \left(\tilde{m}_{ose} \right),$$

where T – time of situation transformation evaluating the object.

The generated confidence interval allows to determine the radius of the expert evaluation set by the following formula: $RA^{(T_{os})} = \max_{\overline{AS}_{ose}} (\tilde{m})$. The obtained value $RA^{(T_{os})}$ is fixed during the first round, and the confidence interval in the subsequent rounds is determined as follows: $\overline{AS}_{ose} \in T_{OS}$, $then \;\; \tilde{m} < RA^{(T_{Os})}$.

The degree of discrepancy between the KF elements– $dis_{ij}(t)$, taking into account the works [17], [21], [22], is determined by the following equation:

$$dis_{ij}(t) = \frac{\left| v^{+}_{ij}(t) - v^{-}_{ij}(t) \right|}{v^{+}_{ij}(t) + v^{-}_{ij}(t)}, \; 0 \le v_{ij}(t) \le 1, \qquad (6)$$

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

where $v_{ij}^{+}(t)$, $v_{ij}^{-}(t)$ – the addition of a positive and negative feature ("F") of situation change at t moments, respectively.

The parameter $dis_{ij}(t)$ characterizes the expert trust during the addition of $v_{ij}(t)$ for component situation $SI_i = \{si_{ij}\}, j = 1,..., m$. For $dis_{ij}(t) \approx 1$ (the case, when $v_{ij}^{+}(t) >> v_{ij}^{-}(t)$ or $v_{ij}^{-}(t) >> v_{ij}^{+}(t)$) the expert trust in feature value $v_{ij}(t) \rightarrow max$. For $dis_{ij}(t) \approx 0$ (the case, when $v_{ij}^{+}(t) \approx v_{ij}^{-}(t)$) the value $v_{ij}(t) \rightarrow min$.

The finally confirmed expert estimate is determined by the following formula:

$$\hat{AS}_{OS} = \left(ES^{+}_{osw}\left(\hat{AS}_{OS}\right) + ES^{-}_{osw}\left(\hat{AS}_{OS}\right) \right) / 2. \quad (7)$$

The proposed solution makes it possible to refill the KB and to correct it when new knowledge or contradictions are revealed. During the research, there was formalized the stage of the questionnaire creation and was proposed a module for automated synthesis of questionnaires. The last ones provide for generation of questions, in particular, with the division of the issue into text and the evaluation scale.

5. EXPERIMENT

In Fig. 1 schematically shows the structure of the Situation Center (SC) for analyzing cyber security tasks using on-line expert evaluation.

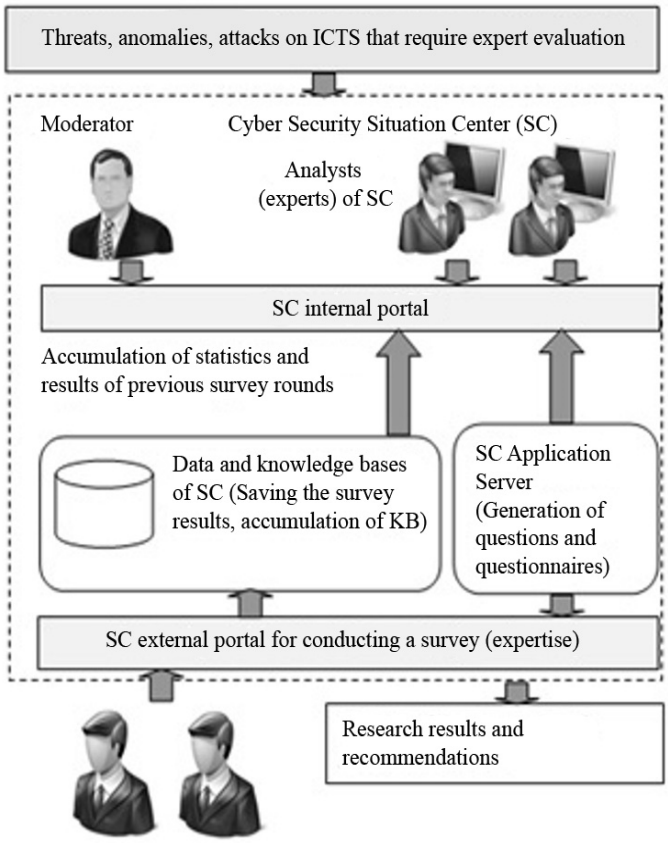


Figure 1: Structure Of The Transport Cyber Security Situation Center Using On-Line Expert Evaluation

The internal portal can be used to organize the work of small groups of experts directly in the SC,

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

in particular, at the stage of compiling of "corrected" questionnaires for all rounds of expert evaluation of the situation.

Table 1 shows an example of a fragment from a questionnaire for experts. The table shows the parameters for the evaluation, the interval rationing, the evaluation scale levels for typical threats IS and CS ICTS [4], [8], [19].

The proposed model is implemented for the SC applications server. The researches were carried out on the basis of several computer centers: 1) the State Enterprise "Design and Technological Bureau for Control Systems Automation of Railway Transport in Ukraine"; 2) the computer center of the State Enterprise "Pridneprovskaya Railway" (Information Security Department); 3) IT-technologies Department of "Kazakhstan Temir Zholy".

Table 1: Fragment Of The Questionnaire For Experts

Parameters	Normalization of the interval to [0,1]	Evaluation and threats scales level	
x_1 – the value of information resources for business processes on transport	$\bar{K}_{os} = 1 / W\left(\overline{\overline{AS}}_{OS}^{-}\right)$	0–0,2 Very low	The events connected with CS and IS, do not occur
x_2 – the amount of the documented changes of SW in ICTS			
x_3 – the level of copy protection			
x_4 – time between a vulnerability detection and its elimination in ICTS			
x_5 – the amount of subsystems with automatic antivirus updates			
x_6 – access control in segments of ICTS		0,2–0,4 Low	Occur rarely
x_7 – system SW update			
x_8 – the presence of cryptographic protection for ICTS	$\bar{K}_{os}^{+} = 1 / W\left(\overline{\overline{AS}}_{OS}^{+}\right)$		
x_9 – average time for elimination of the consequences of the attack			
x_{10} – the number of employees who passed trainings on cyber security		0,4–0,6 Average	Pos-sible
x_{11} – the possibility of external interference in the work of ICTS software and hardware			
x_{12} – the presence of means of critically important information reservation			
x_{13} – cases of information loss (documented /undocumented)			
x_{14} – the presence of attack detecting system			
x_{15} – the amount of applications/Percent of critical applications		0,6–0,8 High	Are fixed
x_{16} – the existence of the procedure of independent audit of IS ICTS			
x_{17} – the existence of means of identification and authentication of users		0,8–1 Very high	Occur cons-tantly
x_{18} – the presence of an active technical means of information protection (TMIP)			
x_{19} – the presence of passive TMIP			

The construction of a structured KB and the application of the proposed model during the implementing the initial information formalization procedures allows to generate a file with the resulting data for the KB. Generation of corrected questionnaires using the frames [25] of structured KB was tested in a new round of expert evaluation based on DM.

After the launch of the DM tour in on-line mode a table with fixed answers of experts is dynamically formed for each question of the questionnaire. The results of the calculation using the mathematical DM apparatus are also dynamically formed after filling the tables for each question.

Fig. 2 shows the results of a preliminary expert evaluation of the security of the analyzed ICTS (with deviations). The security parameter is adopted in the range [0-1] to [24].

Analyzing the evaluation consistency and at the formation of the final result of the expertise, for each of the factors under consideration, at the initial stage there was used the indicator - the expert's confidence at the parameter evaluation [13], [17], [22], [23].

Journal of Theoretical and Applied Information Technology
31st July 2018. Vol.96. No 14

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

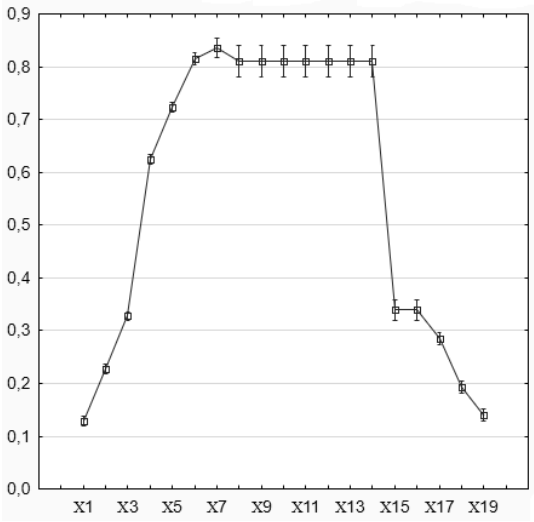
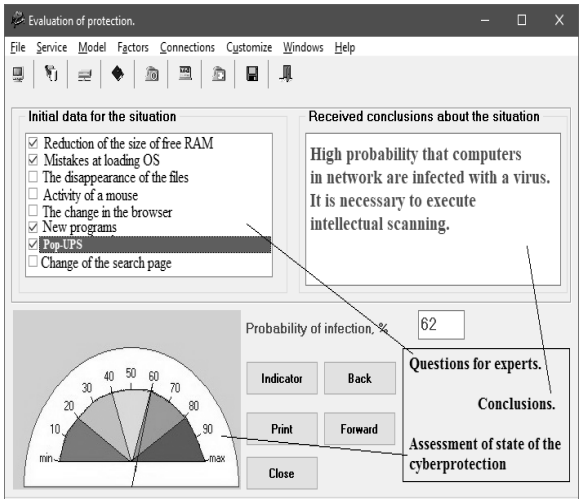
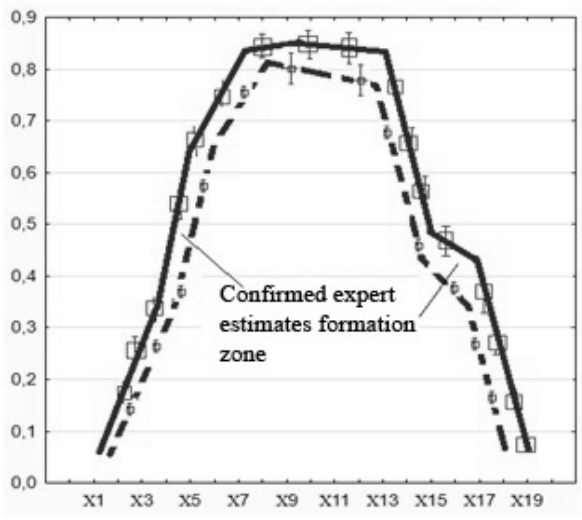


Figure 2: Point Expert Evaluation Of The Security Of The Analyzed ICTS (With Deviations)

Fig. 3. shows the results of the confirmed expert estimates formation and the achievement of consensus using the Delphi method, interval estimates and metrics (parameters, see Table 1), characteristic for various classes of threats, anomalies and cyberattacks. Researches were carried out on the DSS platform "Decision Support System of Management Protection of Information - DMSSCIS", previously described in [25].



A) DSS Interface;



b)

Б) Confirmed Expert Estimates Formation Results

Figure 3: The Formation Results With The Help Of DSS Confirmed Expert Estimates And Achieving Consensus Using The Delphi Method, Interval Estimates And Metrics

As a result of the confirmed expert estimates formation, in particular, after analyzing the consequences of cyber attacks related to WannaCry, Petya viruses, and measures to prevent them in the future, most experts agreed that under certain situation context the "Security level" indicator [24] would increase by 25-27%. There were tested automated tool and software for generation of questionnaires and confirmed expert estimates formation during the research of CICS for several enterprises. The proposed solutions made it possible to reduce financial and time costs for expert evaluation by about 17-20%.

Figures 4 and 5 presents the results of evaluating various parameters of information security and cybersecurity of the computing centers of transport enterprises. Red color shows the results obtained during the survey of experts independently. Blue color - using the software product "DMSSCIS". In the testing of "DMSSCIS" there were involved 11 experts. There have been involved cyber security analysts with work experience in the field of information protection for at least 5 years. Without the "DMSSCIS" system the experts filled out questionnaires in writing. The questionnaires contained questions with the evaluating the protection parameters of information and communication systems (ICS) of the analysed transport enterprises. In the control tests, the

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

experts performed an evaluation of the ICS security using DMSSCIS.

The standard values of the evaluated parameters (p) are assumed to be equal to 1 [8, 25, 26, 31, 32]. If the evaluation of the parameter is 0 – there is no protection.

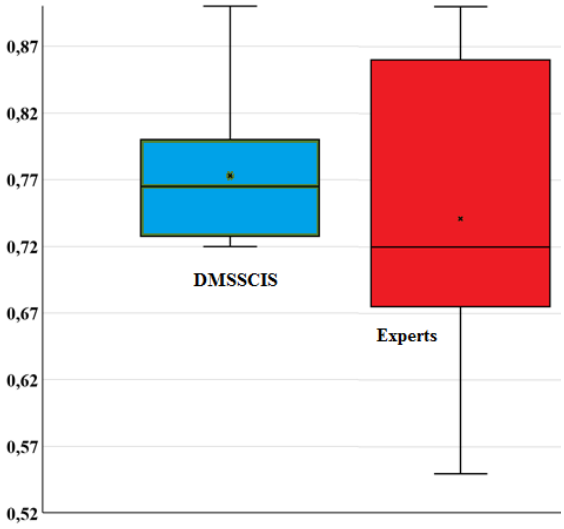


Figure 4: Evaluation Results By Experts Independently And With The Help Of The "DMSSCIS" Interface, The Degree Of ICS Protection Of Transport Enterprises In Ukraine And Kazakhstan

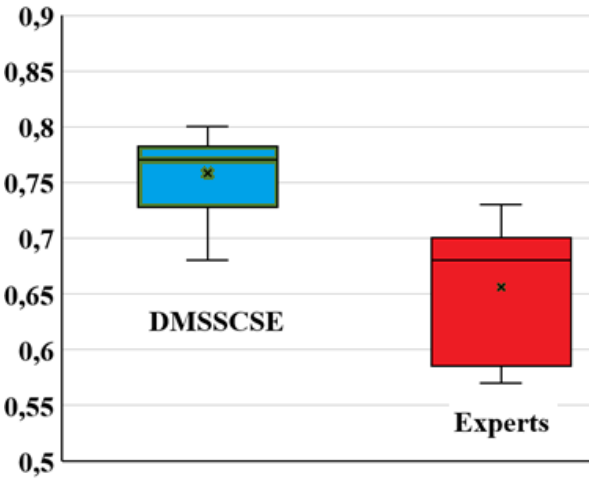


Figure 5: Results Of Evaluation The Transport Enterprises Sites Security In Ukraine And Kazakhstan

Analysis of the data shown on Figures 4 and 5 made it possible to establish that the discrepancy between the experts opinions, who used the DMSSCIS system, was 14-19% less than for the standard paper questionnaires of the ICS safety metrics.

There was also performed the evaluation of the degree of security [8, 25, 26] of the computation centers of transport enterprises in Ukraine and Kazakhstan, figure 6.

Without the use of the "DMSSCIS" system experts were more optimistic about the degree of ICS protection. Note that the further audit of information security (IS) of ICS did not always coincide with the expert evaluation. The evaluation was more consistent with the variant using the "DMSSCIS". The IS audit was carried out by analysts with at least 10 years of work experience in cybersecurity.

Figure 7 shows the histogram of time comparison (in minutes) for self-assessment and with the help of "DMSSCIS" evaluation of the signs of unauthorized access to the information system of the computer center of a transport enterprise in Kiev (Ukraine).

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

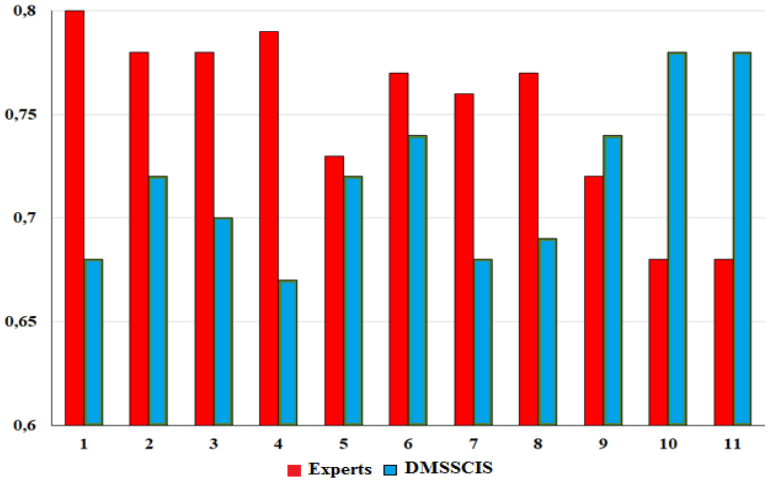


Figure 6: Evaluation By Experts Independently And With The Help Of "DMSSCIS" Of The Degree Of Security Of Computing Centers Of Transport Enterprises In Ukraine And Kazakhstan

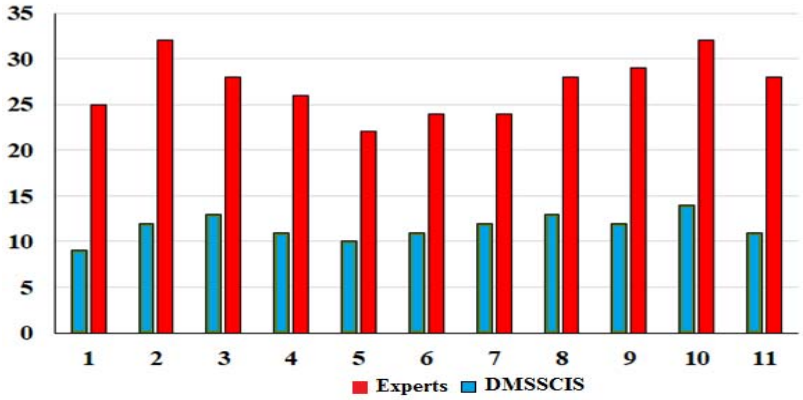


Figure 7: Time Spent By Experts Independently And With The Help Of "DMSSCIS" For The Evaluation Of The Signs Of Unauthorized Access To The Transport Company Information System

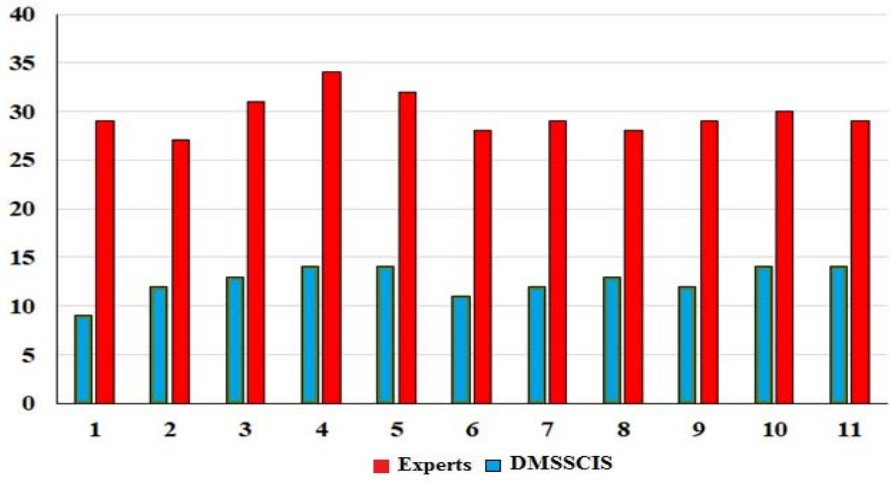


Figure 8: Time For The Site Security Evaluation Of Transport Enterprises In Ukraine And Kazakhstan

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

Figure 8 shows the experimental data on the time spent by experts independently and with the help of "DMSSCIS" for the evaluation the enterprise sites security.

Therefore, it is established that the time spent by experts on data processing using the "DMSSCIS" system is 45-50% less than the variant with paper experts' questionnaires.

A comparative analysis of similar solutions [2, 4, 6, 8, 25, 26] has shown that the "DMSSCIS" system has the following advantages:

- it is possible to integrate the developed software product with the existing information security complexes;
- the efficiency of decision-making in the evaluation tasks of the security degree and ICS information security of transport enterprises has been increased;
- flexible configuration of "DMSSCIS" is possible taking into account the specificity of protection of a particular enterprise ICS.

6. DISCUSSION

Researches confirmed the possibility of integrating in CICS for ICTS the software DSS for SC CS of transport. Test researches were conducted for the tasks of OC IS at the stage of conducting a survey of experts and analysts of IS in on-line mode.

As a part of the practical implementation, the next stage in the development of the proposed models and software for DSS of IS ICTS is the development of a mechanism for the construction and implementation of IS control systems for large ICTS. This, in particular, concerns the projected in the Republic of Kazakhstan Unified State Information Transport System (USITS) and the corresponding SC for CS.

The described solutions complement existing studies [24–26, 33–35], in the context of solving tasks on managing protection of ICTS based on the implementation into comprehensive IPS of DSS on cybersecurity.

Taking into account the results of the conducted researches, it can be noted that the complexity of implementation include:

- the need for technical and economic expertise of DSS of IS ICTS;
- insufficient amount of specialists needed to implement this approach in the USITS framework.

The above reasons at the first stage of implementation made it more difficult for experts to obtain adequate assessments of the security of the information objects selected for the assessment.

However, the proposed model, in our opinion, is more effective than similar models described in works [2, 6, 7].

Limitations of this work. The results presented here are not intended to cover all of the issues related to this topic. They simply reflect a set of shared conclusions that our group agreed, during an intense period of common research (March 2015 – April 2018).

7. CONCLUSIONS

Based on the analysis of the practical tasks of cybersecurity ensuring of information and communication transport systems (ICST) there is proposed a model for formalizing the stage of the confirmed expert estimates formation. The model is based on the Delphi method and is supplemented by fuzzy interval estimates and information security (IS) metrics in the developed decision support system (DSS). The software-implemented DSS contains a knowledge base (KB), as well as an automated tool for generating questionnaires for experts and analysts of IS. The obtained results allowed performing the tests in the on-line platform mode for the cybersecurity situational center on transport in the Republic of Kazakhstan.

The developed software for DSS of IS ICTS allows to fill and formalize the KB taking into account the description of the situation context arising during the implementation of various classes of cyberattacks on CICS transport. The proposed software made it possible to reduce the financial and time costs of the expertise during the process of IISS constructing and IS analyzing of the operating ICTS.

8. ACKNOWLEDGEMENT

The authors acknowledge the financial supported by the Fundamental Research Grant under grant number 0114U005430 (also № 0104U005401, № 0107U006840) received from the Ministry of Education and Science of Ukraine.

REFERENCES:

[1] T. Sawik. “Selection of optimal countermeasure portfo lio in it security planning”, *Decision Support Systems,* Vol. 55, Iss. 1, 2013, pp. 156–164.

[2] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, F. Smeraldi. “Decision support approaches for cyber security investment”,

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

Decision Support Systems, Vol. 86, 2016, pp. 13–23.

[3] 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.

[4] 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) 2011,* vol. 4, no. 6, pp. 505–527.

[5] Chang Li-Yun, Lee Zne-Jung. "Applying fuzzy expert system to information security risk Assessment – A case study on an attendance system", *International Conference on Fuzzy Theory and Its Applications (iFUZZY) 2013*, pp. 346 – 351.

[6] 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) 2014*, pp. 896 – 900.

[7] 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.

[8] Lakhno, V., Petrov, A., & Petrov, A. "Development of a Support System for Managing the Cyber Security of Information and Communication Environment of Transport", *In International Conference on Information Systems Architecture and Technology*, 2017, pp. 113-127. Springer, Cham.

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

[10] M. Carlton & Y. Levy. "Expert assessment of the top platform independent cybersecurity skills for non-IT professionals", *In SoutheastCon 2015,* pp. 1–6. IEEE.

[11] R. K. Abercrombie, F.T. Sheldon, A. Mili. Managing complex IT security processes with value based measures, *Computational Intelligence in Cyber Security 2009.*

[12] A.T. Sherman, L. Oliva, D. DeLatte, E. Golaszewski, M. Neary, K. Patsourakos, D. Phatak, T. Scheponik, G. L. Herman, J. Thompson. Creating a Cybersecurity Concept Inventory: A Status Report on the CATS Project, Appears in the proceedings of the 2017 National Cyber Summit, Huntsville, AL.

[13] Y. Nugraha, I. Brown, A. S. Sastrosubroto. "An Adaptive Wi deband Delphi Method to Study State CyberDefence Requirements", *IEEE Transactions on Emerging Topics in Computing 2016*, Vol. 4, Iss. 1, pp. 47 – 59.

[14] J Bedford, L. Van Der Laan. "Organizational Vulnera bility to Insider Threat", *In: C. Stephanidis. (eds) HCI International 2016 – Posters' Extended Abstracts. HCI 2016. Communications in Computer and Information Science 2016*, vol. 617. Springer, pp. 465–470.

[16] A.M. Johnson. "Business and security executives views of information security investment drivers: Results from a delphi study", *Journal of Information Privacy and Security 2009*, 5(1), pp. 3–27.

[17] D. Pruitt-Mentle. "A Delphi Study of Research Priorties in Cyberawareness", *Educational Technology Policy, Research and Outreach–CyberWatch, 2011*.

[18] M. Chaturvedi, A. N. Singh, M. P. Gupta, J. Bhattacharya. "Analyses of issues of information security in Indian context", *Transforming Government: People, Process and Policy 2014*, Vol. 8 Iss. 3, pp.374–397.

[19] B. Karabacak, S. O. Yildirim, N. Baykal. "A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness", *International Journal of Critical Infrastructure Protection 2016,* Vol. 15, pp. 47–59.

[20] J. Esteves, E. Ramalho, & G. De Haro. "To Improve Cybersecurity, Think Like a Hacker", *MIT Sloan Management Review 2017*, 58(3), 71.

[21] G. Dhillon, R. Syed, & F. de Sá-Soares. "Information security concerns in IT outsourcing: Identifying (in) congruence between clients and vendors", *Information & Management 2017*, 54(4), 452–464.

[22] Pankratova N.D. et al. Foresight and Forecast for Prevention, Mitigation and Recovering after Social, Technical and Environmental Disasters. In: HN. Teodorescu, A. Kirschenbaum, S. Cojocaru, C. Bruderlein. (eds). Improving Disaster Resilience and Mitigation - IT Means and Tools. NATO Science for Peace and Security Series C: *Environmental Security 2014. Springer.*

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

[23] M. Z. Zgurovsky & N. D Pankratova. "System analysis: Theory and applications". *Springer Science &Business Media 2007*.

[24] V. Lakhno, Y. Boiko, A. Mishchenko, V. Kozlovskii & O Pupchenko. "Development of the intelligent decision-making support system to manage cyber protection at the object of informatization", *Eastern-European Journal of Enterprise Technologies 2017*, 2 (9(86)), pp. 53–61.

[25] B. Akhmetov, V. Lakhno, Y. Boiko & A. Mishchenko. "Designing a decision support system for the weakly formalized problems in the provision of cybersecurity", *Eastern-European Journal of Enterprise Technologies 2017*, 1 (2 (85)), pp. 4–15.

[26] V. Lakhno, V. Malyukov, V. Domrachev, O. Stepanenko & O. Kramarov. "Development of a system for the detection of cyber attacks based on the clustering and formation of reference deviations of attributes", *Eastern-European Journal of Enterprise Technologies 2017*, 3 (9(87)), pp. 43–52.

[27] R. M. Savola. "Towards a taxonomy for information security metrics", *In Proceedings of the 2007 ACM workshop on Quality of protection*, pp. 28–30. ACM.

[28] M. Rostami, F. Koushanfar, & R. Karri. "A primer on hardware security: Models, methods, and metrics", *Proceedings of the IEEE 2014,* 102(8), pp.1283–1295.

[29] T. Takahashi, Y. Kadobayashi, & H. Fujiwara. "Ontological approach toward cybersecurity in cloud Computing", *In Proceedings of the 3rd international conference on Security of information and networks 2010*, pp. 100–109, ACM.

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

[31] S. Jajodia, N. Park, F. Pierazzi, A. Pugliese, E. Serra, G. I. Simari, & V. S. Subrahmanian. "A Probabilistic Logic of Cyber Deception", *IEEE Transactions on Information Forensics and Security 2017*, 12(11), pp.2532–2544.

[32] A. Vijayakumar, V. C. Patil, D. E. Holcomb, C. Paar, & S. Kudu. "Physical design obfuscation of hardware: A comprehensive investigation of device and logic-level techniques", *IEEE Transactions on Information Forensics and Security 2017*, 12(1), pp. 64–77.

[33] Al Hadidi, M. M., Ibrahim, Y. K., Lakhno, V., Korchenko, A., Tereshchuk, A. & Pereverzev, A. "Intelligent Systems for Monitoring and Recognition of Cyber Attacks on Information and Communication Systems of Transport", *International Review on Computers and Software (IRECOS)*, 2016, 11(12), pp. 1167–1177.

[34] Lakhno, V. A., Petrov, O. S., Hrabariev, A. V., Ivanchenko, Y. V., & Beketova, G. S. "Improving of information transport security under the conditions of destructive influence on the information-communication system", *Journal of theoretical and applied information technology*, 89(2), 2016, pp. 352–362.

[35] Lakhno, V. A., Kravchuk, P. U., Pleskach, V. L., Stepanenko, O. P., Tishchenko, R. V., & Chernyshov, V. A. "Applying the functional effectiveness information index in cybersecurity adaptive expert system of information and communication transport systems", *Journal of Theoretical and Applied Information Technology*, 95(8), 2017, pp. 1705–1714.