http://doi.org/10.35784/iapgos.3033

received: 19.06.2022 | revised: 03.09.2022 | accepted: 15.09.2022 | available online: 30.09.2022

SIMULATION OF INFORMATION SECURITY RISKS OF AVAILABILITY OF PROJECT DOCUMENTS BASED ON FUZZY LOGIC

Oleksii M. Shushura[1], Liudmyla A. Asieieva[2], Oleksiy L. Nedashkivskiy[1], Yevhen V. Havrylko[1], Yevheniia O. Moroz[3], Saule S. Smailova[4], Magzhan Sarsembayev[5]

[1]National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Department of Design Automation for Energy Processes and Systems, Kyiv, Ukraine, [2]State University of Telecommunications, Kyiv, Ukraine, [3]Taras Shevchenko National University of Kyiv, Kyiv, Ukraine, [4]D.Serikbayev East Kazakhstan State Technical University, Ust-Kamenogorsk, Kazakhstan, [5]Al-Farabi Kazakh National University, Almaty, Kazakhstan

Abstract. *The widespread use of computer technology, its rapid development and use in almost all areas of human activity requires constant updating of information security issues. The activities of many enterprises in the field of IT, construction, and other areas are of a project nature and therefore further research on information security management of projects is relevant. Appearance of changes and the current state of the project results at certain points of time describe the documents that accompany it. In this paper, the information structure of the project is considered as a set of specific documents. During the life cycle of each project document, which includes the creation, transfer, preservation and transformation, there are generally threats to its confidentiality, integrity, accessibility and authenticity. This paper develops a method for assessing the risks of violation of the availability of project documents in solving information security problems. A formal description of many project documents in the form of a generalized hierarchical structure is presented, the connection of documents with the operations performed on them and information systems used during these operations is formalized. Given the incompleteness and dimension of the data, the based on fuzzy logic model was developed to assess the risk of document accessibility. Approaches to the assessment of the damage from the violation of the availability of the project document and the method of calculating the overall assessment of the risk of violation of the documents availability are proposed. The results presented in this paper can be used in decision-making processes regarding information security of projects in organizations that have project activities. The approaches proposed in this paper can serve as a basis for the creation of specialized information technologies to automate the calculation of project risk assessments.*

Keywords: information security of the project, cybersecurity risk assessment, fuzzy logic, risk of accessibility breach

SYMULACJA ZAGROŻEŃ BEZPIECZEŃSTWA INFORMACJI W ZAKRESIE DOSTĘPNOŚCI DOKUMENTÓW PROJEKTOWYCH W OPARCIU O LOGIKĘ ROZMYTĄ

Streszczenie. *Powszechne stosowanie techniki komputerowej, jej szybki rozwój i wykorzystanie niemal we wszystkich dziedzinach działalności człowieka wymaga ciągłej aktualizacji zagadnień związanych z bezpieczeństwem informacji. Działalność wielu przedsiębiorstw w zakresie informatyki, budownictwa i innych dziedzin ma charakter projektowy, dlatego istotne są dalsze badania nad zarządzaniem bezpieczeństwem informacji w projektach. Pojawienie się zmian i aktualny stan wyników projektu w określonych momentach czasu opisują towarzyszące mu dokumenty. W niniejszej pracy struktura informacyjna projektu jest rozpatrywana jako zbiór określonych dokumentów. W cyklu życia każdego dokumentu projektu, który obejmuje tworzenie, przekazywanie, przechowywanie i przekształcanie, występują na ogół zagrożenia dla jego poufności, integralności, dostępności i autentyczności. W pracy opracowano metodę oceny ryzyka naruszenia dostępności dokumentów projektowych w rozwiązywaniu problemów bezpieczeństwa informacji. Przedstawiono formalny opis wielu dokumentów projektowych w postaci uogólnionej struktury hierarchicznej, sformalizowano związek dokumentów z wykonywanymi na nich operacjami oraz systemami informatycznymi wykorzystywanymi podczas tych operacji. Biorąc pod uwagę niekompletność i wymiar danych, opracowano oparty na logice rozmytej model oceny ryzyka dostępności dokumentów. Zaproponowano podejście do oceny szkody z tytułu naruszenia dostępności dokumentu projektu oraz metodę obliczania ogólnej oceny ryzyka naruszenia dostępności dokumentów. Wyniki przedstawione w pracy mogą być wykorzystane w procesach decyzyjnych dotyczących bezpieczeństwa informacyjnego projektów w organizacjach prowadzących działalność projektową. Zaproponowane w pracy podejścia mogą stanowić podstawę do tworzenia specjalistycznych technologii informatycznych automatyzujących obliczanie oceny ryzyka projektu.*

Słowa kluczowe: bezpieczeństwo informacji projektu, ocena ryzyka cyberbezpieczeństwa, logika rozmyta, ryzyko naruszenia dostępności

Introduction

The widespread use of computer technology, its rapid development and use in almost all areas of human activity requires constant updating of information security issues. The use of information technology vulnerabilities by both cybercriminals and certain organizations and states makes it necessary to systematically apply cybersecurity methods and tools both at the national level and at individual enterprises. This is especially important for critical infrastructure companies and their business partners, including construction companies. The introduction of info-communication technologies in the construction industry has raised the question of improving existing and developing new means of cybersecurity to take into account its specifics [1, 7, 9, 21]. The issue of cybersecurity of information systems should be considered not only from the angle of protection of classified or important data, but also in terms of ensuring the functional stability of these systems [6].

Decisions regarding the management of information security of the enterprise should be based on the assessment of its risks, which requires sufficiently accurate quantitative methods and tools. However, in the current environment of increasing risks and costs in the field of information security, the measurement of cybersecurity still remains an underdeveloped topic that requires further research [11].

In the field of information technology for modeling uncertainty, the methods and means of fuzzy logic proposed by L. Zadeh [24] have become widespread. The use of this mathematical apparatus allows in many cases to obtain better results than other approaches, for example, in determining the state of a computer system [8]. The characteristics of information security components often contain incomplete and blur ed information, so fuzzy logic has been widely used in risk assessment models. In particular, fuzzy logic is involved in the system administrator warning system in cybersecurity management of critical infrastructure enterprises [4], in the risk mitigation model based on its effective assessment and human behavioral intervention [3], for generalized risk assessment based on vulnerability, threat, probability and impact [2], when modeling information security risks of enterprise management systems [15]. It is known that the most secure information networks are optical networks, and especially the passive optical networks (PON), the study and modeling of which is devoted many works [16–18]. And even their effective use does not completely solve the problem of information security. However, it should be noted that the activities of many enterprises are project-based and therefore information security management should also be implemented within each project, which requires further research in this area.

In a general sense, a project is seen as a set of operations to achieve goals with limited time and resources. Appearance of changes and the current state of the project results at certain points in time describe the documents that accompany it. For example, for a construction company, the document accompanying the project is the main information asset of the project. Consider the information structure of the project as a set of specific documents. During the life cycle of each project document, which includes the creation, transfer, preservation and transformation, there are threats to its confidentiality, integrity, accessibility and authenticity.

1. Formulation of the problem

The purpose of this work is to develop a model for assessing the risks of information security violations of the availability of project documents based on fuzzy logic. To achieve this goal in this paper formalized the information structure of the project as a set of certain documents, identified input and output linguistic variables, proposed a generalized structure of submodels for calculations.

2. Theoretical research

To formalize the information structure of the project, we denote in the general case the document as $d^i_{lk} \in D$, where D – is the set of project documents; i – document number; l – document form, $l \in \{0, 1, 2, 3\}$: 0 – electronic copy, 1 – signed paper original, 2 – paper copy, 3 – electronic document with electronic-digital signature; k – the number of document copy.

All replicas of the i-th document of l document form will be denoted as d^i_l, and determined by the formula:

$$d^i_l = \bigcup_k d^i_{lk} \tag{1}$$

All replicas of the i-th document of all document form will be denoted as (generalized document), and determined by the formula:

$$d^i = \bigcup_l d^i_l \tag{2}$$

The set of documents D of the project will be divided into their types:

$$D = \bigcup_{m=1}^{n} D_m,\ D_j \bigcap D_m = \varnothing,\ j \neq m \tag{3}$$

where D_m – type of document.

During the life cycle of a document, many different operations can be performed with it, including creation, editing, approval, use, disposal, archiving, and so on. Denote the set of operations on the document d^i as P_i. Each operation $p_{ij} \in P_i$ involves the use of certain software and hardware, the work of certain personnel with different levels of access, and so on. Denote as ISP_{ij} the set of information systems used during the operation $p_{ij} \in P_i$ on the document.

An employee of the enterprise and an employee of the contractor or customer (owner) may be involved in the operation $p_{ij} \in P_i$. The set of operations P_i on the document d^i can be represented in the form of a network graph showing the technological scheme of document processing. Thus different copies of documents in various forms $d^i_{lk} \in D$ can be created, that is to each operation $p_{ij} \in P_i$ in the general case some set of copies of documents is matched.

Violation of the accessibility of the document will be considered the creation of such conditions or the implementation of actions that make it impossible or difficult to access it. Access is blocked or, if possible, for a time that will not ensure the achievement of certain goals or business processes. The threat to the availability of a document is understood as its blocking or destruction, which is associated with user actions, internal failures of the information system, failures of the infrastructure that supports the information system. For example, inability to work with the required document due to lack of appropriate training (lack of general computer education, inability to interpret incoming or outgoing messages, ignorance of the necessary techniques, inability to work with documentation).

The level of risk of violation of the availability RAv^i of the document will defined as:

$$RAv^i = PAv^i \cdot UAv^i \tag{4}$$

where PAv^i – assessment of the possibility of endangering the availability of the document d^i; UAv^i – assessment of damage from the threat of violation of the availability of the document d^i.

The calculation of the assessment of the possibility of endangering the availability of the document d^i is carried out as:

$$PAv^i = \min_{l,k}\{\max_{p_{ij} \in P_i^{lk}} PAv^i_j\} \tag{5}$$

where PAv^i_j – the possibility of the threat of violation of the availability of the document d^i during the operation, where P_i^{lk} – the set of operations in which the document $d^i_{lk} \in D$ is used in l-form and k-replica.

We apply a linguistic approach to the description of risk factors of information security of the project. This will ensure the creation of quantitative estimates for the elements of the model in terms of unclear information about the importance of the level of risk, damage from the threat, the possibility of certain threats, levels of vulnerability to vulnerabilities [15].

To calculate the possibility PAv^i_j of violation of the availability of the document d^i during the operation $p_{ij} \in P_i^{lk}$, a fuzzy model is proposed, the generalized structure of which is shown in figure 1.

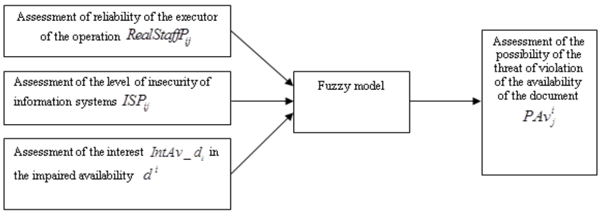

Assessment of reliability of the executor of the operation $RealStaffP_{ij}$
Assessment of the level of insecurity of information systems ISP_{ij}
Assessment of the interest $IntAv\_d_i$ in the impaired availability d^i
Fuzzy model
Assessment of the possibility of the threat of violation of the availability of the document PAv^i_j

Fig. 1. Fuzzy model for assessing the possibility of endangering the availability of the document

As can be seen in figure 1, in the fuzzy model, the inputs are linguistic variables:

- the level of reliability of the executor of the operation $RealStaffP_{ij}$;
- assessment of the level of insecurity of information systems ISP_{ij};
- assessment of the interest $IntAv\_d_i$ of third-party actors in the impaired availability of the document d^i.

For simplicity, we assume that there is only one executor in the operation $p_{ij} \in P_i$. This can be easily achieved, given this assumption when forming a set of operations on the document. An appropriate model based on fuzzy logic can be used to assess the level of reliability of the executor. In this case, a hierarchical fuzzy inference should be used to perform the calculations.

To assess the reliability $RealStaffP_{ij}$ of the executor of the operation $p_{ij} \in P_i$, a fuzzy model is proposed, the structure of which is shown in figure 2.

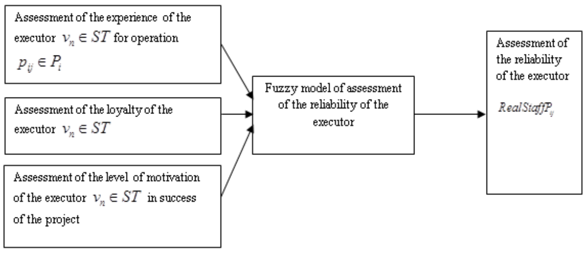

Assessment of the experience of the executor $v_n \in ST$ for operation $p_{ij} \in P_i$
Assessment of the loyalty of the executor $v_n \in ST$
Assessment of the level of motivation of the executor $v_n \in ST$ in success of the project
Fuzzy model of assessment of the reliability of the executor
Assessment of the reliability of the executor
$RealStaffP_{ij}$

Fig. 2. Fuzzy model for assessing the reliability of the executor

In the fuzzy model of estimating the reliability of the executor, the following linguistic variables with the corresponding characteristics are included:

- experience of the executor $ExpStaffP$;
- assessment of the loyalty of the executor $SatStaffP$;
- level of motivation of the executor in success of the project $MotStaffP$.

The description of the above linguistic variables is shown in tables 1–3 in accordance with the methodology of infographic modeling of fuzzy control problems [19].

Table1. Characteristics of the linguistic variable of the executor's work experience CatStaffP

Experience of the executor *ExpStaffP* .	
Type	Input
Block of variables	
Experience	The set of valid values {0...55 years}
Block of terms	
Experience unavailable	Linear z-shaped membership function $\mu(x, 0.5, 1)$
Beginner	Triangular membership function $\mu(x, 0.5, 2, 3)$
Experienced	Linear s-shaped membership function $\mu(x, 1.5, 3)$
Description of the procedure for forming new terms - not specified	
Description of the procedure for forming the membership functions of terms - not specified	

Table 2. Characteristics of the linguistic variable of the executor's work experience CatStaffP

Loyalty of the executor *SatStaffP*	
Type	Input
Block of variables	
Loyalty level	The set of valid values {0…10}
Block of terms	
Disloyal	Linear z-shaped membership function $\mu(x, 0.5, 1)$
Neutral	Triangular membership function $\mu(x, 0.5, 2, 3)$
Loyal	Linear s-shaped membership function $\mu(x, 2, 3)$
Description of the procedure for forming new terms - not specified	
Description of the procedure for forming the membership functions of terms - not specified	

Table 3. Characteristics of the linguistic variable loyalty of the executor MotStaffP

Level of motivation of the executor in the success of the project *MotStaffP*	
Type	Input
Block of variables	
Level of motivation	The set of valid values {0…10}
Block of terms	
Low	Linear z-shaped membership function $\mu(x, 0.5, 2)$
Neutral	Triangular membership function $\mu(x, 0.5, 2, 3)$
High	Linear s-shaped membership function $\mu(x, 2, 3)$
Description of the procedure for forming new terms - not specified	
Description of the procedure for forming the membership functions of terms - not specified	

The description of the initial linguistic variable reliability of the executor *StaffP* is shown in table 4.

Table 4. Characteristics of linguistic variable reliability of the executor StaffP

Reliability of the executor *StaffP*	
Type	Input
Block of variables	
Level of reliability of the executor	The set of valid values {0…10}
Block of terms	
Unreliable	Linear z-shaped membership function $\mu(x, 2, 5)$
Questionable	Triangular membership function $\mu(x, 2, 5, 8)$
Reliable	Linear s-shaped membership function $\mu(x, 5, 8)$
Description of the procedure for forming new terms of the use of quantifiers is very reliable, more or less reliable, very unreliable, unquestionable	
Description of the procedure for forming the membership functions of terms - very reliable $(\mu(x, 5, 8))^2$; more or less reliable $\sqrt{\mu(x, 5, 8))}$; very unreliable $(\mu(x, 2, 5))^2$; unquestionable $1 - \mu(x, 2, 5)$	

To assess the level of insecurity of information systems, it is proposed to use the CVSS standard [10] and calculate the vulnerability of information systems of the operation. Based on this indicator, a linguistic variable is proposed, the description of which in accordance with the methodology of infographic modeling [19] is given in table 5.

Table 5. Description of the linguistic variable of the level of insecurity of information systems

Level of insecurity of information systems *LevelISP* using CVSS vulnerability estimates	
Type	Input
Block of variables	
Level of insecurity using CVSS	The set of valid values {1…10}
Block of terms	
None	Linear z-shaped membership function $\mu(x, 0, 0.1)$
Low	Triangular membership function $\mu(x, 0.1, 3.9, 4)$
Medium	Trapezoidal membership function $\mu(x, 3.9, 4.0, 6.9, 7)$
High	Trapezoidal membership function $\mu(x, 6.9, 7.0, 8.9, 9)$
Critical	Triangular membership function $\mu(x, 8.9, 9, 10)$
Description of the procedure for forming new terms - not specified	
Description of the procedure for forming the membership functions of terms - not specified	

To form the membership functions of the terms of the linguistic variable, the processing of expert estimates based on the method of analysis of Saaty hierarchies was used [5, 20].

In order to assess the level of interest in impaired accessibility of the document, it is proposed to use the method of hierarchy analysis, based on expert assessments according to the three-level hierarchy of threat actors and types of documents shown in figure 8. In other cases, when this assumption cannot be applied, this assessment is established by an expert [12–14].

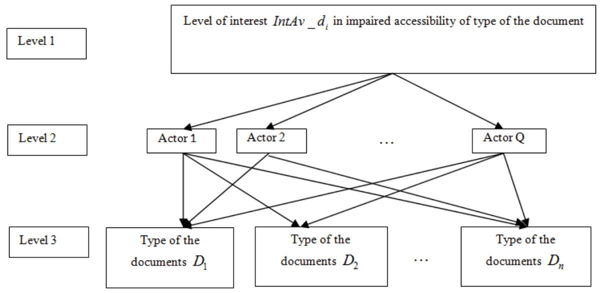
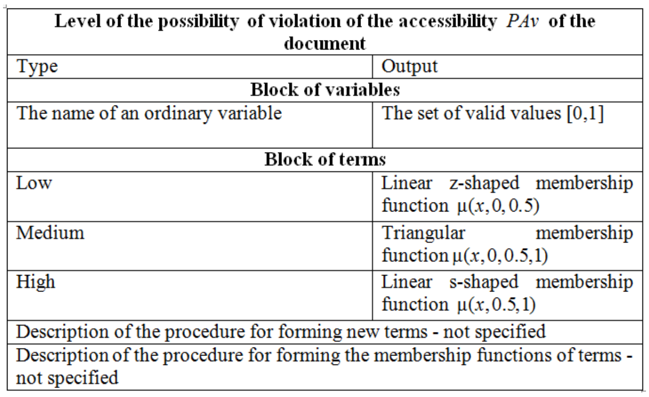

Level 1
Level of interest $IntAv\_d_i$ in impaired accessibility of type of the document
Level 2
Actor 1
Actor 2
…
Actor Q
Level 3
Type of the documents D_1
Type of the documents D_2
…
Type of the documents D_n

Fig. 8. Tree of criteria for assessing the level of interest in violating the availability of the document

The description of the linguistic variable of the possibility of violation of the accessibility of the document is shown in table 6.

Table 6. Description of the linguistic variable possibility of violation of document accessibility



Level of the possibility of violation of the accessibility PAv of the document	
Type	Output
Block of variables	
The name of an ordinary variable	The set of valid values [0,1]
Block of terms	
Low	Linear z-shaped membership function $\mu(x,0,0.5)$
Medium	Triangular membership function $\mu(x,0,0.5,1)$
High	Linear s-shaped membership function $\mu(x,0.5,1)$
Description of the procedure for forming new terms - not specified	
Description of the procedure for forming the membership functions of terms - not specified	

On the basis of the offered linguistic variables and their terms the fuzzy production rules for performance of calculations on models are constructed [23, 24].

In a simplified form, the set of rules for fuzzy products is as follows:

$$\text{Rule } R\text{: <IF>} \bigcap_{i=1}^{N} A_i \text{ <THEN>} \bigcap_{j=1}^{M} C_j$$

where N – the number of subconditions included in the rule R; M – the number of subconclusions included in the rule R; A_i – is a subcondition that is part of the R rule and is a fuzzy statement consisting of an input linguistic variable and a corresponding term; C_j – is a subconclusion that is part of the rule R and is a fuzzy statement consisting of the original linguistic variable and the corresponding term.

Using one of the algorithms of fuzzy inference, for example, the Mamdani method, based on the rules of the fuzzy model to assess the possibility of violation of the availability of the document calculates the possibility PAv^i of violation of the availability of the document d^i during the operation $p_{ij} \in P_i^{lk}$. Next, using formula (5), a general assessment PAv^i of the possibility of a threat of violation of the availability of the document d^i is calculated.

To calculate the quantitative assessment of the risk of violation of the availability of the document in accordance with formula (4), it is necessary to calculate the assessment UAv^i of the damage from the threat of violation of the availability of the document d^i.

The calculation of the damage assessment UAv^i from the threat of violation of the availability of the document d^i requires the creation of a set of partial indicators that form the damage or loss. A generalized list of these partial indicators is presented in table 1. The indicators are divided into three groups: external loss or damage to the enterprise, internal loss or damage to the enterprise, financial losses of the enterprise. It is proposed to calculate the value of UAv^i by using the method of hierarchy analysis, the tree of criteria which consists of the levels of partial indicators of damage, types of project documents and documents distributed by type. Damage from accessibility is assessed in monetary terms or in points that can be used to make decisions about information security.

Table 7. List of partial damage/loss indicators

No	Title of the indicator	Group of indicators
1	Damage to the authority of the organization	External damage/loss
2	Damage to the authority of the state in the international arena	
3	Legal costs	
4	Negative reaction at the government level	
5	Publication of negative materials in the press	
6	The possibility of committing terrorist acts	
7	The possibility of man-made disasters	
8	Dismissal of specialists of the organization	Internal damage/loss
9	Reducing the level of information security	
10	Loss or destruction of the organization's assets	
11	Influence on the decisions made by the staff of the organization in business processes	
12	The need to verify and restore the integrity of the asset	
13	Deterioration of the emotional climate in the team	
14	Disorganization of activities	
15	The need for manual work	
16	Reducing the competitiveness of the organization	Financial loss
17	Loss of benefits when concluding contracts	
18	Decrease in liquidity and share price	
19	Inability of the organization to fulfill its obligations to customers and suppliers	
20	The need for additional research	
21	Ability to steal assets and conduct unaccounted transactions	
22	Decrease in prices for products, sales	
23	Loss of patenting, sale of licenses	
24	Anticipation of competitors bringing similar products to market	
25	Abandonment of strategic decisions that have become ineffective	
26	Deterioration of credit conditions	
27	Falling profitability	
28	Reducing the level of cooperation with business partners	
29	Mass theft, fraud	

3. Conclusions

1) The paper develops a method for assessing the risks of violation of the availability of project documents in solving information security problems. A formal description of many project documents in the form of a generalized hierarchical structure is presented, the connection of documents with the operations performed on them and information systems used during these operations is formalized. Given the incompleteness and dimension of the data, based on fuzzy logic, a model was developed to assess the risk of document accessibility. Approaches to the assessment of the damage from the violation of the availability of the project document and the method of calculating the overall assessment of the risk of violation of the availability of documents are proposed.
2) These results can be used in decision-making processes regarding information security of projects in organizations that have project activities, including IT companies, construction companies, critical infrastructure companies and others. The approaches proposed in this paper can serve as a basis for the creation of specialized information technologies to automate the calculation of project risk assessments.

References

[1] Abid H. et al.: Structuration Model of Construction Management Professionals, Use of Mobile Devices. Journal of Management in Engineering 37(4), 2021 [http://doi.org/10.1061/(ASCE)ME.1943-5479.0000930].

[2] Al-Ali M. et al.: Improving risk assessment model of cyber security using fuzzy logic inference system. Computers & Security 74, 2018, 323–339 [http://doi.org/doi:10.1016/j.cose.2017.09.011].

[3] Al-Ali M., Al Mogren A.: Fuzzy logic methodology for cyber security risk mitigation approach. Journal of Networking Technology 8(3), 2017.

[4] Alam J. et al.: Advance Cyber Security System using fuzzy logic. Journal of Management & IT ACME 10, 2014, 17–29.

[5] Azarova A.: Information Technologies and Neural Network Means for Building the Complex Goal Program Improving the Management of Intellectual Capital. Lecture Notes on Data Engineering and Communications Technologies 77, 2022, 534–547.

[6] Barabash O. et al.: Application of Petri Networks for Support of Functional Stability of Information Systems. IEEE First International Conference on System Analysis & Intelligent Computing (SAIC), Kyiv 2018, 36–39.

[7] Bharadwaj R. K., de Sotob B. G.: Cyber security challenges and vulnerability assessment in the construction industry. Conference Creative Construction, Budapest 2019, 30–37 [http://doi.org/10.3311/CCC2019-005].

[8] Gavrylenko S. et al.: Development of a method for identifying the state of a computer system using fuzzy cluster analysis. Advanced Information Systems 4(2), 2020, 8–11 [http://doi.org/10.20998/2522-9052.2020.2.02].

[9] https://www.construction-institute.org/events/education/free-webinar-cybersecurity-for-construction (available 09.02.2022).

[10] https://www.first.org/cvss/v3.1/user-guide (available 16.02.2022).

[11] https://www.nist.gov/cybersecurity/measurements-information-security (available 09.02.2022).

[12] Kvyetnyy R. et al.: Blur recognition using second fundamental form of image surface. Proc. SPIE 9816, 2015, 98161A.

[13] Kvyetnyy R. et al.: Method of image texture segmentation using Laws' energy measures. Proc. SPIE 10445, 2017, 1044561.

[14] Kvyetnyy R. et al.: Modification of fractal coding algorithm by a combination of modern technologies and parallel computations. Proc. SPIE 9816, 2015, 98161R.

[15] Mishchenko A. V. et al.: A vague model for assessing the security of information security and the level of security of ERP systems. Telecommunications and Information Technologies 66, 2020, 142–151 [http://doi.org/10.31673/2412-4338.2020.011451].

[16] Nedashkivskiy O. et al.: Mathematical support for automated design systems for passive optical networks based on the β-parametric approximation formula. International Journal of Advanced Trends in Computer Science and Engineering 9(5), 2020, 8207–8212 [http://doi.org/10.30534/ijatcse/2020/186952020].

[17] Nedashkivskiy O.: Precise method of balancing passive optical networks with irregular splitter with two or more outputs. 2nd International Conference on Advanced Information and Communication Technologies (AICT), 2017, 228–231 [http://doi.org/10.1109/AIACT.2017.8020107].

[18] Nedashkivskyy O. L. et al.: Methods of creating passive optical networks with the distributing bus topology. Control, Navigation and Communication Systems 2(42), 2017, 206–217.

[19] Shushura O. M.: Infological modeling of information systems subject industries in solving of fuzzy control tasks. Link 2, 2018, 53–56.

[20] Shyian A. A. et al.: Modeling communication between the public and the authorities while implementing innovative projects in the context of e-democracy and public administration. Science and Innovation 16(6), 2021, 18–27.

[21] Sonkor M., de Sotob B. G.: Operational Technology on Construction Sites: A Review from the Cybersecurity Perspective. Journal of Construction Engineering and Management 147(12), 2021 [http://doi.org/10.1061/(ASCE)CO.1943-7862.0002193].

[22] Trishch R. et al.: Methodology for multi-criteria assessment of working conditions as an object of qualimetry. Engineering Management in Production and Services 13(2), 2021, 107–1141.

[23] Trishch R. et al.: Qualimetric method of assessing risks of low quality products. MM Science Journal 2021, 4769–4774.

[24] Zadeh L.A.: Fuzzy sets. Information and Control 8, 1965, 338–353.

D.Sc. Oleksii M. Shushura
e-mail: leshu@i.ua

Doctor of Technical Sciences, Associate Professor, Professor of the Department of Automation of Designing of Energy Processes and Systems, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine. Author of over 101 publications, including 1 monographs, 4 textbooks, more than 47 scientific articles in professional journals, of which 1 are in the scientometric databases Scopus and Web of Science.

http://orcid.org/0000-0003-3200-720X

M.Sc. Liudmyla A. Asieieva
e-mail: aseewal@i.ua

Postgraduate student, State University of Telecommunications, Kyiv, Ukraine. Author of 4 publications in professional journals.

http://orcid.org/0000-0001-5954-4211

D.Sc. Oleksiy L. Nedashkivskiy
e-mail: al_1@ua.fm

Doctor of Technical Sciences, Associate Professor, Professor of the Department of Automation of Designing of Energy Processes and Systems, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine. Author of more than 40 publications, including 1 monographs, 5 textbooks, more than 25 scientific articles in professional journals, of which 4 are in scientometric databases Scopus and Web of Science.

http://orcid.org/0000-0002-1788-4434

D.Sc. Yevhen V. Havrylko
e-mail: gev.1964@ukr.net

Doctor of Engineering Sciences, Professor, Department of design automation for energy processes and systems National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine. Author of more than 33 publications, including 2 textbooks, 3 patents for inventions and more than 20 scientific articles in professional journals, of which 5 are in scientometric databases Scopus and Web of Science.

http://orcid.org/0000-0001-9437-3964

Ph.D. Yevheniia O. Moroz
e-mail: morozeo@knu.ua

Associate professor, Ph.D. Department of Theory and History of Sociology, Taras Shevchenko National University of Kyiv. Scientific interests: history of sociology, modern sociological theories, theories of cultural capital, post-structuralist approach, urban studies, data analysis.

http://orcid.org/0000-0002-2618-3541

Ph.D. Saule Smailova
e-mail: Saule_Smailova@mail.ru

Saule Smailova is currently a lecturer at the Department of Information Technology. She is a co-author over 60 papers in journals, book chapters, and conference proceedings. Member of Expert Group in the Computer Science specialization of IQAA. Her professional interests are teaching, artificial intelligence, software engineering, data processing.

http://orcid.org/0000-0002-8411-3584

Ph.D. Magzhan Sarsembayev
e-mail: magatrone@mail.ru

Senior lecturer of the Department of Computer Science of Al-Farabi Kazakh National University. Author of more than 10 scientific works published in leading journals of Kazakhstan Republic and the far abroad. Research area: High performance computing, intelligent systems of control, software engineering, 3d modeling and design.

http://orcid.org/0000-0003-2139-2456