Development of Sectoral Intellectualized Expert Systems and Decision Making Support Systems in Cybersecurity

Bakhytzhan Akhmetov[1], Valeriy Lakhno[2], Berik Akhmetov[3], and Zhuldyz Alimseitova[4(✉)]

[1] Kazakh National Pedagogical University named after Abay, Almaty, Kazakhstan
[2] European University, Kyiv, Ukraine
[3] Caspian State University of Technologies and Engineering named after Sh. Yesenov, Aktau, Kazakhstan
[4] Satbavev University, Almaty, Kazakhstan
zhuldyz_al@mail.ru

Abstract. The paper considers the prerequisites for the integration of various expert and decision support systems for information security and cybersecurity. Analyzed the possibility of sectoral pooling and sharing of knowledge bases of such intellectualized systems. The model of the knowledge management subsystem in sectoral expert and decision making support systems for information security and cybersecurity of critical computer systems is described. Also article presents the results of studies of the knowledge management system of existing local expert systems and decision making support systems for information protection. Algorithms for the distribution of requests between similar systems are specified.

Keywords: Cybersecurity · Decision making support systems
Expert systems · Clusters

1 Introduction

At the initial stage of implementation of decision making support systems (DMSS) [1, 2] and expert systems (ES) [3], in particular adaptive [4], in information protection (IP) and cybersecurity (CS) problems, their architecture matched to the classical version [5]. However, as the tasks related to the provision of CS have become more complicated, problems have arisen that can no longer be solved within the framework of classical architectures of the DMMS and ES for IP. For example, when in the process of logical inference it becomes necessary to use the conclusions of several independently functioning DMSS or ES. If the DMSS or ES was initially developed only for the solution of narrow-profile tasks, such as supporting solutions for choosing hardware-compatible rational variants of complex information protection systems [3] or expert analysis of complex features detected during the targeted attack [4], in such case to extend the range of solutions for other than the initial options is not possible. The relevance of this study is determined, first of all, by the state of the problematic of

R. Silhavy et al. (Eds.): CoMeSySo 2018, AISC 860, pp. 162–171, 2019.
https://doi.org/10.1007/978-3-030-00184-1_15

the integrated implementation of the critical important computer systems (CICS) of DMSS and the ES, combined into sectors (clusters [6]) into the contours of IP and CS. This causes the further development of the methodological apparatus, and the principles for the creation of sectoral intellectualized DMSS and ES for IP and CS CICS tasks.

2 Analysis of the Literature Data and the Formulation of the Problem

The increasing complexity of cyberattacks, especially targeted ones on CICS, aroused interest in the development of intellectualized DMSSES in the field of CS [7, 8]. The need for prompt decision-making related to the provision of CS of CICS made promising studies on the development of sectoral DMSSES able to combine their knowledge in the framework of the solution of the tasks [7].

The studies [9, 10] analyze the experience of using ES and DMSS in the problems of risk assessment for CS CICS. The scope of knowledge base (KB) of these systems was limited only to risk assessment.

The studies [11, 12] describe the DMSS using for decision-making in insufficiently structured situations for estimating the CS CICS KVKS. However, the research [12] is not brought to hardware and software implementation yet. The experience of using intelligent DMSS and ES in the tasks of management of IP and CS at individual enterprises is presented in studies [13, 14]. The scope of these systems was limited only to the management of information security.

The studies [15, 16] analyze the experience of commercial DMSS and ES implementation on IP and CS. The authors note that commercial systems have a closed nature, and their acquisition by individual enterprises is associated with significant financial costs.

The study [17] has shown that the problems of introducing DMSS and ES in the context of their multitasking were not systematically considered.

The conclusions of studies [7, 8, 12, 15] allow us to speak about the problem of the systemic introduction of adaptive DMSS and ES into the contours of IP and CS CICS. At the same time, the problems of theoretical substantiation and development of the basic principles for the creation of sectoral intellectualized ES and DMSS in the tasks of CS CICS remain unresolved.

3 Purpose and Objectives of Research

The goal of the work is the development of the basic principles and methodology for the creation of sectoral intellectualized ES and DMSS for the tasks of IP and CS CICS.

In order to achieve the aims of the work there is a need to solve the following tasks:

- to develop a model for the functioning of the subsystem of coordination and control of the knowledge output in sectoral DSSES for IP tasks;
- to test the control system and integration of the DB of local DSS and ES by IP.

4 Models and Methods

In sectoral DSSES the sector (cluster) is considered as an information unit. The sector integrates the capabilities of several independent (i.e. local) ES or DSS, Fig. 1. We will assume that the sector nodes can exchange specific information related to different tasks of the IP and CS. But the end user, for example, the analyst of IS, the cluster is available as a single resource. Therefore, the task of the sectoral system is the distribution of user requests and their conversion for specific local DSS or ES on IP and CS.

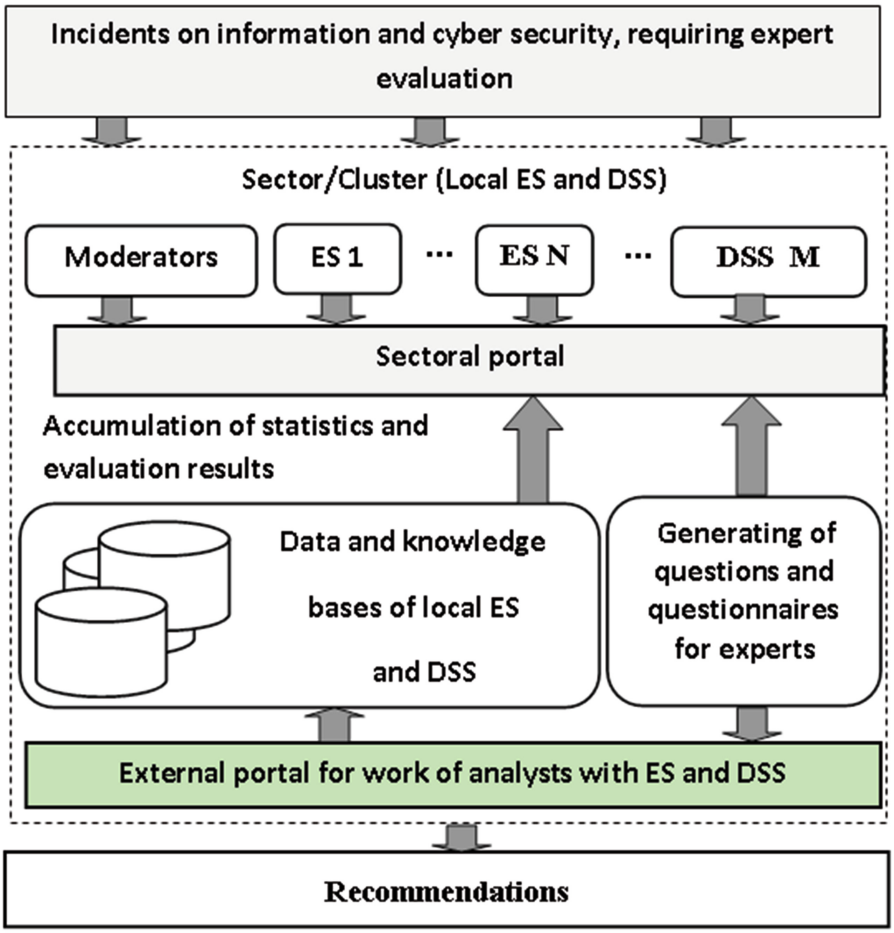

Fig. 1. Structural diagram of the sectoral (cluster) platform for combining local DSS and ES on cybersecurity

Let introduce the following notations: the initial (input) data – X; the resulting (output) data – Y; W – representation of the sets of input variables into the set of resulting data. Then $X = \langle x_1, \ldots, x_m \rangle$, $Y = \langle y_1, \ldots, y_n \rangle$, $W = \langle w_1, \ldots, w_n \rangle$. Where $X \cap Y = \varnothing$.

Sectoral DSSES will be considered as resulting if the following requirements are met:

1. $Y = w\langle X \rangle$.
2. $(\forall x_i \in X)(\exists q_1 \in x_1, \ldots, q_i \in x_i, q_i \in x_i, \ldots, q_m \in x_m)$
   $\times [w(q_1, \ldots, q_i, \ldots, q_m) \neq w(q_1, \ldots, q_i, \ldots, q_m)]$.

At the first stage of the request processing there is specified a set of variables to the sectoral DSSES – $x_i = f_i(x_1, \ldots, x_n)$. Values x_i should to be obtained during the implementation of $Y^r = \langle y_1^r, \ldots, y_n^r \rangle$.

Then, $y_i^r = z_i(x_{i1}, \ldots, x_{im})$.

The set of functions $Z^1 = \langle z_1, \ldots, z_m \rangle$ forms a list of $X^1 = \bigcup_{i=1}^{m} x_i$ in a resulting list $Y^r = Z^1(X^1)$, where X1 – list of variables of the final rank of the functional structural module of the sectoral DSSES. Then $u = (X, Y, W)$: $X^1 = X^{u1} \bigcup Y^1$, where $X^{u1} \bigcap Y^1 = \varnothing$.

Let consider that X^1 contains variables that are the initial data for the module U^1. In list Y^1 there are included the parameters which should be calculated during the operation of the module U^1.

The list Y^1 is presented through a new list. For example: $Y^1 = Z^2(X^2)$, where $X^2 = X^{u2} \bigcup Y^2$, $X^{u2} \bigcap Y^2 = \varnothing$.

Operations continue as long as the list of variables not belonging to X^1 for the rank k is not exhausted.

The described model can be represented in the form of a graph of variables $x_i = f_i(x_1, \ldots, x_n)$, Fig. 2. The nodes of the graph, denoted by red dots, correspond to the resulting variables.

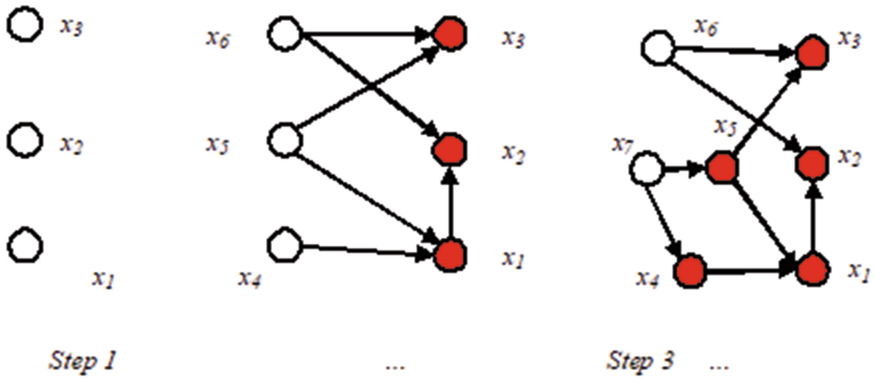

Fig. 2. Solution steps

At the decision stages, i.e. at each step of the graph construction, there are drawn arrows to non-initial nodes. We assume that the process is complete in the case when all non- initial nodes are connected by arrows. Correct is the result if there are no loops in the resulting graph. The proposed approach makes it possible to link knowledge from local DSS and ES for the related tasks and subject areas (for example, cybersecurity, the choice of technical means of protection, the cost of ISS, risk assessment for IS, etc.). In addition, it is possible to compile a tree of logical output for a sectoral DSS or ES on IP and CS of CICS.

5 Experiment

The proposed model, taking into account the results of the works [1, 4, 12], was implemented in the sectoral (cluster) system on cybersecurity – Cluster system of cybersecurity ("CLSC"). The knowledge base of "CLSC" integrated the DSS DB and ES of DMSSCIS and "DMSSCSE", respectively to the works [4, 18]. CLSC was tested in the computer centers of several companies [1, 4].

The effectiveness of the CLSC sectoral (cluster) platform, which integrated local DSS and ES on cybersecurity, was also tested during computational experiments (Figs. 2 and 3). As initial data there were taken the parameter values generated by the program according to the data from [1, 4, 12].

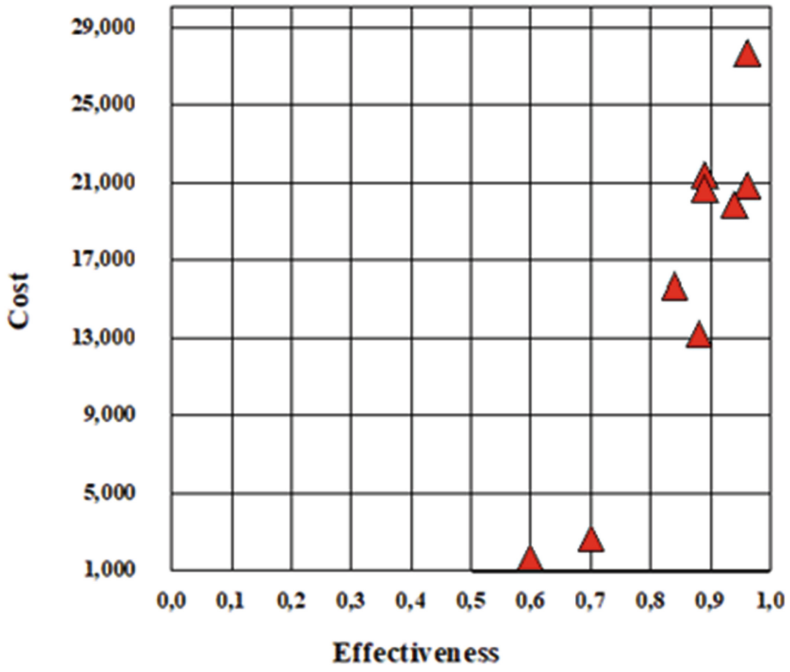

Fig. 3. Extended search area for the optimal samples of TMP for CICS

During the experiment there were compared the possibilities of sectoral DSS ("CLSC" and local DSS and ES (DMSSCIS and "DMSSCSE", [4, 18]) at evaluating the decisions regarding: the selection of compatible software and hardware protection tools, optimization of the cost of IISS for CICS, evaluation of risks for IS, evaluation and predicting the transformation of the situation for identified anomalies or threats in CICS, etc.

For example, during the computational experiments there was checked the correctness and adequacy of the algorithm (model) of the functioning of the subsystem for coordinating and control of knowledge output in the sectoral intellectualized DSS ("CLSC", for finding optimal solutions among the proposed variants of technical means of protection (TMP) of CICS, as well as of IISS for CICS.

During the computational experiment there were obtained two-dimensional arrays, which are presented in the form of a point diagram for the TMP, see Fig. 3, and for IISS for CICS, Fig. 4.

The triangles on Fig. 3 – coordinates of the effectiveness and cost values for the considered samples of TMP. Squares, Fig. 4 – coordinates of the effectiveness and cost values for the considered samples of complex means of information security and cybersecurity for CICS.

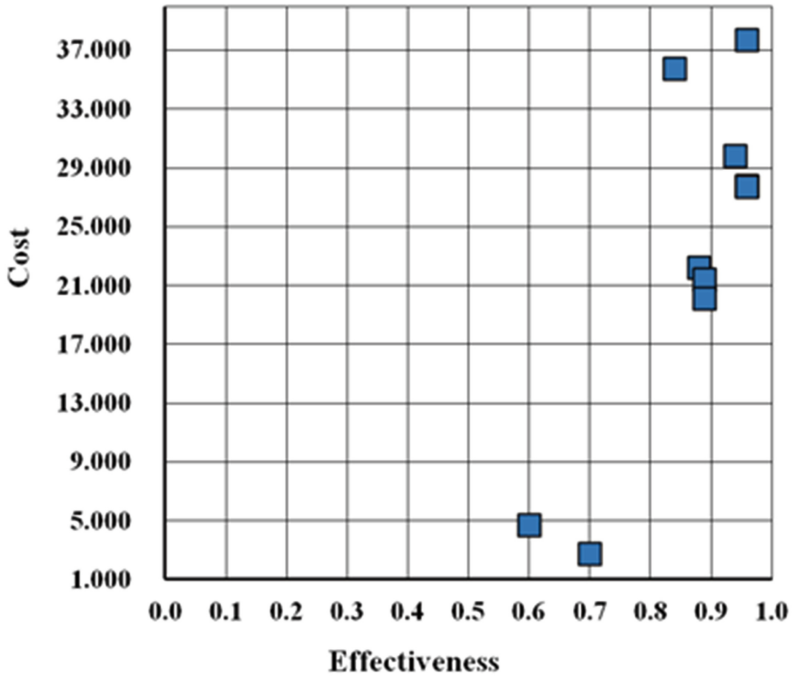

Fig. 4. Extended search area for the optimal samples of IISS for CICS computer network segment

For TMP and IISS as a protection object there was considered a segment of a computer network or a local CICS network [1–4]. The cost parameters were calculated in conventional monetary units.

The results obtained on the graph are an expanded search area for optimal solutions using the "effectiveness-cost" criterion [12].

The implementation of the research results on real CICS, Fig. 5, showed that the proposed solutions allow to increase the degree of protection of CICS, in particular due to the complex integration of local DSS and ES into cybersecurity tasks.

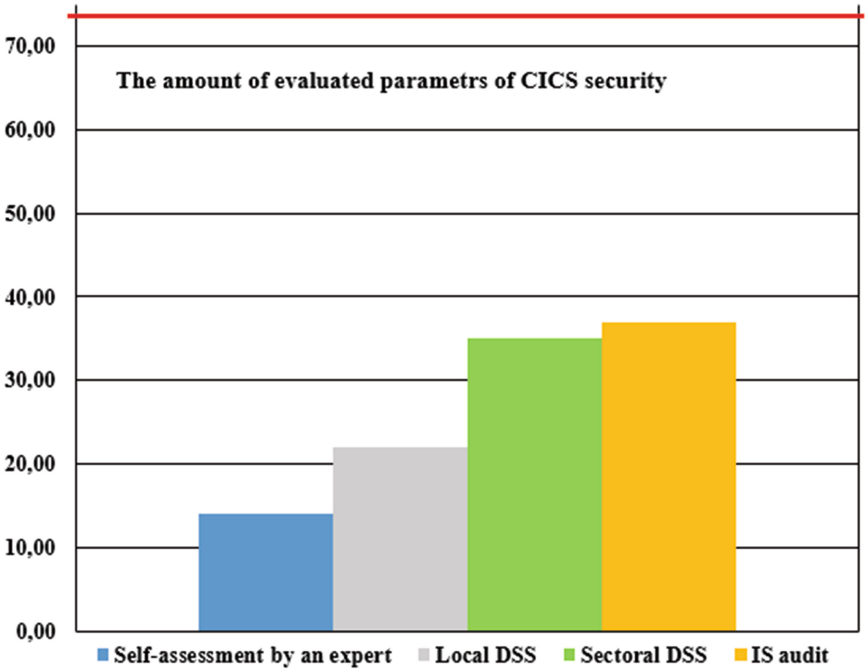

Fig. 5. Test results of the sectoral DSS "CLSC". Solution search completeness evaluation

Figure 5 shows the prototype testing results of the sectoral DSS "CLSC". The total number of evaluated parameters of CICS security in test researches is 75. The amount of detected parameters that differ from the norm, for a self-assessment by experts (with experience up to 5 years) is shown in blue, with the help of local DSS – gray, for the sectoral DSS "CLSC" – green. During the test 5 experts were involved. The control audit of the security parameters was carried out by 3 specialists on CS with at least 10 years of experience (yellow color).

Calculation of the amount of rules involved in the process of logical inference showed that in the sectoral DSS "CLSC" their amount is 5–7% less than in local DSS and ES [4, 18]. This is due to the fact that only the necessary rules for a specific task are sampled.

The sectoral DSS "CLSC" according to the main parameters (decision search time, prediction accuracy, search depth, etc.) exceeds solutions described in [4, 12, 18]. For example, the test showed that decisions support related to the choice of rational variants of TMP and ISS, the costs at the protection tools selection step are reduced by 16–19%.

6 Discussion of the Obtained Results and Prospects for Further Researches

The conducted researches are the development of work [19]. The proposed approach has advantages in comparison with traditional local DSS and ES in the tasks of IP and CS. Firstly, sectoral integration of systems makes it possible to combine the accumulated information of local DSS and ES in the DB. Secondly, sectoral (cluster) systems account better the specifics of the functioning of specific CICS, for example, in the tasks of selecting rational hardware compatible TMP or IISS [14] or at the decisions support on the operational control of cybersecurity, in conditions of uncertainty, inconsistency and incompleteness of knowledge about the state of the object [18, 19].

The potentially eliminated disadvantage of sectoral DSS or ES, and in particular CLSC, is the need to employ sufficiently qualified specialists, that is not always possible in real operating conditions. Also, to the disadvantages there can be attributed the additional financial costs for the development and implementation of coordination and control subsystems of the knowledge output.

The development of this research area can be the improvement of the interaction of the algorithm and program modules of the sectoral DSS "CLSC" with modules of the "DMSSCIS" system [17–19].

In general, on the basis of the conducted researches, it is possible to state the effectiveness of the proposed method and algorithms, as well as the software package for the sectoral DSS "CLSC".

7 Conclusions

1. There are considered prospects of integration of various expert and decision support systems for the tasks of information protection and cybersecurity ensuring on the basis of their sectoral aggregation and joint use of knowledge data bases. Proposed the model of the knowledge output control subsystem in sectoral ES and DSS for the IP and CS tasks of CICS.
2. Proposed a model and conducted computational research experiments of the knowledge control system of the existing local DSS and ES on IP, integrated into the cluster. Tested the prototype of the sectoral (cluster) decisions support system on CICS cybersecurity ensuring. Evaluated the effectiveness of the sectoral DSS "CLSC" use in comparison with local ES and DSS used in the tasks of decision-making support on IP and CS.

References

1. Akhmetov, B., Lakhno, V., Boiko, Y., Mishchenko, A.: Designing a decision support system for the weakly formalized problems in the provision of cybersecurity. Eastern-Eur. J. Enterp. Technol. **1**(2), 4–15 (2017). Article no. 85
2. Rees, L.P., Deane, J.K., Rakes, T.R., Baker, W.H.: Decision support for cybersecurity risk planning. Decis. Support Syst. **51**(3), 493–505 (2011)
3. Chang, L.Y., Lee, Z.J.: Applying fuzzy expert system to information security risk assessment-a case study on an attendance system. In: IEEE 2013 International Conference on Fuzzy Theory and Its Applications (iFUZZY), pp. 346–351 (2013)
4. Lakhno, V., Tkach, Y., Petrenko, T., Zaitsev, S., Bazylevych, V.: Development of adaptive expert system of information security using a procedure of clustering the attributes of anomalies and cyber attacks. Eastern-Eur. J. Enterp. Technol. **6**(9), 32–44 (2016)
5. Goztepe, K.: Designing fuzzy rule based expert system for cyber security. Int. J. Inf. Secur. Sci. **1**(1), 13–19 (2012)
6. Mahmood, T., Afzal, U.: Security analytics: big data analytics for cybersecurity: a review of trends, techniques and tools. In: 2013 2nd National Conference on Information Assurance (NCIA), pp. 129–134 (2013)
7. Kim, K., Kim, I., Lim, J.: National cyber security enhancement scheme for intelligent surveillance capacity with public IoT environment. J. Supercomput. **73**(3), 1140–1151 (2017)
8. Medhat, K., Ramadan, R.A., Talkhan, I.: Security in mission critical communication systems. In: Multimedia Services and Applications in Mission Critical Communication Systems, p. 270 (2017)
9. Radziwill, N., Benton, M.: Cybersecurity Cost of Quality: Managing the Costs of Cybersecurity Risk Management, [Electronic resource] (2017). https://arxiv.org/ftp/arxiv/papers/1707/1707.02653.pdf
10. Jalali, M., Siegel, M., Madnick, S.: Decision Making and Biases in Cybersecurity Capability Development: Evidence from a Simulation Game Experiment, [Electronic resource] (2017). https://arxiv.org/ftp/arxiv/papers/1707/1707.01031.pdf
11. Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., Smeraldi, F.: Decision support approaches for cyber security investment. Decis. Support Syst. **86**, 13–23 (2016)
12. 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, pp. 113–127 (2017)
13. Benaroch, M.: Real options models for proactive uncertainty-reducing mitigations and applications in cybersecurity investment decision-making, p. 39 (2017)
14. Wagner, N., Şahin, C.Ş., Winterrose, M., Riordan, J., Pena, J., Hanson, D., Streilein, W.W.: Towards automated cyber decision support: a case study on network segmentation for security. In: IEEE Symposium Series on Computational Intelligence (SSCI), pp. 1–10 (2016)
15. Atymtayeva, L., Kozhakhmet, K., Bortsova, G.: Building a knowledge base for expert system in information security. In: Soft Computing in Artificial Intelligence, pp. 57–76 (2014)
16. Silva, M.M., de Gusmão, A.P.H., Poleto, T., e Silva, L.C., Costa, A.P.: A multidimensional approach to information security risk management using FMEA and fuzzy theory. Int. J. Inf. Manag. **34**(6), 733–740 (2014)
17. Tamjidyamcholo, A., Baba, M.S.B., Shuib, N.L.M., Rohani, V.A.: Evaluation model for knowledge sharing in information security professional virtual community. Comput. Secur. **43**, 19–34 (2014)

18. Lakhno, V., Zaitsev, S., Tkach, Y., Petrenko, T.: Adaptive Expert systems development for cyber attacks recognition in information educational systems on the basis of signs' clustering. In: Advances in Computer Science for Engineering and Education. ICCSEEA 2018. Advances in Intelligent Systems and Computing, vol. 754, pp. 673–682 (2018)
19. Akhmetov, B., Lakhno, V.: System of decision support in weakly formalized problems of transport cybersecurity ensuring. J. Theor. Appl. Inf. Technol. **96**(8), 2184–2196 (2018)