UDC 004.056
DOI: 10.25140/2411-5363-2020-1(19)-124-132

Vitalii Lytvynov, Mariia Dorosh, Iryna Bilous, Mariia Voitsekhovska, Valentyn Nekhai

DEVELOPMENT OF THE AUTOMATED INFORMATION SYSTEM FOR ORGANIZATION'S INFORMATION SECURITY CULTURE LEVEL ASSESSMENT

Relevance of the research. *Ensuring the effectiveness of the information security systems requires creation of an appropriate information security culture for the employees of the organization in order to reduce human-related risks.*

Target setting. *The techniques currently available for assessing information security risk are excluded as a source of the potential vulnerability. Considering the role of the personnel in the organization's information security systems, there is a need to create automated systems of human-machine interaction assessment through the level of the personnel information security culture, and to determine the integral indicator of the organization's information security culture.*

Actual scientific researches and issues analysis. *Open access publications on the problems of integrating the information security culture into the corporate culture of the organization as a tool for ensuring the proper information security level of business processes are considered.*

Uninvestigated parts of general matters defining. *The absence of formalized models for assessing the organization's information security culture level, as well as an automated process for its assessing were revealed by source analysis.*

The research objective. *The purpose of the article to build a model that describes the process of obtaining an organization's information security culture level assessment in IDEF0 notation. Then, to create an architecture and database for system of information security culture assessment to support the general organization's information security system.*

The statement of basic materials. *According to functional requirements, a conceptual model of «The organization`s ISC level determination» development process was created. Input information, governing elements, execution elements and mechanism, and output information were defined. To accomplish these tasks, an architecture and database of information system for assessing the information security culture level of the organization were proposed.*

Conclusions. *The functional model of top-level development process was proposed. Formed functional requirements became the basis for development of information system architecture with description of its modules and database structure.*

Keywords: *culture; information security; organization; personal culture; information system; architecture; database.*
Fig.: 3. References: 19.

Relevance of the research. One of the key problems in development and implementation of information security systems (ISS) is to ensure its effectiveness by reinforcing the knowledge and skills of employees in field of information security. However, integrated information security tools can`t still guarantee the security of the organization's information resources. This situation is commonplace because most of information gathering, processing and storage processes are provided by the employees who are active participants in the internal information environment.

In order to counteract external and internal threats effectively, there is a need to develop new approaches to implement an information security culture (ISC) as a basis for creating a secure information environment for the organization.

This paper is devoted to development of the organization's ISC level assessment system based on determination of the employees' ISC level, information security risk analysis, and industry requirements.

Target setting. Now, the organization's ISC level definition exists in the form of recommendations or organization's IS policies. Existing techniques for information security risk assessment are almost exclude a person as a source of potential vulnerability (the exception is the OCTAVE technique [1], which takes into account employee awareness). Therefore, an ISC assessment software should be created to support existing ISS.

Actual scientific researches and issues analysis. Ensuring the safety of activities through the development of a high-level security culture is currently at the heart of organizing activities in one of the most dangerous industries as nuclear energy is [2].

Adele Da Veiga & Jan H. P. Eloff [3] underline the importance of employees ISC in the overall organization's ISS through policy BYOD action. Thomas Schlienger and Stephanie Teufel [4], Johan van Niekerk & Rossouw von Solms [5], Steven Furnell & Kerry-Lynn Thomson [6], point to the need to manage development of the organization's ISC, and Waldo Rocha Flores, Egil Antonsen & Mathias Ekstedt [7] paid attention to the national mentality and culture influence

in the context of globalization. To overcome the obstacles might be encountered in the organization's ISC development through the psychological features of employees, Areej Alhogail and Abdulrahman Mirza have proposed the change management models described in [8].

The weakness of researches mentioned above is differentiation in respondents' selection. The main respondents were representatives of the information security departments, single IT department employees and maintenance specialists. This approach excludes another company`s employees despite their interaction with internal information resources.

Uninvestigated parts of general matters defining. The gap in formalized models for assessing the organization's information security culture level was revealed by source analysis. The absence of an automated process for the organization's information security culture level requires the creation of system for the information security culture level assessment to support the organization's information security system.

The research objective. The paper purpose is building a model to describe the process of obtaining an organization's information security culture level assessment in IDEF0 notation. Then, to create an architecture and database (DB) of ISC assessment system to support the general organization's information security system.

The statement of basic materials. The main functional requirements for the information system are:

• collecting, processing, storing information, such as set of questions for questionnaire formation, results of interviewing respondents, expert assessment of the ISC level (on personal, department, and organization tiers);

• formation and output of results: comparative analysis of the current state of the ISC level with the requirements of regulatory documentations, and IS-risk analysis results;

• creating, storing and refining a set of standard recommendations to increase the existing ISC level of organization.

The following development process models are created using AllFusion Process Modeler (formerly known as BPwin) [9]. AllFusion Process Modeler is a CASE tool for modeling, analysis, documentation and optimization of business processes. Through visualization of resources flows, executors, regulations and results, this software product provides a complete model of the process with the necessary detailing.

1 The top-level functional model

The conceptual model of the development process «The organization`s ISC level determination» is presented in the fig. 1.

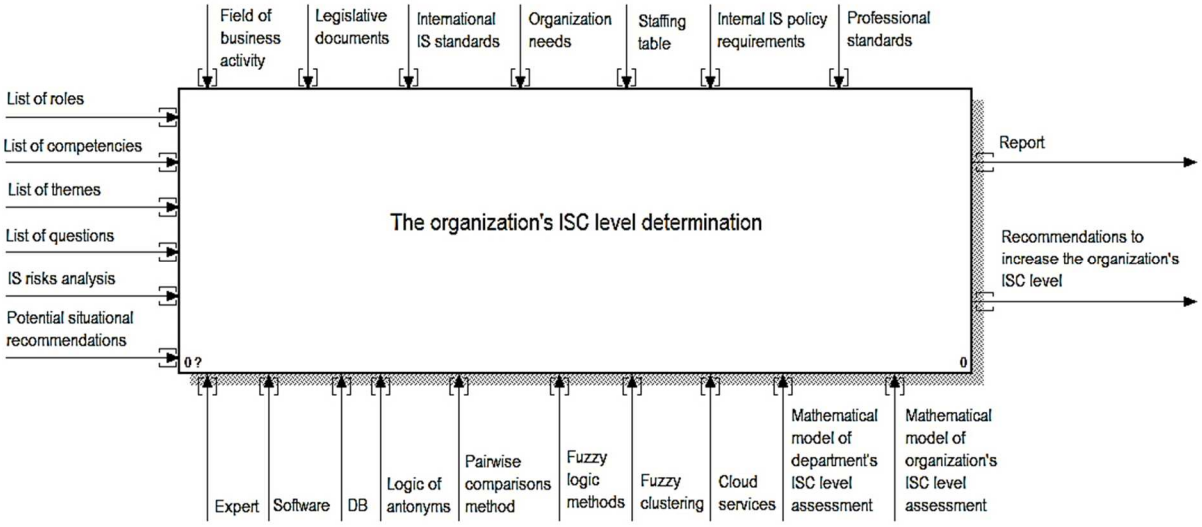

Fig. 1. Functional model of top-level development process «The organization`s ISC level determination»

System inputs are: list of roles, competencies, themes, questions, potential situational recommendations, and organization's IS risks analysis. This information is required to get started. Governing elements of the system are legislative documents and international IS standards (ISO/IEC 27000 group of standards), the organization's scope and needs, internal IS policies, staffing table, job instructions, and professional standards with a set of IS competencies. Execution elements and mechanisms are: experts in the field of information security of organizations (their duties include filling the database with input information, determining weights, forming questionnaires, disseminating and collecting feedback, creating a fuzzy model rule base, checking reports and recommendations); cloud services for questionnaires distribution and of answers collection; software as a tool used for interaction with system by all participants of the process; database for storing information. The main methods are: logic of antonyms [10] (to form the competency array); the method of pairwise comparisons [11] (to determine the weights of questions within the questionnaire); fuzzy logic methods [12] (to assess the personal ISC level for employees) and fuzzy clustering (to generate clusters of questions by theme); general mathematical models of the ISC level assessment for departments and organization [13].

As output, the system should provide the report on the organization's ISC level assessment and recommendations how to improve this level.

1.1. Input information

List of themes identifies aspects related to employees' work activities as users of the internal information environment. The list of themes is formed by experts on the basis of knowledge in this subject area.

List of roles. In the performance of his/her duties, an employee may perform several roles at different levels. For example, responsibilities may be extended with some basic requirements as PC administering in addition with filling some information system with new data. As a source of list of roles may be the organization's staffing table and a set of job instructions.

List of questions. While forming the questionnaires, the expert fills the DB with correctly formed questions and answers that will be offered to the respondents for choice.

List of competencies. The source of competencies list is the professional standard, requirements or organization needs, job instructions, internal organization's IS policies, etc. The list of competences serves to determine the completeness of relevant user`s competences in the internal information environment (employee) according to roles he/she performs within the position.

Potential situational recommendations are a list of recommended actions that are result from the coincidence of adverse assessments according to certain criteria for personal ISC assessing.

IS risks analysis of the organization is the basis for requirements formation to the ISC level of the organization, identifies aspects that need to be strengthened through deepening of knowledge for conducting successful business activities of the organization. The IS risk analysis allows to identify the vulnerable elements of the system (software, processes, participants) and to prepare requirements for personal ISC, departments and organization in general.

1.2. Governing elements of the system

The legislative documents is the legislative base of Ukraine, which consists of a set of legislative, regulatory and normative acts on information security in Ukraine.

The laws of Ukraine "On Information" from 02.10.1992 № 2657-XII [14], «On Protection of Personal Data» from 01.06.2010 № 2297-VI [15], «On basic principles of cyber security in Ukraine» [16], «On Protection of Information in Automated Systems» [17], «On Electronic Documents and Electronic Document Circulation» [18] etc., and regulatory documents, resolutions of Cabinet of Ministers of Ukraine, etc. are based on this.

According to *the industry standard of Ukraine* for the information security management system (ISMS) 2.0/ISO/IEC 27002:2010 «The information technology. Methods of protection. A set of rules for managing information security» [19], requirements for information security is based on three main sources:

• risk assessment for the organization based on the organization's business strategy. The result of IS risk analysis is the list of identified threats and the assessment of vulnerabilities and potential consequences.

• legal requirements under the law, contractual terms with partners and contractors; socio-cultural environment.

• the internal policy of the organization in the field of information security, which regulates the procedures of information processing and production in the internal information environment.

International IS standards of the ISO/IEC 2700X Group (such as ISO/IEC 27001, 27002, 27032, etc.) are used as best practices; they may be served as a source of guidance for improving the situation.

Staffing table is a source for filling a list of jobs and related roles. The staffing table is a must-have document for the organization. The domain of organization's activity determines both the requirements and the themes, which is subsequently used for forming the questionnaires.

Professional standards are the basis for forming a competency array. You should also pay attention to the production needs that accompany the organization. If the conditions of internal information security policy do not allow the execution of certain business processes by outsourcing, such business processes should be provided by qualified and highly specialized specialists in a specific domain, possessing unique competencies.

1.3. Execution elements and mechanisms

An expert is a carrier of deep specific knowledge and practical experience in the field of organization's information security. An expert (or group of experts) is involved in each stage of the organization's ISC level assessment.

The expert`s primary functions are filling the DB tables of the system with primary information (forming requirements for information security; filling the tables of typical situational recommendations (measures) aimed at increasing the level ISC of the employee and the organization; creating a list of questions for questionnaires and their distribution by theme; forming a list of roles (based on staffing table); filling the competency array).

In the second stage, the expert assigns weights that determine the measure of questions belonging to the set of themes, weight of each question (as its influence on the resultant assessment of the survey); establishing the impact of roles on the overall ISC level of the department; assigning competency scales within each role. The expert creates a rule base of the fuzzy model for the assessment of employee's personal level ISC, as well as a set of rules for defining recommendations.

Also, on the final stage, the expert checks the correctness of the received report and a set of recommendations to enhance the ISC level of organization through the introduction of measures to raise awareness and practical experience of employees (increasing personal ISC level).

Software consists of 6 modules, each of them is involved in different stages of an organization's information security audit. They can be briefly described as data collection module, questionnaire generation module, survey conducting module, ISC level assessment of the department and the organization modules, and integrated assessment module. The software architecture is detailed in Paragraph 2.

Database. To implement the ISC assessment system of the organization the single database is used, not a collection of modular databases. It contains information on such basic entities as user information, questionnaires, requirements, and more. The entity diagram is described in details in Paragraph 3.

Logic of antonyms. While filling the information system with the input information, the logic of antonyms is used while forming the competence array from the list of competences. Logic of antonyms allows to specify the type of relationship (strong or weak) between the competencies that qualified professional must have performing a set of roles within the responsibilities of a particular position.

Fuzzy clustering is used in the formation of question clusters by themes according to the membership array for further questionnaires generation.

Fuzzy logic methods. On the basis of linguistic assessments, the respondent's personal ISC level is determined by a fuzzy assessment model. Further defuzzificated survey result is transferred on the input of mathematical model of the department's ISC level assessment.

Pairwise comparisons method is the basis for assigning weights to the impact of each question on the resulting questionnaire assessment. These values are set by the expert on the basis of the created matrix of pairwise comparisons.

Cloud services. The survey is conducted online using questionnaires created and distributed with the support of cloud services (Google Forms, Microsoft Forms, Visual Paradigm Forms, etc.). This approach has the following advantages: free access, does not require specialized development knowledge, provides automated collection of answers in a spreadsheet (Google Sheet, Microsoft Excel, Visual Paradigm Form Results, etc.), and ability to upload to the DB of information system ISC level assessment.

Mathematical model of department's ISC level assessment described in paper [13] determines the ISC level of department based on personal assessments of its employees taking into account the array of role weights corresponding to the positions of respondents.

Mathematical model of organization's ISC level assessment [13] determines the mechanism for determining the overall level of organization's ISC based on results of the ISC level assessments of departments obtained on the previous stage.

1.4. Output information

The organization's ISC level assessment information system has two main functions:

1. An assessment of organization's existing ISC level based on the personal assessment of the organization's employees. The results should be reported;

2. Events of non-compliance detection with the information security requirements. The report should include a set of recommendations for action to increase ISC level employees and organization both.

Output information for the organization's ISC level information system is a report on the organization's ISC level assessment and recommendations for upgrading the organization's ISC level in case the indicators do not meet the requirements of the organization's ISC.

Report is a document generated by the system as a result of activities aimed at determining the ISC level of the organization, relying on ISC level assessments of employees, taking into account the organization's information security requirements, job responsibilities determined with information security competencies.

Recommendations. In case of insufficient level of available ISC, the system provides appropriate recommendations, which should include explanations and guidelines (tips) to eliminate gaps in theoretical and/or practical training and to gain additional experience in order to supplement the users` IS competence. Recommendations may also include links to thematic materials, seminars, webinars, courses, papers, and other educational materials.

2. The information system architecture

The architecture of the information system for determining the ISC level of the organization is shown on fig. 2 and can be used to implement the tasks to information system.

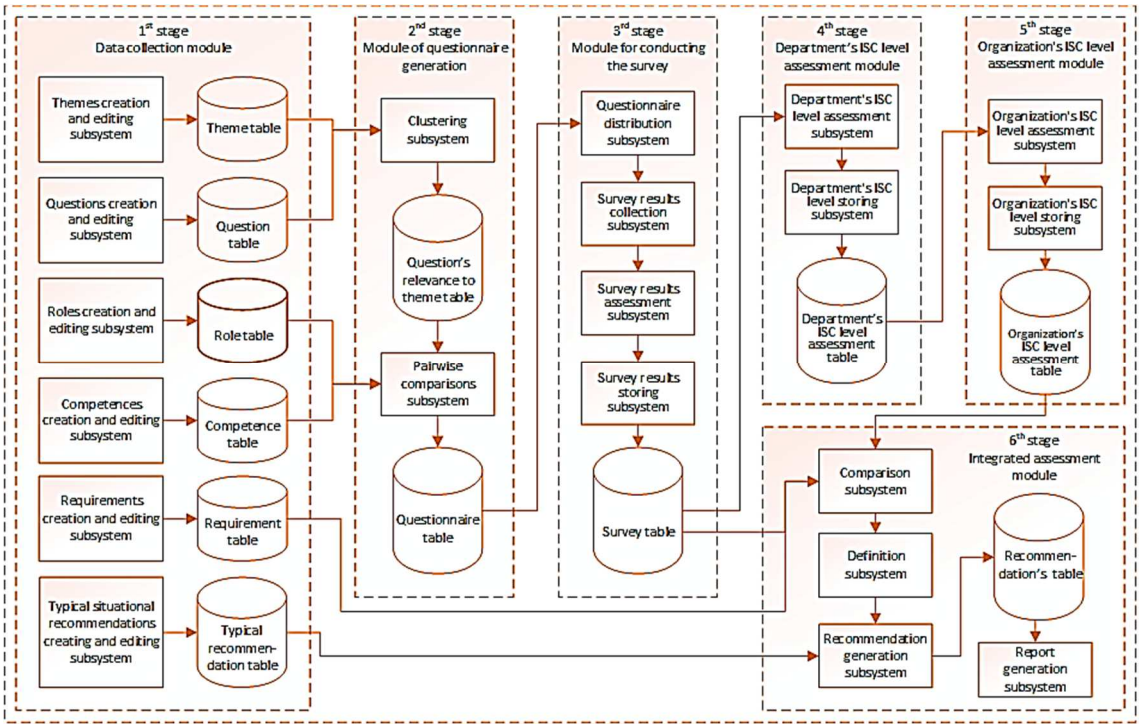

Fig. 2. Information system architecture for determining the ISC level of the organization

The system consists of 6 main modules.

• Data collection module. DB is filled with all the necessary information for further questionnaire generation and assessment by an IS expert (or group of experts).

• Module of questionnaire generation. It distributes questionnaires by theme. The pairwise comparison method is used for estimation of questions` weights in base on the set of competences and roles of the employees for testing.

• Module for conducting the survey. It provides access to employees of the organization to the questionnaire and stores the results of the tests.

• Department's ISC level assessment module. It forms an overall assessment of the ISC level for department on the results of completed questionnaires or passed tests.

• Organization's ISC level assessment module. It forms the overall ISC level of the entire organization based on the assessment of all departments.

• Integrated assessment module. It generates a report on the results of the employees testing and provides recommendations aimed to improve it based on a defined the ISC level of the organization.

3. Database

DB is an integral part of the automated system for the ISC level assessing of the organization. The DB logical model is presented on fig. 3.

Let us focus on the most essential entities and relationships used in the DB.

Within the questionnaire, the questions may relate to separate themes or related ones. The degree of question's affiliation to some theme is determined by expert and contained in the table «Question's relevance to the theme».

The question's impact on the overall questionnaire's assessment is also determined by expert and contained in the «Question's relevance to the questionnaire» table.

Each «Question» is linked to multiple entries in the «Answer» table. The choice of the user answer to the certain question is determined by ticking the box (type Boolean, true/false) in the «Answer result» table.

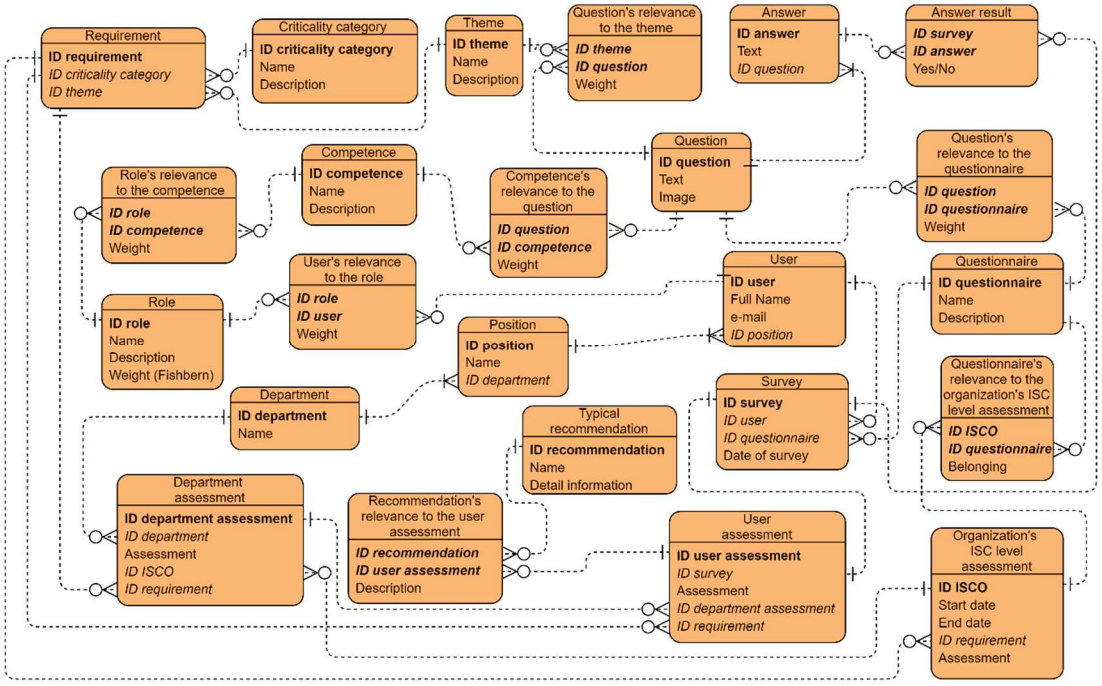

Fig. 3. The DB logical model

The «Survey» table contains information about the questionnaire that has been generated and the corresponding user which it was provided to be filled out. The «User» is associated with the relevant «Position» that he/she occupies within the «Department».

The «User Assessment» table links the appropriate questionnaire of the user, the assessment obtained as a result of the data processing by the module of personal ISC fuzzy assessment, and the requirement for the «User» of the «Competence».

The «Department assessment» receives the result after processing by the department's ISC level assessment module, that is stored by the corresponding «Assessment» attribute, and also contains link to the «Department» table, to the «Organization's ISC level assessment», and the «Requirement» that is associated with the department's activities.

The «Organization's ISC level assessment» table has fields of the beginning and end assessment. This allows to identify a set of survey results as those conducted within a single event.

«The questionnaire's relevance to the organization's ISC level assessment» is determined by the Boolean variable (true/false value), indicating whether the questionnaire was involved in the organization's ISC level assessment.

The table «Criticality category» serves as the basis for the information security requirements based on organizations membership to the criticality category of the infrastructure object. Also, the results of the organization's information security risk analysis are considered when filling the table «Recommendation's relevance to the user assessment».

Conclusions according to article. This work is a continuation of studies series that are dedicated to assessing the organization's information security culture level. The functional model of the top-level business process is offered. Formed functional requirements became the basis for development of information system architecture with description of its modules and database structure.

References

1. Lomakov, Iu. A. (2013). Metodiki otsenivaniia riskov i ikh programmnye realizatsii v kompiuternykh setiakh [Methods of risk assessment and their software implementation in computer networks]. *Molodoi uchenyi – Young scientist*, 2, 43–46. URL: https://moluch.ru/archive/49/6279.

2. Begun, V. V., Shirokov, S. V., Begun, S. V., Pismenniy, E. M., Litvinov, V. V., Kazachkov, I. V. (2012). *Kultura bezpeky v yadernii energetitsi [Culture of safety in nuclear power]*. Kyiv [in Ukrainian].

3. Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), 196–207. DOI: 10.1016/j.cose.2009.09.002.

4. Schlienger, Thomas & Teufel, Stephanie. (2003). Information security culture: From analysis to change. *South African Computer Journal*, 31, 46-52.

5. Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, 29(4), 476–486. DOI: 10.1016/j.cose.2009.10.005.

6. Furnell, S., & Thomson, K. L. (2009). From culture to disobedience: Recognising the varying user acceptance of IT security. *Computer Fraud and Security,* 2009 (2), 5–10. DOI: 10.1016/S1361-3723(09)70019-3.

7. Flores, W., Antonsen, E. & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioural information security governance and national culture. *Computers & Security*, 2014 (43), 90–110. DOI: 10.1016/j.cose.2014.03.004.

8. Alhogail, Areej & Mirza, A. (2014). A framework of information security culture change. *Journal of Theoretical and Applied Information Technology*, 64, 540–549.

9. Dubeikovskii, V. I. (2007). *Effektivnoe modelirovanie s AllFusion Process Modeler [Effective modeling with AllFusion Process Modeler]*. Moscow [in Russian].

10. Holota, Ya. Ya. (1992). O formalizatsii logiki nepolnykh znanii (logiki antonimov) [On the formalization of the logic of incomplete knowledge (the logic of antonyms)]. *Logika i razvitie nauchnogo znaniia – Logic and development of scientific knowledge* (pp. 92-112). St Petersburg University [in Russian].

11. Saaty, Thomas L. (2008-06). Relative Measurement and its Generalization in Decision Making: Why Pairwise Comparisons are Central in Mathematics for the Measurement of Intangible Factors – The Analytic Hierarchy/Network Process (PDF). *RACSAM (Review of the Royal Spanish Academy of Sciences, Series A, Mathematics)*, 102 (2), 251–318.

12. Bellman, R. E., Zadeh, L. A. (1970). Decision-making in a fuzzy environment. *Management Science*, 17 (4), 141-164. DOI: 10.1287/mnsc.17.4.B141.

13. Shkarlet, S., Lytvynov, V., Dorosh, M., Trunova, E., Voitsekhovska, M. (2020). The Model of Information Security Culture Level Estimation of Organization. Mathematical Modeling and Simulation of Systems. MODS 2019. *Advances in Intelligent Systems and Computing*, 1019, 249-258. DOI: https://doi.org/10.1007/978-3-030-25741-5_25.

14. Pro informatsiiu [On information]. № 2657-XII (October 02, 1992). URL: https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12.

15. Pro zakhyst personalnykh danykh [On Protection of Personal Data]. № 2297-VI (June 01, 2010). URL: https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2297-17.

16. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [On basic principles of cyber security in Ukraine]. № 2163-VIII (October 05, 2017). URL: https://zakon.rada.gov.ua/laws/main/2163-19.

17. Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh [On Protection of Information in Automated Systems]. № 80/94-VR (July 05, 1994). URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

18. Pro elektronni dokumenty ta elektronnyi dokumentoobih [On Electronic Documents and Electronic Documents Circulation]. № 851-IV (May 22, 2003). URL: https://zakon.rada.gov.ua/laws/show/851-15.

19. Informatsiyni tekhnologiyi. Metody zakhystu. Zvid pravyl dlya upravlinnya informatsiynoyu bezpekoyu (ISO/IEC 27002:2005, MOD): GSTU SUIB 2.0/ISO/IEC 27002:2010 [Information technology – Security techniques – Code of practice for information security management (ISO/IEC 27002:2005, MOD): Branch standard of Ukraine ISMS 2.0/ISO/IEC 27002:2010] (2010). Kyiv: National bank of Ukraine [in Ukrainian].

УДК 004.056

Віталій Литвинов, Марія Дорош, Ірина Білоус, Марія Войцеховська, Валентин Нехай

РОЗРОБКА АВТОМАТИЗОВАНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОЦІНКИ РІВНЯ КУЛЬТУРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

Актуальність теми дослідження. *Забезпечення ефективності впровадженої СЗІБ вимагає створення відповідної культури інформаційної безпеки співробітників організації з метою зниження ризиків, пов'язаних із людським чинником.*

Постановка проблеми. *Наявні сьогодні методики оцінки ІБ-ризиків випускають з поля зору людину як джерело потенційної вразливості. Враховуючи роль персоналу в СЗІБ організації, випливає необхідність у створенні автоматизованих систем оцінки людино-машинної взаємодії через рівень КІБ персоналу, а також інтегральний показник КІБ організації.*

Аналіз останніх джерел і публікацій. *Розглянуто публікації у вільному доступі, присвячені проблемам інтеграції культури інформаційної безпеки в корпоративну культуру організації як інструмента забезпечення належного рівня інформаційної безпеки бізнес-процесів.*

Виділення недосліджених частин загальної проблеми. *Аналіз джерел виявив відсутність формалізованих моделей оцінки рівня КІБ організації, а також автоматизованого процесу її оцінки.*

Постановка завдання. *Мета статті полягає в описі процесу отримання оцінки рівня КІБ організації за допомогою функціональної моделі в нотації IDEF0, архітектури та бази даних системи оцінки КІБ з метою підтримки СЗІБ організації.*

Виклад основного матеріалу. *Згідно з функціональними вимогами розроблено концептуальну модель бізнес-процесу «Визначити рівень КІБ організації». Визначені вхідна інформація, керуючі елементи системи, елементи та механізми виконання, а також вихідна інформація. Для реалізації поставлених завдань запропоновано архітектуру та базу даних інформаційної системи оцінки рівня КІБ організації.*

Висновки відповідно до статті. *Запропоновано функціональну модель бізнес-процесів верхнього рівня. Сформовані функціональні вимоги стали основою для розробки архітектури інформаційної системи з описом її модулів та структури бази даних.*

Ключові слова: *культура; інформаційна безпека; організація; персонал; інформаційна система.*
Рис.: 3. Бібл.: 19.

Vitalii Lytvynov –Doctor of Technical Sciences, Professor, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
Литвинов Віталій Васильович – доктор технічних наук, професор, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
E-mail: v.v.lytvynov.dept@gmail.com
ORCID: https://orcid.org/0000-0001-9622-3871
Scopus Author ID: 57211432068

Dorosh Mariia – Doctor in Technical Sciences, Professor of Information Technologies and Software Engineering Department, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
Дорош Марія Сергіївна – доктор технічних наук, професор кафедри інформаційних технологій та програмної інженерії, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
E-mail: mariyaya5536@gmail.com
ORCID: https://orcid.org/0000-0001-6537-9857
Scopus Author ID: 56912183600
ResearcherID: AAF-2603-2019

Bilous Iryna – PhD in Technical Sciences, Associate Professor of Information Technology and Software Engineering department, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
Білоус Ірина Володимирівна – кандидат технічних наук, доцент кафедри інформаційних технологій та програмної інженерії, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
E-mail: iryna.bilous.it@gmail.com
ORCID: https://orcid.org/0000-0003-3092-678X
Scopus Author ID: 57208344519
ResearcherID: G-3887-2014

Voitsekhovska Mariia – PhD student of Information Technology and Software Engineering department, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
Войцеховська Марія Михайлівна – аспірантка кафедри інформаційних технологій та програмної інженерії, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
E-mail: m.voitsekhovska@gmail.com
ORCID: http://www.orcid.org/0000-0002-1711-101X
Scopus Author ID: 57192818403

Nekhai Valentyn – assistant of Information Technology and Software Engineering department, Chernihiv National University of Technology (95 Shevchenka Str., 14035 Chernihiv, Ukraine).
Нехай Валентин Валентинович – асистент кафедри інформаційних технологій та програмної інженерії, Чернігівський національний технологічний університет (вул. Шевченка, 95, м. Чернігів, 14035, Україна).
E-mail: kilavv@live.com
ORCID: http://www.orcid.org/0000-0002-6209-5661
Scopus Author ID: 57211428428
ResearcherID: F-4825-2016

Lytvynov, V., Dorosh, M., Bilous, I., Voitsekhovska, M., Nekhai, V. (2020). Development of the automated information system for organization's information security culture level assessment. *Technical sciences and technologies*, *1* (19), 124-132.