DOI: https://doi.org/10.15276/hait.05.2022.22
UDC 004.94

Functional modeling of the organization's information security culture state monitoring system development

Mariia M. Voitsekhovska[1)]
ORCID: https://orcid.org/0000-0002-1711-101X; m.voitsekhovska@stu.cn.ua. Scopus Author ID: 57192818403
Mariia S. Dorosh[1)]
ORCID: https://orcid.org/0000-0001-6537-8957; mariyaya5536@gmail.com. Scopus Author ID: 56912183600
Viktor F.Grechaninov[2)]
ORCID: https://orcid.org/0000-0001-6268-3204; vgrechaninov@gmail.com. Scopus Author ID: 57219055091
Olena V. Verenych[3)]
ORCID: https://orcid.org/0000-0003-0972-6361; verenych@ukr.net. Scopus Author ID: 57189383746
[1)] Chernihiv Polytechnic National University, 95, Shevchenko Str. Chernihiv, 14035, Ukraine
[2)] Institute of Mathematical Machines and Systems Problems of the NASU, 42, Acad. Glushkov Ave. Kyiv, 03187, Ukraine
[3)] Kyiv National University of Construction and Architecture, 31, Povitroflotsky Ave. Kyiv, 03037, Ukraine

ABSTRACT

The mass transition to remote work, which triggered the quarantine and then military actions on the territory of Ukraine, led to new challenges to increase the level of information protection. In addition, permanent information and cyber-attacks create a persistent danger to physical and information systems. This, in turn, requires a clear understanding of the level of information security of various organizations, especially for critical infrastructure. An important component of the organization's information security is the information security culture of all participants in internal information processes. Such kind of influence is usually called the Human Factor. The paper`s aim reveals with two goals. The first goal is the information processes functional modeling of the information security culture level assessment automation as a part of the overall organization`s security system. The second part consists in the information security system of project (ISSoP) maturity model development to provide the vital level of trust to organization within project activities. The functional model of system development presents a number of separate processes: the formation of questionnaires, data collection, and assessment of information security culture at the personal, department and organizational levels. Defined input and output data, mechanisms, models, methods and control elements for each process. This model can be included as a component of the system for determining the level of the common organization`s information security system. The maturity stages of the information security culture in a project include different Info-Sec activities at various stages of its life cycle. Such kind of activities need to be taken into account while developing organization`s information security systems.

Keywords: Information security; information system; organization, culture

***For citation*: Voitsekhovska M. M., Dorosh M. S, Grechaninov V. F., Verenych O. V."Functional modeling of the organization's information security culture state monitoring system development". *Herald of Advanced Information Technology*. 2022; Vol. 5 No. 4: 297–308. DOI: https://doi.org/10.15276/hait.05.2022.22**

INTRODUCTION

A few years ago, remote work was a common practice for a few. Then COVID-19 quarantine forced a mass transition from offices to homes. Work from home office became even more relevant for Ukrainians during the full-scale invasion of the Russian Federation. Such a drastic change returned to the game all risks eliminated mostly in corporate networks. The main reason is the lack of security equipment in the home network, which is so expensive and inaccessible to the regular user.

Let's mention about using personal laptops for business purposes and we'll obtain the most vulnerable information security system (ISS) rather equal to its absence.

At the same time, organizations whose activities allow remote work of employees try to maintain all or most business processes at the previous level. And project activity is not an exception.

Note that in contrast to the normal activities of the organization, remote work for projects is more common, as projects are implemented in most cases with the involvement of external participants, but information security issues are almost not included to the basic standards of project management.

LITERATURE REVIEW

This issue attracts research attention in various domains. E.g., the study [1] defined the importance of information security in software development projects. The agile development paradigm conflicts with traditional security assurance by emphasizing

© Voitsekhovska, M., Dorosh, M., Grechaninov V., Verenych, O., 2022

This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/deed.uk)

the delivery of functional requirements and a reduction in structured and linear development styles. The authors highlight the importance of agile security practices centering around individuals and culture and contributes to the literature by providing a representation of agile security practices that encompasses a broad range of focal areas.

In turn, Robert J. Ellison in work [2] pointed that the need for information security of the project is justified with fact that Software errors can be introduced by disconnects and miscommunications during the planning, development, testing, and maintenance of the components. The likelihood of disconnects and miscommunications increases as more system components have to satisfy security requirements. The author claims that project managers should consider the additional communications requirements, linkage among life-cycle activities, and the potential usage environment as these items relate to security needs.

As Eva Short noticed: "Understanding phishing attacks, promoting better password management and the basics of encryption are all things employees should be educated about if a company wants them to make better choices in this regard" [3]. Moreover, she outlines the cyber safety is similar to the road safety: "eminently practical information that every person living in society needs to know" [3].

The global COVID-19 quarantine, on the one hand, provoked intensive adaptation to new working conditions and served as a push for the transition to remote work in "digitized" domains. On the other hand, the anxiety associated with remote access vulnerabilities occurred. Understanding these threats has led to increased user awareness activities [4].

The Report [5] on joint research by the ISACA and CMMI Institute conducted in 2018, also indicates the importance of taking measurements of culture indicators. As one of the trends noted in Report is employee training (especially in BYOD case) devoted to personal devices safe using and social networks behavior. Some companies use games during group training, motivating the most security-conscious employees with rewards.

Other survey [6] showed that ⅔-s of responded professionals in IS domain labeled employees as the "weakest link" in cyber threats protection efforts.

Anna Georgiadou et. al [7] propose a cyber-security culture evaluation model gathered core security human-related elements, most commonly used in security frameworks. Later, Anna`s team conducted the survey on the organizations` cyber security culture readiness to remote work due to COVID-19 pandemic [8]. Nurul Asmui Azmi Md Azmi et. al. [9] made attempt to predict information security culture within telecommunication companies` employees in Malaysia, emphasizing the employees` security behavior as link between information security awareness and information security culture. Nevertheless, none of mentioned ISC evaluation models and tools embedded into information security system of organization as a routine. Another approach for information security culture evaluation was proposed by Krunoslav Arbanas et. al. [10], and presented framework includes technological, organizational and social aspects.

Since timing is one of the key criteria for most projects, the work within the project requires strict adherence to the project plan. Therefore, the working arrays of information finally settled in personal gadgets, gathered to private networks.

Therefore, taking into account the global nature of the changes that have taken place, following questions about the safety of business processes and project activities, problems arise in preventing sensitive resources leaks, and in the worst case, in eliminating the consequences.

THE PURPOSE OF THE ARTICLE

The aim of this work is to carry out the information processes functional modeling to automate the of the information security culture level assessment as a part of the overall organization`s security system.

In addition, the overall level of organization`s security directly affects the degree of project stakeholders` trust. It`s necessary to determine the maturity level of information security management systems (ISMS) of all project stakeholders. And all mentioned above leads to decision to create the model of information security system of project (ISSoP) maturity development.

METHODS

Functional modeling in the IDEF0 notation allows to visualize and display with the required detail the necessary elements (inputs, controls, execution mechanisms and results). The main emphasis is on the logical relationship between the work performed. The conceptual model depicted in this way is represented by a "black box" and then may be detailed.

The conceptual model is created with system analysis methods.

MAIN PART. FUNCTIONAL MODEL OF ORGANIZATION'S ISC LEVEL DETERMINATION

The functional model is based on the conceptual model [11] and presented on the Fig. 1.

To get a complete picture of the processes necessary for assessing the information security culture (ISC) level of organization, a conceptual model can be represented as a sequence of six tasks depicted by a functional model.

As a result of the decomposition of the general issue "Determine the level of the organization's ISC" (Fig. 2), the process is divided into 6 main tasks:

- Fill the system with input information.
- Generate questionnaires.
- Conduct the survey.
- Assess the ISC level by of departments.
- Assess the ISC level of organization.
- Create the report and provide recommendations.

Before assessing the organization's ISC level, the expert with the help of software should fill the system with the necessary information using the Data Collection module. The Fig. 2 clearly presents the stages, as well as the controls and mechanisms involved in the relevant stage. The initial information (lists of themes, roles, questions, and competencies; potential situational recommendations; and results of IS risks analysis of the organization) stored in a database to be used to generate questionnaires. Taking into account the originality of each organization because of differences in scope, mission and structure, the expert has to generate separate sets of questionnaires and stored in the database. After collecting and structuring all the information, filling in the weight matrices, and generating questionnaires, the system is ready to assess the organization's ISC level.

Using cloud services, each employee is provided with a questionnaire for the survey. After completing the survey, all the answers of employees are used to assess the ISC for each department of the organization separately. On the basis of the received results on departments definition of ISC level of organization as a whole is carried out. The final stage is to generate a report on the results of the evaluation, and provide the organization with recommendations on the choice of measures to improve the level of ISC.

Each task is performed with the support of the developed software and data-base. An expert is an integral participant of all the processes.

Task No. 1 functional model

Task No.1 divides on several subtasks visualized on Fig. 3.

Form requirements for the organization's ISC level. According to the provisions of regulatory documentation, the requirements of the organization's internal IS policy, as well as the best practices on ISO/IEC 27000 group of international standards, also based on the organization's IS risks analysis, the expert forms requirements for the organization's ISC on certain indicators. The received requirements to the level of organization ISC are saved in a database.

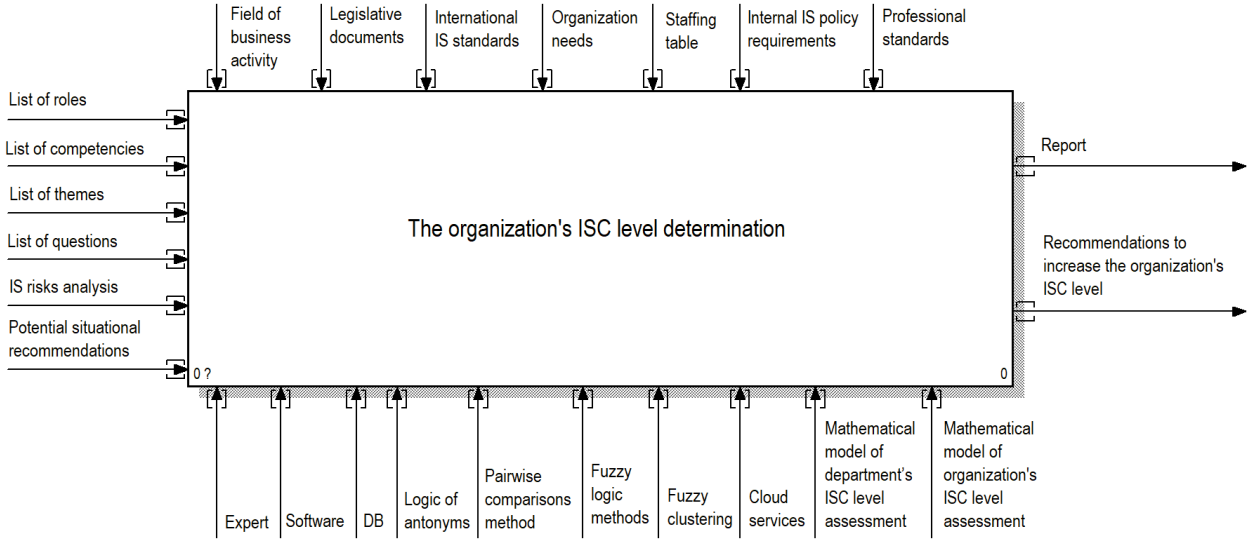

Fig. 1. **Conceptual model of top-level development process "The organization`s ISC level determination"**

Source: **compiled by the [11]**

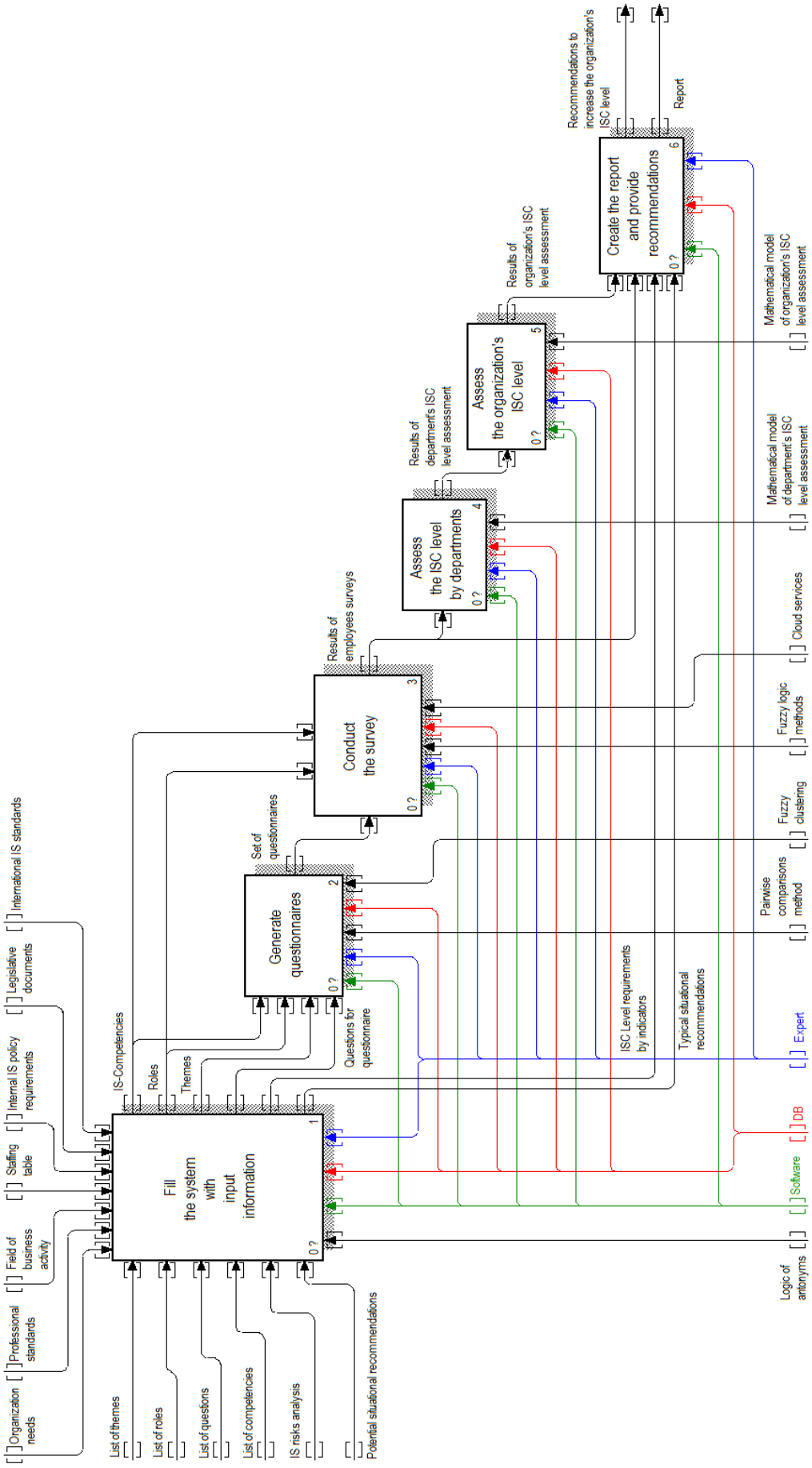

Fig. 2. **"Determine the level of the organization's ISC" task functional model**

Source: **compiled by the authors**

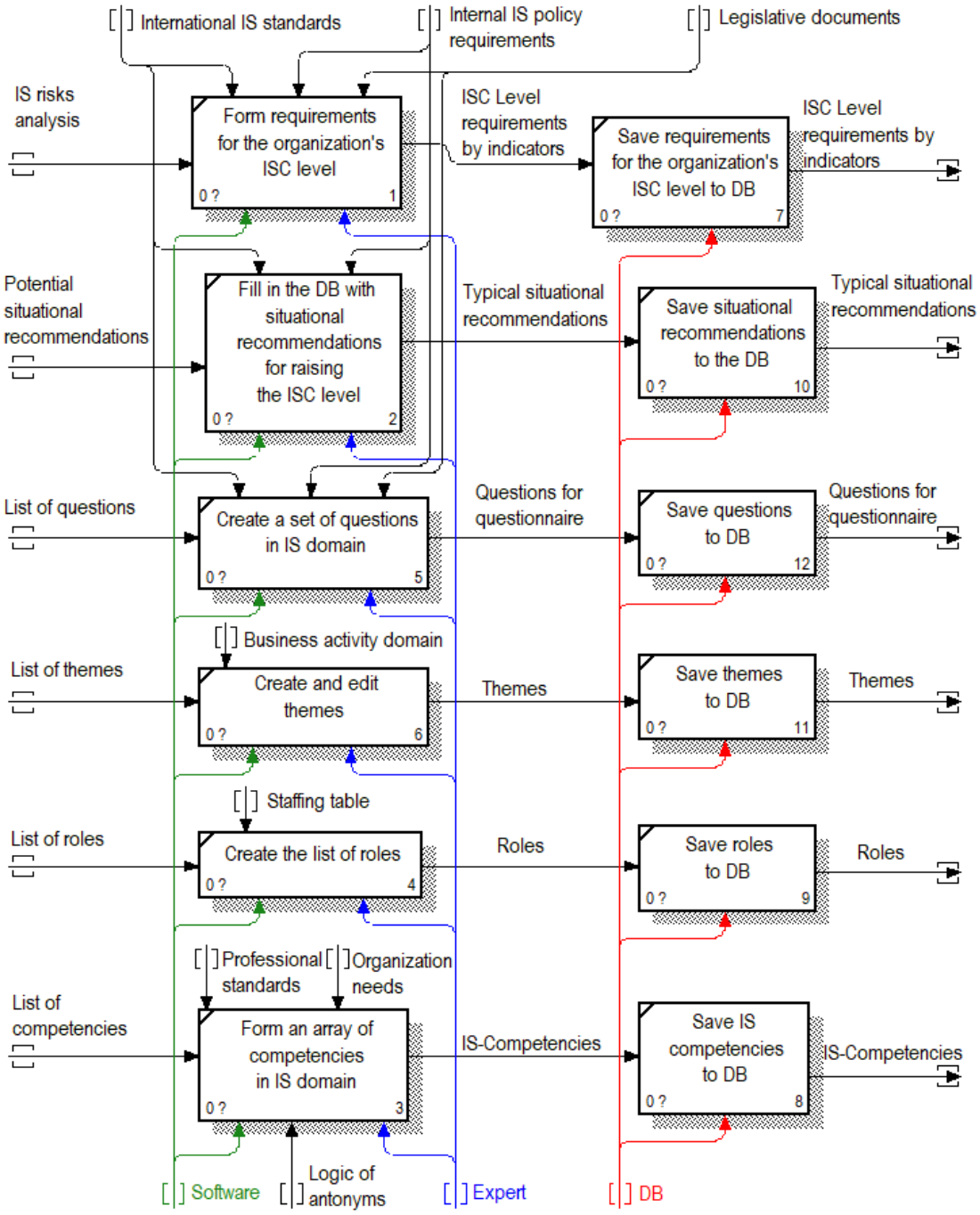

Fig. 3. **"Fill the system with input information" task functional model**

Source: **compiled by the authors**

Fill in the database of situational recommendations for raising the ISC level (personal, department and organization). The expert, having knowledge of possible measures to increase the level of ISC, forms situational recommendations that should be saved in the relevant table of the database.

Create a set of questions in IS domain. When creating the list of questions to be used in the generation of questionnaires, the expert should be guided by regulations, international standards in the field of IS (primarily ISO/IEC 27001, 27002) and the IS policy requirements force within the organization. Selected and edited questions, as well as answer options are entered in the relevant tables of the database.

Create and edit themes. Themes should be formed based on the scope of the organization. Themes may relate to technical and technological aspects, interaction with the external information space and its participants, other aspects of activities that directly or indirectly affect the ISC. Selected and edited *themes save to DB.*

Create the list of roles. The list of roles is filled by an expert on the basis of the staff list of the organization and job descriptions. *The list of roles is stored in the DB.*

Form an array of competencies in IS domain. The list of competencies is mandatory input and should be edited by an expert based on the professional standards and needs of the organization. The decision to include a certain competence in the matrix is supported on the logic of antonyms. Selected *competencies saved to the database table.*

The results of the first stage are the requirements for the ISC level, situational recommendations, themes, questions for the questionnaire, roles and IS competencies.

Task No. 2 functional model

The processes of the Task No.2 are presented in Fig. 4. The task "Generate questionnaires" is divided into three subtasks.

Form fuzzy clusters of questions by themes. The array of questions for the questionnaire is divided into clusters according to themes using fuzzy clustering. The expert determines the degree of question belonging to each of the themes.

Assign the weight of the impact to each question on the resulting evaluation of the questionnaire. Based on the set of competencies for each role, the expert assigns weights for each question within the questionnaire. Determination of weights is realized with the pairwise comparisons method.

Save the weight matrix to the appropriate database table.

The result of processing the input data on the second stage is a set of questionnaires corresponded to certain roles and highlight the level of user competencies on certain themes.

Task No. 3 functional model

The task "Conduct the survey" presented in Fig. 5 provides the following subtasks.

Distribute questionnaires by positions (competencies). The distribution of the questionnaires formed at the previous stage is carried out by the expert according to the positions occupied by users (employees) within the framework of job responsibilities. The questionnaires generated as forms and distributed using cloud services, contain questions and answer options.

Collect survey results. The subtask of automated results collection is solved with use of cloud services. This approach allows automatic filling of tables with data such as date and time of the survey, contact email address (disabling the option to collect this information makes it possible to conduct anonymous surveys, which is convenient for self-assessment), and answers (selected item or detailed answer of the respondent, which requires the assessment of the expert himself). At the same time, both standard and unique questionnaires, formed for each user separately, may be provided for the questionnaire.

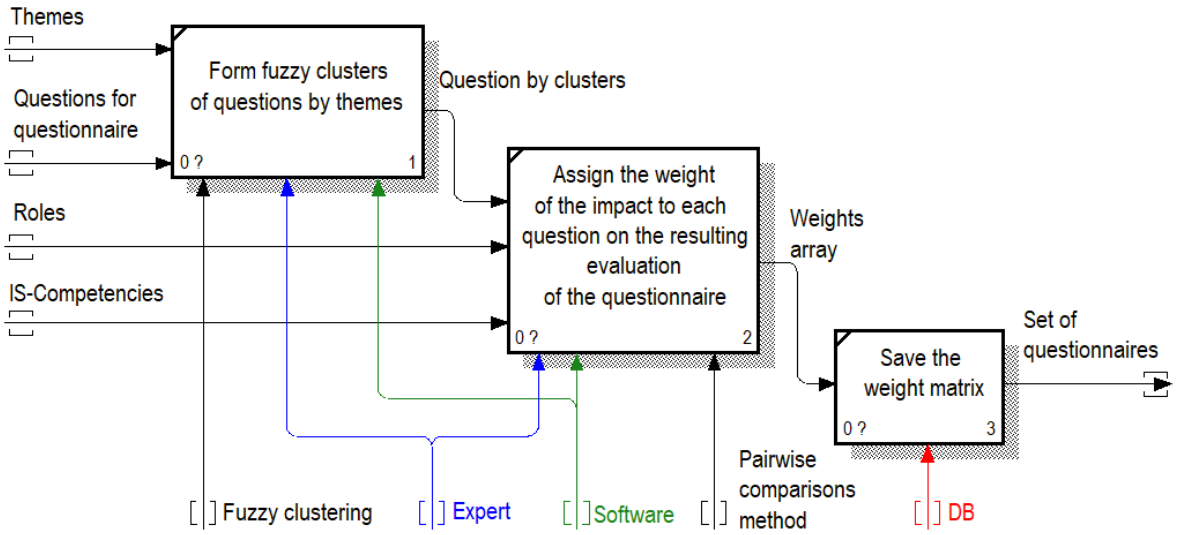

Fig. 4. **"Generate questionnaires" task functional model**
Source: **compiled by the authors**

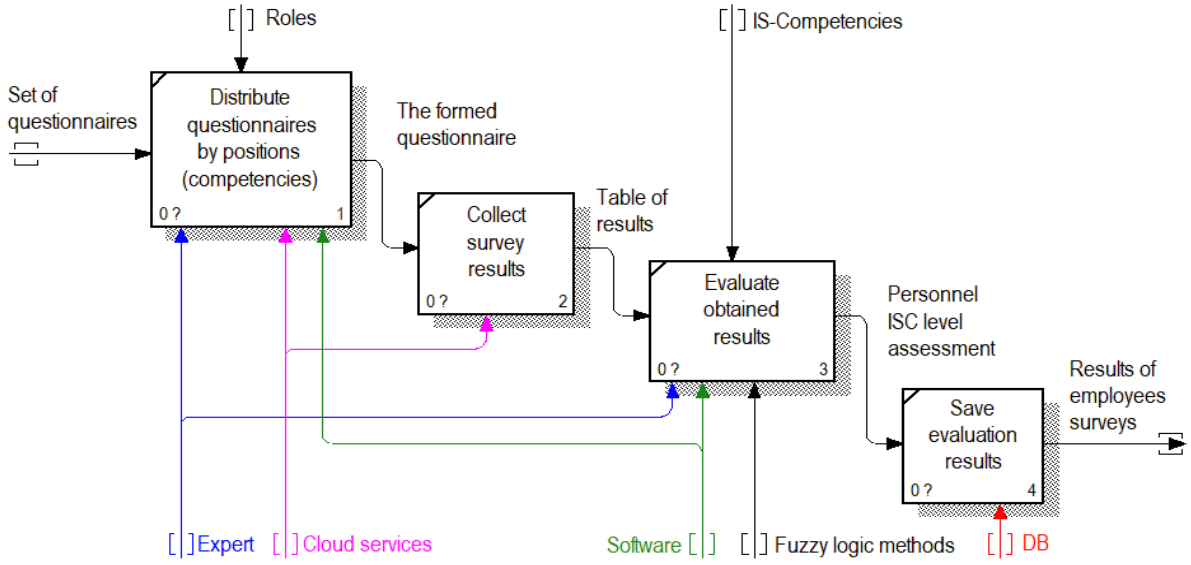

Fig. 5. **"Conduct the survey" task functional model**
Source: **compiled by the authors**

Evaluate obtained results. The evaluation of the survey results is carried out by an expert on the basis of fuzzy logic [12], taking into account the competencies that must be sufficiently available.

Save evaluation results. Estimates of processing the respondents' answers using the fuzzy evaluation are stored in the database. These records contain a time note, which allows to rank the questionnaire to the definite event to assess the ISC level of the organization (as a project or stage of the process), as well as to observe the dynamics of personal ISC of employees.

Task No. 4 functional model

The results obtained on the previous stage are the input information for the process "Assess the ISC level by departments" as shown on Fig. 6.

The task of the ISC level assessment on departments tier provides on the result of determining the personal ISC level among employees of the department. Based on the mathematical model [9] for estimating the department's ISC, the expert obtains the result of each department's ISC assessment. The obtained results are stored in the database table.

Task No. 5 functional model

The fifth task "Assess the organization's ISC level" (Fig. 7), like the previous one, consists of two subtasks.

Evaluate the ISC level of organization. Received indicators of departments ISC are the input information of the block. The expert defines the general estimation of organization's ISC using mathematical model [13] of ISC estimation of the organization.

Save results to the database. The record containing the result of the previous process is entered into the database with a note on the date (or period) of the assessment.

Task No. 6 functional model

The final task of the organization's ISC assessment is the successive implementation of two processes. Decomposition of the business process "Create the report and provide recommendations" is presented on Fig. 8. Let`s consider in details.

Compare the obtained results with the requirements for the ISC level by indicators. The input for this is the previously defined (at the first stage) requirements for the ISC level by indicators, access to available in the system standard situational recommendations, as well as the results of employee surveys and the results of assessing the ISC level of the organization. In case of underestimated results, the system refers to the database of production rules and determines the appropriate recommendation. A set of such recommendations will be included in the report.

Generate a report. The data obtained after the comparison form the basis for generating the report. Relevant recommendations are selected from the database regarding measures to increase the ISC level of employees, as well as recommendations for managers, which elements should be addressed at the administrative level. The expert checks the prepared report.

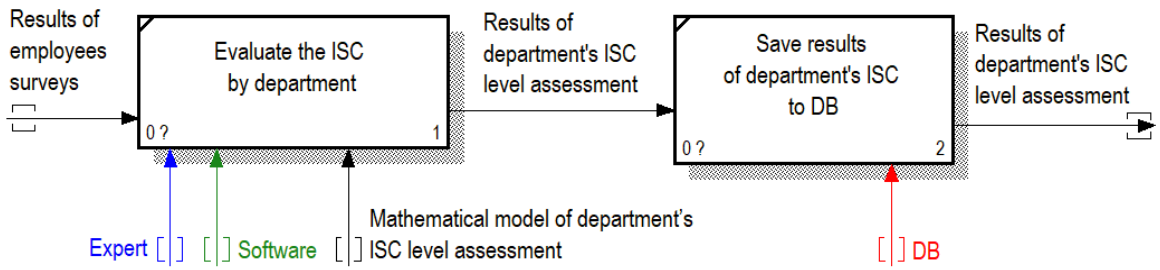

Fig. 6. **"Assess the ISC level by departments" task functional model**
Source: **compiled by the authors**

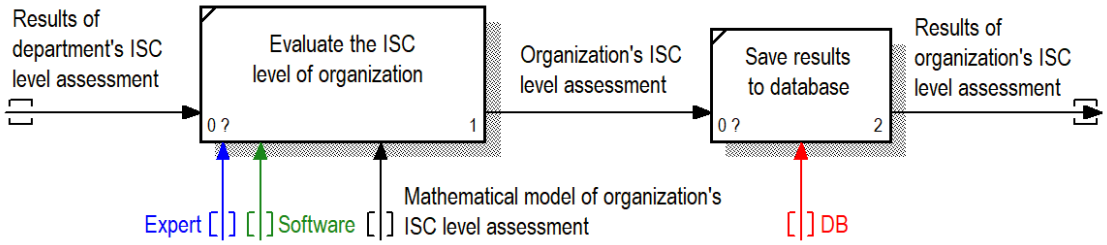

Fig. 7. **"Assess the ISC level of organization" task functional model**
Source: **compiled by the authors**

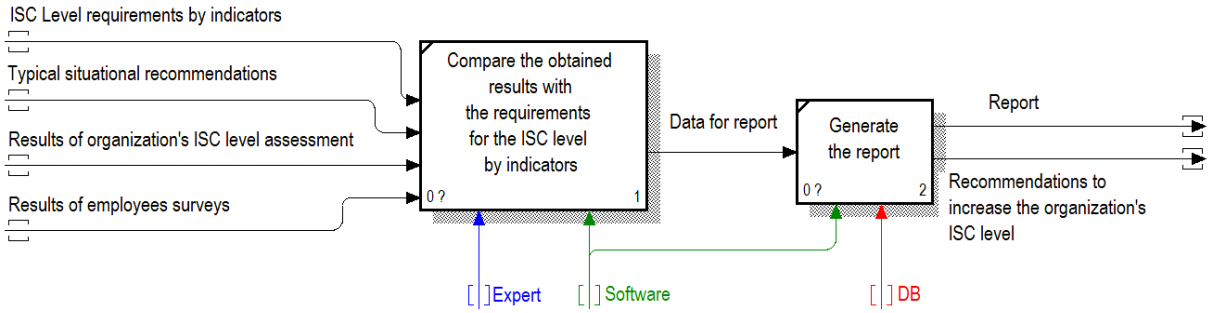

Fig. 8. **"Create the report and provide recommendations" task functional model**
Source: **compiled by the authors**

Determination of ISS maturity stages in Project (ISSoP)

An important component of the organization is its project activities, which should also provide an appropriate level of information security culture, which is one of the components of the overall level of security of the organization. The degree of project information security directly affects the degree of project stakeholder's trust, which in turn determines the opportunities for development of the organization through their implementation. The most significant information security risks that affect PM are: DDoS attack, self-propagating ransomware, malware, phishing, employees, vishing.

Unlike the ISC organization, the ISC project has some features:

- It must take into account the ISC level of the project stakeholders;
- It is necessary to create a separated common information environment of the project, which from project to project will contain different components and, accordingly, different requirements for their security;
- Should take into account the general concept of information security management of the organization;
- Requires constant monitoring due to the change of project stakeholders during its implementation;
- Depends on the level of awareness of the project manager in the field of information security;
- The need to determine the degree of influence of the level of information security of the project on the overall success of its implementation.
- All these features affect the overall level of

security of project information, and should be taken into account when building a general information security system of the organization.

- To determine ISSoP is necessary to determine the maturity level of ISMSs [14] of all project stakeholders. Such assessment can be made on the basis of the ISSoP maturity levels defined in Fig. 9.

The *first* stage "Project Initialization". At this time, the focus is on addressing the feasibility of the project, and P-M`s efforts are aimed at proving the project effectiveness and attracting the necessary stakeholders for its implementation. At this stage, resolving InfoSec issues can be driven by potential stakeholders and depends entirely on their own attitude to the issue. Only the primary means of informational interaction between stakeholders can be formed here. It is implemented using but not only project management systems (PMS). They answer a series of questions to determine the status of a project at a specific point in time and identify risks early on. As such systems are often the sole source (accumulator) of project activity, it is important that this information is securely protected from persons without an appropriate level of access. At this stage, it is important to determine the importance of InfoSec for each project stakeholder.

Stage *two* is "Fragmentary Protection". It should be formed at the project planning stage, as the project stakeholders are already identified here, and a communication plan for the project is developed. It is important to choose the software tools for interaction, planning and control of the project, depending on the defined security requirements. The project forms separate documents governing the InfoSec of the project and its stakeholders.

The *third* stage is "System Protection". It should be achieved at the stage of project implementation. Past workflows make it possible to create a common information safe space for project stakeholders. Sustainability of processes at this stage allows formalizing and documenting the main provisions of the project InfoSec; stakeholders understand its values and all processes are combined into a common information flow. As a result, the project provides an opportunity to analyse information on all aspects of management activities, as well as to obtain prompt information on the degree of use of resources for all project stakeholders. It uses protection systems integrated into the system that does not need to be certified. Protective activities are regulated by regulatory documents.

Stage *four* – "Managed Protection" – coincides with the project completion phase. Here, it is important to retain the generated project information and provide technical support for the project results implementation. In this case, the formed Project InfoSec can be the basis for further interaction with its adjustment for new stakeholders.

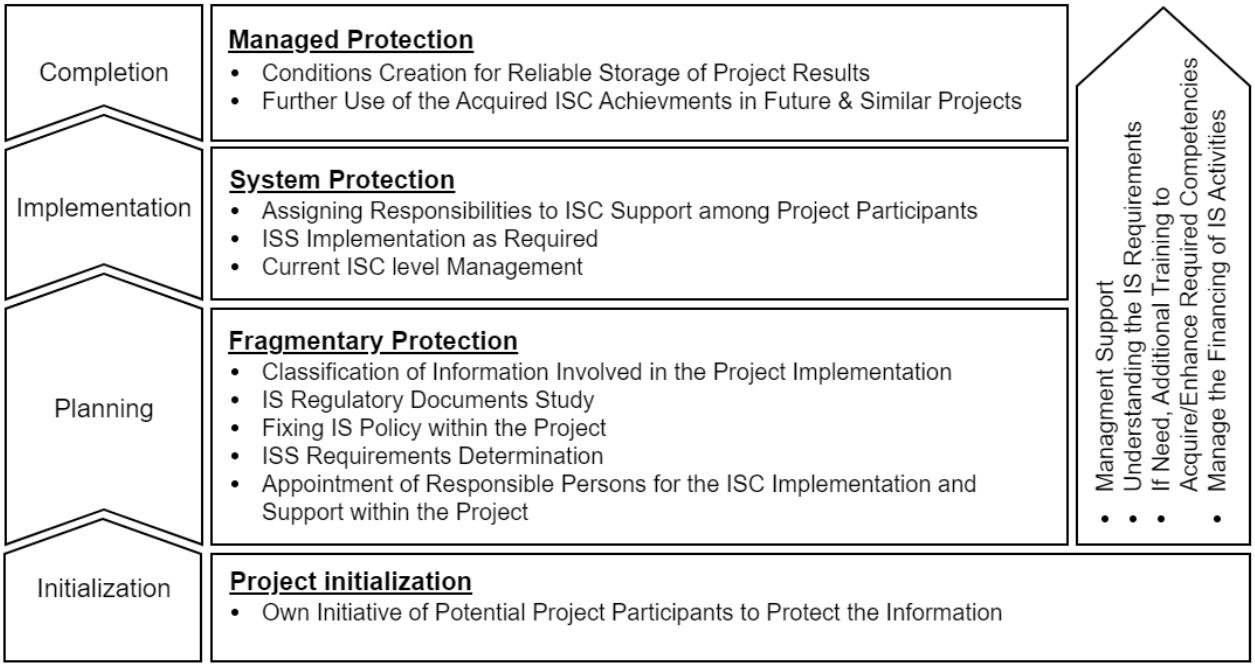

Fig. 9. **Stages of maturity for ISMS of project**
Source: **compiled by the authors**

At this stage, the security features are fully operational, and the integrated ISS in the project creates the conditions for reliable and safe operation by applying a set of security measures that meet the basic requirements:

- Successfully resist the vast majority of the attacks.
- In case of significant failures, which can occur during external influences of various kinds (including, and as a result of successful attacks), the system must have the capacity for complete self-recovery or restored in the acceptable terms and with minimal losses.
- When building a system, the optimal ratio (system price) / probable losses must be considered.

CONCLUSIONS

Performed functional modeling of the system of the organization's information security culture level assessment clearly defines the main stages and their characteristics for the construction of individual modules of the information system for assessing the overall level of organization`s the security. On the other hand, such systems can be separate tools for determining the ISC at any organizational level.

The considered levels of ISC project development, as a component of the overall security system of the organization, also ensure the integrity of the system, as the project activity is part of the organization and that ensures its development. The identified features of information security management in the project prove the need to develop and apply separate approaches to the formation of a secure project space.

Further research may be in the field of mathematical modeling to determine the integrated indicator of the ISC level, taking into account the project activities.

REFERENCES

1. Newton, N., Anslow, C. & Drechsler, A. "Information security in agile software development projects: A critical success factor perspective". *In: Proceedings of the 27th European Conference on Information Systems (ECIS)*. Stockholm & Uppsala: Sweden. 2019. – Available from: https://aisel.aisnet.org/ecis2019_rp/92. – [Accessed: Sept. 2021].

2. Ellison, R. J. "Security and project management". Software Engineering Institute, Carnegie Mellon University. 2013. – Available from: https://resources.sei.cmu.edu/asset_files/WhitePaper/2013_019_001_297293.pdf. – [Accessed: Sept. 2020].

3. Short, E. "What is cybersecurity culture, and why is it important in the workplace?" Silicone Republic. 2018. – Available from: https://www.siliconrepublic.com/careers/cybersecurity-culture-workplace. – [Accessed: Sept. 2020].

4. "How to manage ransomware attacks against your remote workforce". Cyber Security Hub. 2020. – Available from: https://www.cshub.com/network/webinars/how-to-manage-ransomware-attacks-against-your-remote-workforce. – [Accessed: Sept. 2021].

5. "Cyber security culture report: Narrowing the culture gap for better business Result". ISACA/CMMI Institute. 2018. – Available from: https://cmmiinstitute.com/getattachment/c335c66a-7000-48b4-b953-acbf395c5832/attachment.aspx. – [Accessed: Sept, 2021].

6. Miller, D. "The Weakest Link. The role of human error in cybersecurity". SecureWorld. 2018. – Available from: https://www.secureworldexpo.com/industry-news/weakest-link-human-error-in-cybersecurity. – [Accessed: Sept. 2021].

7. Georgiadou, A., Mouzakitis, S., Bounas, K. & Askounis, D. A. "Cyber-security culture framework for assessing organization readiness". *Journal of Computer Information Systems*. 2022; 62 (3): 452–462. DOI: https://doi.org/10.1080/08874417.2020.1845583.

8. Georgiadou, A., Mouzakitis, S. & Askounis, D. Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Secur J*. 2022. 35: 486–505. DOI: https://doi.org/10.1057/s41284-021-00286-2.

9. Md Azmi, N. A. A., Teoh, A. P., Vafaei-Zadeh, A. & Hanifah, H. "Predicting information security culture among employees of telecommunication companies in an emerging market". *Information and Computer Security*. 2021; 29 (5): 866–882. DOI: https://doi.org/10.1108/ICS-02-2021-0020.

10. Arbanas, K., Spremic, M. & Zajdela Hrustek, N. “Holistic framework for evaluating and improving information security culture’. *Aslib Journal of Information Management.* 2021; 73 (5): 699–719. DOI: https://doi.org/10.1108/AJIM-02-2021-0037.

11. Lytvynov, V., Dorosh, M., Bilous, I., Voitsekhovska, M. & Nekhai, V. “Development of the automated information system for organization’s information security culture level assessment”. *Technical Sciences and Technologies.* 2020; 1 (19): 124–132. DOI: https://doi.org/10.25140/2411-5363-2020-1(19)-124-132.

12. Dorosh, M., Voitsekhovska, M. & Balchenko, I. “Research and determination of personal information security culture level using fuzzy logic methods. In: Hu, Z., Petoukhov, S., Dychka, I., He, M. (eds). Advances in computer science for engineering and education *II*. *ICCSEEA* 2019. *Advances in Intelligent Systems and Computing.* 2020; 938: 503–512. *Springer, Cham*. DOI: https://doi.org/ 10.1007/978-3-030-16621-2_47.

13. Shkarlet, S., Lytvynov, V., Dorosh, M., Trunova, E. & Voitsekhovska, M. “The model of information security culture level estimation of organization. In: Palagin, A., Anisimov, A., Morozov, A., Shkarlet, S. (eds). Mathematical modeling and simulation of systems. MODS 2019. *Advances in Intelligent Systems and Computing.* 2020; 1019: 249–258. *Springer: Cham.* DOI: https://doi.org/10.1007/978-3-030-25741-5_25.

14. Zaginailov, Iu. N. “Teoriia informatcionnoi bezopasnosti i metodologiia zashchity informatcii”. *Information Security Theory and Information Security Methodology*. *Directmedia.* Moscow-Berlin: 2015.

Conflicts of Interest: the authors declare no conflict of interest

Received 05.10.2022
Received after revision 25.11.2022
Accepted 15.12.2022

DOI: https://doi.org/10.15276/hait.05.2022.22
УДК 004.94

Функціональне моделювання розробки системи моніторингу стану культури інформаційної безпеки організації

Войцеховська Марія Михайлівна [1)]
ORCID: https://orcid.org/0000-0002-1711-101X; m.voitsekhovska@stu.cn.ua. Scopus Author ID: 57192818403
Дорош Марія Сергіївна [1)]
ORCID: https://orcid.org/0000-0001-6537-8957; mariyaya5536@gmail.com. Scopus Author ID: 56912183600
Гречанінов Віктор Федорович [2)]
ORCID: https://orcid.org/0000-0001-6268-3204; vgrechaninov@gmail.com. Scopus Author ID: 57219055091
Вереніч Олена Володимирівна [3)]
ORCID: https://orcid.org/0000-0003-0972-6361; verenych@ukr.net. Scopus Author ID: 57189383746
[1)] Національний університет «Чернігівська політехніка», вул. Шевченка, 95. Чернігів, 14035, Україна
[2)] Інститут проблем математичних машин і систем НАНУ, пр. Акад. Глушкова, 42. Київ, 03187, Україна
[3)] Київський національний університет будівництва та архітектури, пр. Повітрофлотський, 31. Київ, 03037, Україна

АНОТАЦІЯ

Масовий перехід на дистанційну роботу, що ініціював карантин, а потім військові дії на території України, зумовив необхідність протистояти новим викликам забезпеченням захисту інформації на більш високому рівні. До того ж, постійні інформаційні та кібер-атаки створюють сталу небезпеку для фізичних та інформаційних систем. Це, в свою чергу, вимагає чіткого розуміння рівня забезпечення інформаційної безпеки різних організацій, особливо критичної інфраструктури. Важливою компонентою інформаційної безпеки організації є культура інформаційної безпеки всіх учасників внутрішніх інформаційних процесів, вплив якої прийнято називати людський фактор. Мета роботи розкривається у двох цілях. Першою метою є функціональне моделювання інформаційних процесів автоматизації оцінки рівня культури інформаційної безпеки

як частини загальної системи безпеки організації. Друга частина полягає в розробці моделі зрілості системи інформаційної безпеки проекту (ISSoP), щоб забезпечити життєво важливий рівень довіри до організації в рамках проектної діяльності. Функціональна модель розробки системи представлена у вигляді окремих процесів: формування опитувальників, збору даних, проведення оцінки культури інформаційної безпеки на персональну, груповому (підрозділ) та організаційному рівнях. Визначені вхідні та вихідні дані, механізми, моделі, методи та елементи управління для кожного процесу. Дану модель можна долучити як складову системи визначення рівня загальної інформаційної системи безпеки організації. Визначено стадії зрілості культури інформаційної безпеки проекту та процесів підтримки на різних етапах його життєвого циклу, які також потрібно враховувати при розробці таких систем.

Ключові слова: інформаційна безпека; інформаційна система; організація; культура

ABOUT THE AUTHORS

Mariia M. Voitsekhovska - PhD in Computer Sciences, Information Technology and Software Engineering Department. Chernihiv Polytechnic National University, 95, Shevchenko Str. Chernihiv, 14035, Ukraine
ORCID: https://orcid.org/0000-0002-1711-101X; m.voitsekhovska@stu.cn.ua. Scopus Author ID: 57192818403
***Research field*:** Fuzzy logic; human-computer interaction; human factor in information security systems of organizations and projects; information security

Войцеховська Марія Михайлівна - доктор філософії (Комп'ютерні науки), кафедра Інформаційних технологій та програмної інженерії. Національний університет «Чернігівська політехніка», вул. Шевченка, 95. Чернігів, 14035, Україна

Mariia S. Dorosh - Doctor of Engineering Sciences, Professor of Information Technology and Software Engineering Department. Chernihiv Polytechnic National University, 95, Shevchenko Str. Chernihiv, 14035, Ukraine
ORCID: https://orcid.org/0000-0001-6537-8957; mariyaya5536@gmail.com. Scopus Author ID: 56912183600
***Research field*:** Modeling and design of intelligent systems; knowledge management; convergence of project management systems; Human factor in information security systems of organizations and projects.

Дорош Марія Сергіївна - доктор технічних наук, професор кафедри Інформаційних технологій та програмної інженерії. Національний університет «Чернігівська політехніка», вул. Шевченка, 95, Чернігів, 14035, Україна

Viktor F. Grechaninov - PhD in Engineering Sciences, Head of Intelligent Information and Analytical Systems Department. Institute of Mathematical Machines and Systems Problems of the NASU, 42 Acad. Glushkov Ave. Kyiv, 03187, Ukraine
ORCID: https://orcid.org/0000-0001-6268-3204; vgrechaninov@gmail.com. Scopus Author ID: 57219055091
Research field: Intelligent information and analytical systems

Гречанінов Віктор Федорович - канд. техніч. наук, завідувач відділу Інтелектуальних інформаційно-аналітичних систем. Інститут проблем математичних машин і систем НАНУ, пр. Акад. Глушкова, 42. Київ, 03187, Україна

Olena V. Verenych - Doctor of Engineering Sciences, educator and researcher of Project Management Department. Kyiv National University of Construction and Architecture, 31, Povitroflotsky Ave. Kyiv, 03037, Ukraine
ORCID: https://orcid.org/0000-0003-0972-6361; verenych@ukr.net. Scopus Author ID: 57189383746
Research field: eLearning; communication mental space, and interaction in project management

Вереніч Олена Володимирівна - доктор технічних наук, викладач та науковий співробітник кафедри Управління проектами. Київський національний університет будівництва та архітектури, пр. Повітрофлотський, 31. Київ, 03037, Україна