

Ergonomic Support for Decision-Making Management of the Chief Information Security Officer

Sergiy Gnatyuk^{1,2} [0000-0003-4992-0564], Nataliia Barchenko³ [0000-0002-5439-8750],
Olena Azarenko¹ [0000-0003-2927-5545], Andrii Tolbatov⁴ [0000-0002-9785-9975],
Victor Obodiak³ [0000-0002-8539-1252] and Volodymyr Tolbatov³ [0000-0002-6564-9658]

¹ National Aviation University, Kyiv, Ukraine

² Yessenov University, Aktau, Kazakhstan

³ Sumy State University, Sumy, Ukraine

⁴ Sumy National Agrarian University, Sumy, Ukraine

sergio.gnatyuk@gmail.com

Abstract. The paper considers the actual task of making managerial decisions by the Chief Information Security Officer. The need for the optimal distribution of tasks between department officers is shown. This problem is considered as a linear programming problem. An ergonomic approach is proposed to obtain quantitative estimates of the algorithms of officers' activities. The use of the functional-structural theory of ergotechnical systems made it possible to formalize, describe and evaluate the activities of officers. The obtained probabilistic-temporal characteristics of various tasks were used as initial data for solving the optimization problem. To apply this approach in the activities of the leader, an information technology for supporting management decision-making has been developed and described. An example of implementation for two management decision-making strategies is shown in this paper.

Keywords: Information Security, Management Task, Information Technology, Decision-Making, Chief Information Security Officer, Ergonomic Approach.

1 Introduction

The duties of the Chief Information Security Officer (CISO) include not only informing management about the risks to the company's activities and direct participation in risk management, developing information security documents, studying the latest technologies and security trends, but also implementing other strategic work, such as responding to incidents and assigning tasks to their prevention, analysis, elimination of consequences, etc. Naturally, it is not the CISO himself who performs the specified routine work, but entrusts it to the employees of his service. The reliability of the company as a whole largely depends on the correct distribution of tasks between its subordinates. As a rule, CISO makes such decisions more or less intuitively, based on his knowledge of the health, productivity and reliability of the employees. But such decisions can lead to non-optimal results.

Copyright © 2020 for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0) CMiGIN-2019: International Workshop on Conflict Management in Global Information Networks.

2 Related works analysis and problem statement

The final areas of information security management in organizations of various kinds of activities [1] include:

1. Asset management of the organization [1-3, 18, 19].
2. Resource management of the information security system implemented in the organization [1, 2, 4].
3. Management of risks and threats to information security [2, 5, 6].
4. Management of documentation and information help system in the organization [1, 2, 7, 13].
5. Information security audit management [6, 8, 9].
6. Management of the analysis of the effectiveness of the information security system [1, 4, 10].
7. Management of tasks and activities of employees engaged in the processes of ensuring information security in the organization [11] etc.

As one can see, the task of managing the activities of employees involved in information security processes in the organization has not been completely solved. This task can be considered as one of the tasks of ergonomics - the distribution of functions between operators-executors. The use of the ergonomic approach allows the manager to use scientific and practical developments in this subject area. From the point of view of the ergonomic approach, the operator-manager has the following tasks:

- organization of activities of executing operators [12];
- creation of optimal psychological working conditions [13];
- ensure reliability [14].

In paper [15], the basic principles of the functional-structural theory of ergotechnical systems (ETS) and its application for various tasks of constructing problems of ergonomic quality and such systems with a constant functional structure as the workshop control system are described.

In paper [16], the problem of the distribution of functions for flexible systems with a variable functional structure was solved. One can see that the problem of the distribution of functions can be effectively solved only on the basis of estimates of the accuracy and timeliness of the functioning algorithms, i.e. human-machine interaction processes. This approach can be implemented on the basis of the functional-structural theory of ergotechnical systems [17], which provides tools for modeling human-machine interaction:

- formalized description of functioning algorithms,
- determination of probability-time indicators of the quality of functioning algorithms, and
- optimization.

This approach can be extended to ensure the reliability of information security management activities. Untimely and erroneous implementation of information security management actions can lead to a violation of the integrity, accessibility and confidentiality of information, which entails material damage.

Information security officers have different qualifications and work experience, which leads to different values of faultlessness and execution time of both individual works and the entire functioning algorithm.

The unsolved problem is the formation of initial data for evaluating the functioning algorithms. It is proposed to take data from special directories that are focused on the average operator. However, there are no such directories for information security management activities.

The purpose of the study is to develop information technology to support the decision-making of the CISO, which ensures the optimal appointment of the security officers to perform information security management tasks.

In this case, it is necessary to take into account various strategies:

- 1) All employees should be allocated to tasks (one employee - one task)
- 2) Maximum reliability must be ensured (one employee can perform several tasks; the tasks are not assigned to some employees).

To achieve this goal, it is necessary to solve the following tasks:

- developing a mathematical model for solving the problem
- developing an approach to ensure the evaluation of functioning algorithms with source data
- checking the possibility of using the developed models and approaches to build information technology for decision support of the CISO.

3 The optimal appointment of CISO to perform tasks

There are n officers and m actual tasks. Any officer can be appointed to accomplish any task, but with different assumed accuracy of the execution. It is necessary to allocate officers to carry out tasks in such a way that they complete tasks with maximum error-freeness within the available time reserve.

The task can be represented as a following linear programming problem.

$$B(X) = \sum_{i=1}^n \sum_{j=1}^n b_{ij} x_{ij} \rightarrow \max ,$$

$$\sum_{j=1}^n x_{ij} = 1, (j = \overline{1, n}), \sum_{i=1}^n M_{ij} x_{ij} \leq T_i, x_{ij} \in \{1; 0\}.$$

The variable x_{ij} represents the appointment of officer j for task i and takes the value 1 if the officer is assigned to complete the task, and 0, otherwise b_{ij} is the probability of an error-free operation. T_i is allowable execution time of i task, M_{ij} is the mathematical expectation of the time to complete the operation.

The second strategy assumes that one officer may be assigned to complete only one mission. At the same time, we need the tasks have been completed with maximum error-freeness within the existing time reserve. The restriction determines the assignment of one task to one officer:

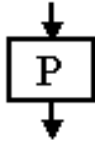
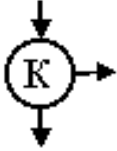
$$B(X) = \sum_{i=1}^n \sum_{j=1}^n b_{ij} x_{ij} \rightarrow \max ,$$

$$\sum_{i=1}^n x_{ij} = 1, (i = \overline{1, n}), \sum_{j=1}^n x_{ij} = 1, (j = \overline{1, n}), \sum_{i=1}^n M_{ij} x_{ij} \leq T_i, x_{ij} \in \{1; 0\}.$$

4 Application of the ETS theory for quantitative assessment of the quality of task performance

The generalized structural method that underlies the ETS uses a functional network as a description of functioning algorithms (FA). To describe the FA used typical functional unit (TFU) (table 1).

Table 1. TFU parameters

TFU	Conventional symbol	Indicator	
		Symbol	Description
Work operation		B ¹ (B ⁰)	The probability of an error-free operation;
		M(T)	The mathematical expectation of the time to complete the operation
Monitoring the functioning		K ¹¹ (K ¹⁰)	The conditional likelihood that the operation being verified, when actually performed correctly, will be recognized as correct (incorrect) (K ¹¹ +K ¹⁰ =1);
		K ⁰⁰ (K ⁰¹)	The conditional likelihood that the operation being verified, when actually performed incorrectly, will be recognized as incorrect (correct) (K ⁰⁰ +K ⁰¹ =1); The mathematical expectation of the time to complete the operation

To conduct a quantitative assessment of the quality and reliability of operation in the FS apparatus, a set of TFS was obtained.

To build an AF model, it is necessary to prepare a list of work to be performed. Each work put in line with the TFU. For each TFU, determine the probability-time characteristics. Using Table 2 to obtain quantitative indicators of the quality of performance AF [17-19].

Table 2. The typical functional structure (TFS) parameters

TFS	TFS diagram	Formula
1. Sequential execution of work operations		$B = \prod_{i=1}^n B_i$
		$M(X) = \sum_{i=1}^n M(X_i)$
2. Cycle functional diagram “Operation with monitoring the functioning without limitation on the number of cycles”		$B = B^1 K^{11} \frac{1}{1 - (B^1 K^{10} + B^0 K^{00})}$
		$M(X) = (M(X_p) + M(X_k))M(L)$ $M(L) = \frac{1}{1 - (B^1 K^{10} + B^0 K^{00})}$

The formation of the source data for the task of evaluating the functioning algorithm

Providing the task of evaluating the functioning algorithm (FA) with source data is one of the main problems of ergonomic modeling. We cannot accept the assumption of an “average operator” in this study. The proposed approach implements the technology of intelligent analysis [18, 19] of data accumulated in the database of the results of activities of the office employees.

We solve the approximation problem using neuro-fuzzy inference technology [20]. In this technology, a logical conclusion bases on fuzzy logic, and membership functions are adjusted using neural networks. The parameters of the officer, hardware and software, time constraints are fed to the input, and at the output, we obtain probability-time indicators of the quality of the operation.

Information technology for ergonomic support for management decision-making of the CISO

Fig. 1 demonstrates the functional structure of the developed system.

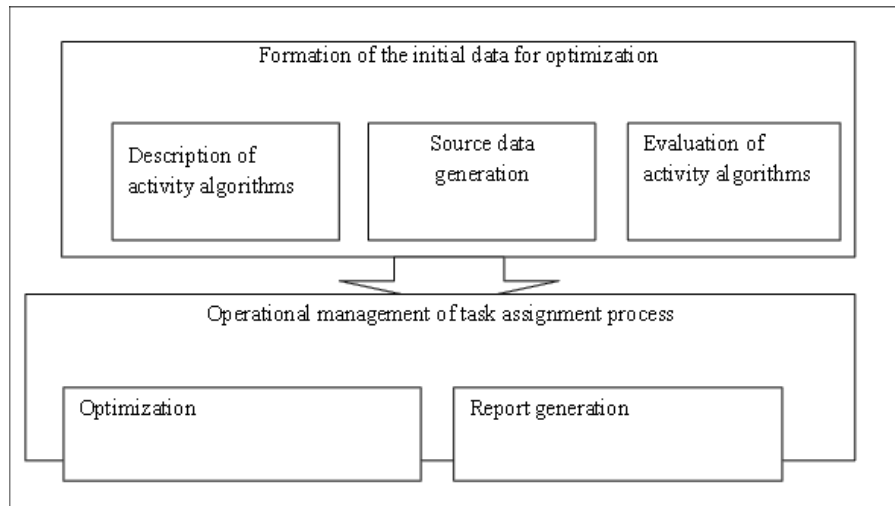


Fig.1. The functional structure of the developed system

Model implementation example

Let the CISO have the task to formulate a security office work plan. Every information security officer should be given a mission. Currently relevant tasks:

- Task1 - website check
- Task2 - audit of wireless networks
- Task3 - prevention of physical intrusion.

The lead time for the first task is no more than 620; the lead time for the second task is no more than 500; the lead time for the third task is no more than 160. Tasks can be assigned to three officers.

It is necessary to distribute the execution of tasks between officers in such a way as to ensure maximum reliability of the assignment. In this case, the time limit for each task should be taken into account.

To perform each task, the office has developed certain algorithms. So the algorithm for solving each tasks are:

Task 1 (website verification), the following actions are performed:

1. Examining the existing site code
2. Examining published vulnerabilities
3. Threat analysis
4. Hacking attempts through existing vulnerabilities

5. QA & TA Analysis
6. Data Analysis
7. Elimination of vulnerabilities and the introduction of new technologies based on the analysis.
8. Testing applications.

To solve Task 2 (audit of wireless networks) consists of the following actions:

1. Definition of existing technologies and coverage
2. Studying the configuration of access points and servers
3. Analysis of traffic and existing threats
4. Attempted unauthorized entry
5. Analysis of the data obtained in paragraphs 1-4
6. The introduction of modified technologies.

Task 3 solution (physical intrusion prevention) involves the following actions:

1. Familiarization with literature
2. Learning from previous invasion techniques
3. Consultation with external sources
4. Independent attempts to penetrate
5. Analysis of all information and conclusions
6. Security penetration

Models of performing tasks in the form of a work graph are presented in Fig. 2.

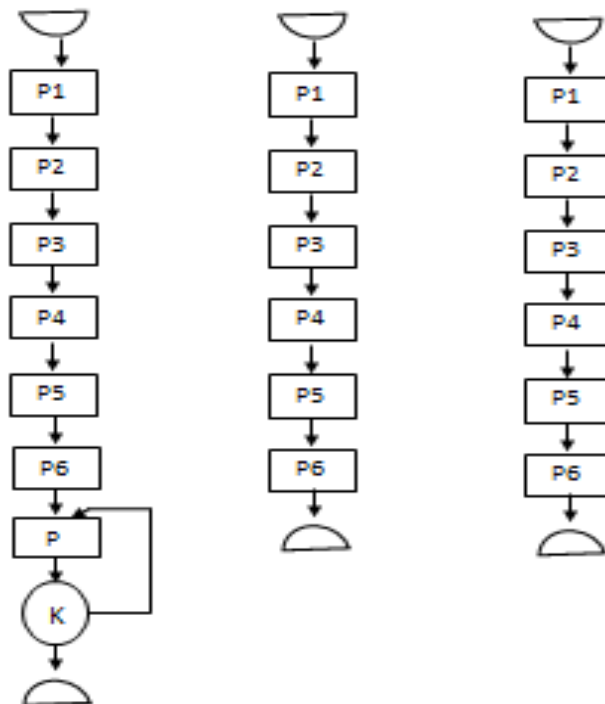


Fig. 2. Models of performing tasks

The initial data on the quality of the work operations of the activity algorithms for the implementation of tasks are given in Tables 3-6.

Table 3. The quality of the work operations of the activity algorithms for the task 1

Officers	Parameters of Working operations	p1	p2	p3	p4	p5	p6	p7
1	B	0,99	0,98	0,96	0,98	0,99	0,98	0,998
	M	56	64	40	56	56	56	240
2	B	0,978	0,998	0,987	0,996	0,967	0,952	0,943
	M	59	61	45	57	59	54	247
3	B	0,988	0,986	0,987	0,998	0,987	0,987	0,975
	M	58	62	43	58	58	55	245

Table 4. The quality of the work operations of the activity algorithms for the task 2

Officers	Parameters of Working operations	p1	p2	p3	p4	p5	p6
1	B	0,99	0,98	0,96	0,98	0,99	0,98
	M	56	64	40	56	56	56
2	B	0,978	0,998	0,987	0,996	0,967	0,952
	M	59	61	45	57	59	54
3	B	0,988	0,986	0,987	0,998	0,987	0,987
	M	58	62	43	58	58	55

Table 5. The quality of the work operations of the activity algorithms for the task 3

Officers	Parameters of Working operations	p1	p2	p3	p4	p5	p6
1	B	0,978	0,982	0,999	0,99	0,98	0,97
	M	16	12	3	24	40	56
2	B	0,909	0,991	0,997	0,967	0,952	0,943
	M	20	15	5	26	42	58
3	B	0,987	0,978	0,975	0,988	0,974	0,999
	M	15	13	4	25	40	53

The initial data on the quality of the control operation are given in table 6.

Table 6. Initial data on the quality of the control operation

Officers	Parameters of control operations		
	Quality control		Time
	K^{11}	K^{00}	M
1	0,99	0,97	24
2	0,989	0,968	28
3	0,979	0,987	27

Here, B^1 is the probability of error-free execution of a work operation; K^{11} is the probability of recognition of a work operation performed correctly, when actually performed correctly; K^{00} is the probability of recognition of a work operation performed incorrectly, when actually performed incorrectly; and M are the mathematical expectation of the operation time [20-23].

The data in tables 3, 4 and 5 are obtained by the subsystem for the formation of the source data. The principle of operation is based on the use of expert methods of assessment and neuro-fuzzy modeling. The source data are loaded automatically. The manager needs to choose only a list of employees, a list of tasks, and set time limits.

The results are presented in the form of a job assignment matrix (Fig. 3), in the form of correlation of employees and tasks for strategy 1.

Tasks	Officers		
	Piter Volkov	Tanay Sveredenko	Victor Nikolenko
Task 1	1	0	0
Task 2	0	0	1
Task 3	0	0	1

Fig. 3. The result of solving the optimization problem

Tasks	Officers
Task 1	Piter Volkov
Task 2	Victor Nikolenko
Task 3	Victor Nikolenko

Fig. 4. Assigning employees to tasks

Resulting performance indicators (the probability of error-free execution and the mathematical expectation of the execution time) are presented in Fig. 5.

Officers	B	M, hour
Piter Volkov	0,996	595
Victor Nikolenko	0,960	470
Victor Nikolenko	0,905	150

Fig. 5. Resulting performance indicators

Visualization of the resulting quality indicators makes it possible to visually assess the predicted quality of performance (Fig. 6).

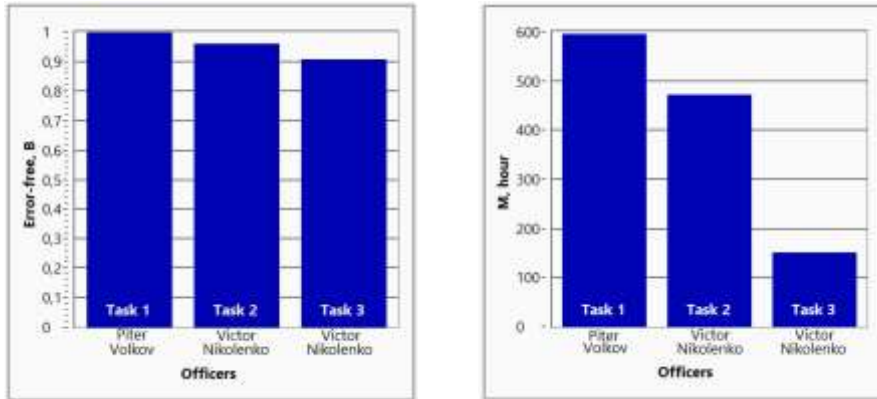


Fig. 6. Graphical representation of the resulting quality indicators

The results are presented in the form of a job assignment matrix (Fig. 7), in the form of correlation of employees and tasks for strategy 2.

Tasks	Officers		
	Piter Volkov	Tanay Sveredenko	Victor Nikolenko
Task 1	1	0	0
Task 2	0	1	0
Task 3	0	0	1

Fig. 7. The result of solving the optimization problem

Tasks	Officers
Task 1	Piter Volkov
Task 2	Tanay Sveredenko
Task 3	Victor Nikolenko

Fig. 8. Assigning employees to tasks

Resulting performance indicators (the probability of error-free execution and the mathematical expectation of the execution time) are presented in Fig. 9.

Officers	B	M, hour
Piter Volkov	0,996	595
Tanay Sveredenko	0,864	497
Victor Nikolenko	0,905	150

Fig. 9. Resulting performance indicators

Visualization of the resulting quality indicators makes it possible to visually assess the predicted quality of performance (Fig. 10).

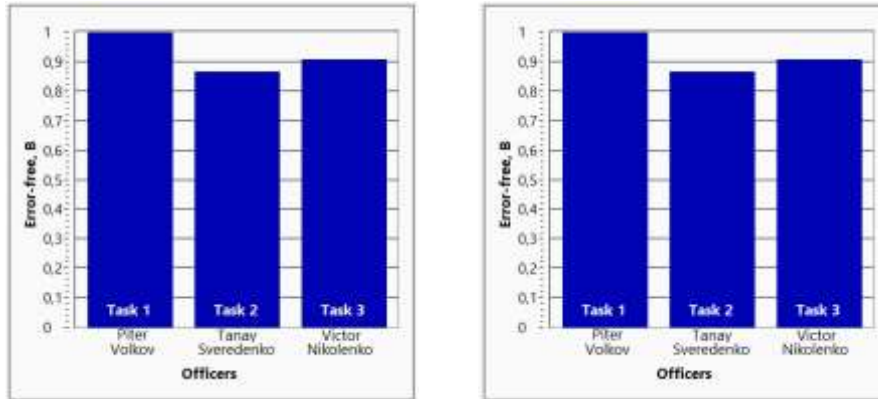


Fig. 10. Graphical representation of the resulting quality indicators

5 Discussion

The developed information technology allows the CISO to carry out the optimal appointment of his officers to perform tasks to ensure information security. Decision making is based on the obtained quantitative indicators of the quality of the tasks. Reliability of execution is maximized, taking into account time constraints. The structure of officers' activities and their individual characteristics of reliability and speed are taken into account.

However, it should be noted the high complexity of the method at the stage of preparation of the initial data. For successful operation of the system, it is necessary, first, to formalize the algorithms for performing tasks and obtain data on the probability-time indicators of the quality of operations for each officer [24-26].

6 Conclusions

The following main results were received in this paper:

- It is proposed to use the functional-structural theory of ergotechnical systems to ensure the security of information systems.
- The approach to the use of the specified method by the CISO for the optimal selection of specific performers from among the employees of the unit is demonstrated to perform information security tasks depending on the quality indicators of the work performed by each employee and the available time limit for the duration of each task, with the goal of maximizing the accuracy of the execution of the functioning algorithms, depending on the quality indicators of each employee.

- The possibility of such an optimal solution has been taken into account when one performer executes several tasks and tasks will not be given to another potential performer at all.

Unlike previously used methods, the use of the theory of ergotechnical systems to ensure the security of information systems allows us to formalize the process of decision-making by CISO to a greater extent.

The practical significance is that since the task is reduced to the linear programming problem, it can be solved within the framework of a wide class of information technologies and can be quickly included in the CISO's decision support system in companies of various types of activities.

In the future, studies will be conducted on the use of the functional-structural theory of ergotechnical systems in the development of CISO's policies, procedures, and guidelines, for example, to assess risks, identify and analyze incidents.

References

1. Peltier, Thomas R. *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*, Auerbach Publications, 2016.
2. Nazareth, Derek L., and Jae Choi, "A system dynamics model for information security management", *Information & Management* 52.1 (2015): pp. 123-134.
3. Safa, Nader Sohrobi, Rossouw Von Solms, and Steven Furnell. "Information security policy compliance model in organizations." *Computers & Security* 56 (2016): 70-82.
4. Layton, Timothy P. *Information Security: Design, implementation, measurement, and compliance*. Auerbach Publications, 2016.
5. Joshi, Chanchala, and Umesh Kumar Singh. "Information security risks management framework—A step towards mitigating security risks in university network". *Journal of Information Security and Applications* 35 (2017): pp. 128-137.
6. Soomro, Zahoor Ahmed, Mahmood Hussain Shah, and Javed Ahmed. "Information security management needs more holistic approach: A literature review". *International Journal of Information Management* 36.2 (2016): 215-225.
7. Grudzień, Łukasz, and Adam Hamrol. "Information quality in design process documentation of quality management systems". *International Journal of Information Management* 36.4 (2016): pp. 599-606.
8. Livshitz, Ilya, Pavel Lontsikh, and Sergey Eliseev. "The optimization method of the integrated management system security audit". 2017 20th Conference of Open Innovations Association (FRUCT). IEEE, 2017.
9. Jacobs, Stuart. *Engineering information security: The application of systems engineering concepts to achieve information assurance*. John Wiley & Sons, 2015.
10. Yoon, Junseob, and Kyungho Lee. "Advanced assessment model for improving effectiveness of information security measurement". *International Journal of Advanced Media and Communication* 6.1 (2016), pp. 4-19.
11. Hsu Jack Shih-Chieh, et al. "The role of extra-role behaviors and social controls in information security policy effectiveness". *Information Systems Research* 26.2 (2015): 282-300.
12. A.R. Haji Hosseini, M.J. Jafari, Y.Mehrabi, G.H. Halwani, A. Ahmadi, Factors influencing human errors during work permit issuance by the electric power transmission network operators, *Indian J. Sci.Technol*, 2012, vol. 5, issue 8, pp. 3169-3242.
13. Lavrov E., Tolbatov A., Pasko N., Tolbatov V. Cybersecurity of distributed information systems. The minimization of damage caused by errors of operators during group activity,

- Proceedings of 2017 2nd International Conference on Advanced Information and Communication Technologies, AICT 2017, Lviv, 2017, p. 83-87.
14. F. De Felice, A. Petrillo, Methodological Approach for Performing Human Reliability and Error Analysis in Railway Transportation System, *International Journal of Engineering and Technology*, 2011, vol. 3, issue 5, p. 341-353
 15. M.G. Grif, O. Sundui, E.B. Tsoy, Methods of designing and modeling of man-machine systems, *Proceedings of International Summer workshop Computer Science*, 2014, p. 38-40.
 16. E. Lavrov, N. Pasko, A. Krivodub, N. Barchenko, V. Kontsevich, Ergonomics of IT outsourcing. Development of a mathematical model to distribute functions among operator, *Eastern-European Journal of Enterprise Technologies*, 2016, vol. 2, issue 4 (80), p. 32-40. doi: 10.15587/1729-4061.2016.66021
 17. V. Lyubchak, E. Lavrov, N. Pasko, Ergonomic support of man-machine interaction. Approach to designing of operators' group activities, *International Journal of Bio-Medical Soft Computing and Human Sciences*, 2011, vol. 17, issue 2, p. 53-58.
 18. Zaritskiy O., Pavlenko P., Tolbatov A., Data representing and processing in expert information system of professional activity analysis, *Proceedings of the 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science, TCSET 2016, Lviv-Slavske, 2016*, p. 831-833.
 19. Zaritskiy O., Pavlenko P., Sudic V., Tolbatov A. et al, Theoretical bases, methods and technologies of development of the professional activity analytical estimation intellectual systems, *Proceedings of 2017 2nd International Conference on Advanced Information and Communication Technologies, AICT 2017, Lviv, 2017*, p. 101-104.
 20. Walia Navneet, Harsukhpreet Singh and Anurag Sharma. ANFIS: Adaptive neuro-fuzzy inference system-a survey, *International Journal of Computer Applications* 123.13 (2015).
 21. S. Gnatyuk, Critical Aviation Information Systems Cybersecurity, Meeting Security Challenges Through Data Analytics and Decision Support, *NATO Science for Peace and Security Series, D: Information and Communication Security*. – IOS Press Ebooks, Vol.47, №3, pp. 308-316, 2016.
 22. S. Gnatyuk, V. Sydorenko, M. Aleksander, Unified data model for defining state critical information infrastructure in civil aviation, *Proceedings of the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Kyiv, Ukraine, May 24-27, 2018, pp. 37-42.
 23. Fedushko S. (2020) Adequacy of Personal Medical Profiles Data in Medical Information Decision-Making Support System. *CEUR Workshop Proceedings*. – 2020. Vol 2544: Proceedings of the International Conference on Rural and Elderly Health.
 24. Fedushko S., Michal Gregus ml., Ustyianovych T. Medical card data imputation and patient psychological and behavioral profile construction. The 9th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH 2019) November 4-7, 2019, Coimbra, Portugal *Procedia Computer Science*. Volume 160, 2019, pp. 354-361.
 25. Fedushko S., Trach O., Kunch Z., Turchyn Y., Yarka U. Modelling the Behavior Classification of Social News Aggregations Users. *CEUR Workshop Proceedings*. 2019. Vol 2392: Proceedings of the 1st International Workshop on Control, Optimisation and Analytical Processing of Social Networks (COAPSN-2019). pp. 95–110.
 26. Trach O., Fedushko S. (2020) Determination of Measures of Counteraction to the Social-Oriented Risks of Virtual Community Life Cycle Organization. In: Shakhovska N., Medykovskyy M. (eds) *Advances in Intelligent Systems and Computing IV. CCSIT 2019. Advances in Intelligent Systems and Computing*, vol. 1080. Springer, Cham. pp. 680-695.