Досліджена система цінностей учасників наукових міжнародних проектів з кіберзахисту. Побудовано модель визначення ступеня конвергенції цінностей учасників таких проектів, яка дозволяє відстежувати процеси формування, перетворення та змін цінностей під час реалізації проекту. Розроблені рекомендації щодо реагування менеджером проекту на зміни цінностей, призначені для забезпечення ефективної взаємодії між учасниками проекту

Ключові слова: проект з кіберзахисту, цінності проекту, конвергенція цінностей, ядро цінностей, взаємодія в проекті, учасники проекту

Исследована система ценностей участников международных научных проектов киберзащиты. Построена модель определения степени конвергенции ценностей участников таких проектов, которая позволяет отслеживать процессы формирования, преобразования и изменения ценностей при реализации проекта. Разработанные рекомендации по реагированию менеджером проекта на изменения ценностей предназначены для обеспечения эффективного взаимодействия между участниками проекта

Ключевые слова: проект по киберзащите, ценности проекта, конвергенция ценностей, ядро ценностей, взаимодействие в проекте, участники проекта

UDC [004.056:01.83](083.94)
DOI: 10.15587/1729-4061.2016.85215

THE STUDY OF PARTICIPANTS' VALUES CONVERGENCE ON THE EXAMPLE OF INTERNATIONAL SCIENTIFIC PROJECT ON CYBER SECURITY

M. Dorosh
PhD, Associate Professor*
E-mail: dorosh.m@inbox.ru
O. Trunova
PhD, Associate Professor*
E-mail: e.trunova@gmail.com
D. Itchenko
PhD, Lecturer**
E-mail: itchenko@list.ru
M. Voitsekhovska
Postgraduate student*
E-mail: m.voitsekhovska@gmail.com
M. Dvoieglazova
PhD, Associate Professor**
E-mail: maryna.dvoieglazova@gmail.com
*Department of Information Technology and Software Engineering***
Department of Public Administration and Management organization*
***Chernihiv National University of Technology
Shevchenko str., 95, Chernihiv, Ukraine, 14027

1. Introduction

Efficient activity of organizations under conditions of today's information society requires the formation of developed business environment, open to international cooperation. It is necessary to take into account rapid development of new technologies of information wars, operating around the world. Thus, we face the task of permanent development of new models and methods of cyber security at the international level, the implementation of which will allow enhancing a culture of information security of project participants. A solution to this problem may be found only under conditions of international cooperation and joined efforts in development and implementation of new methods and models in this area [1].

Establishing effective international cooperation is impossible without the use of project management, the main task of which in this case will be to ensure efficient interaction between project participants for its successful implementation. A determining factor of solving this problem is the formation of distributed information infrastructure as a catalyst for the application of methods of project management. The center of this infrastructure can be a project office on the basis of major enterprises and organizations [2]. Since such projects are mainly aimed at the development of new, innovative methods and models, while scientific organizations play a crucial role, such projects can be referred to as scientific.

Rapid changes that take place in Ukraine and in the world today lead to a reasessment of values of all social and economic groups, as well as at the personal level. This results in significant changes in the strategies of behavior of economic entities in all areas of economic, social and political life, which causes the need for improvement of existing and creation of new methods and approaches to making management decisions to ensure effective interaction between project participants.

The difference in the values of participants is especially vivd in the course of implementation of international projects. It is significantly influenced by different conditions of development of countries as a whole, as well as social groups and individuals in these countries. There is an extensive practice of remote control of international projects through modern means of communication, which, on the one hand, greatly simplifies and accelerates the processes of interaction

in projects, but, on the other hand, hinders full understanding of each other because of the lack of personal perception and understanding of feelings and values of other stakeholders.

Thus, the relevance of this study is explained by rapid development of international cooperation on cyber security, which takes place in the project environment. The key to successful implementation of such projects is establishing effective interaction between all participants, which requires development of new methods and models in this direction.

2. Literature review and problem statement

Today there are a lot of articles in the field of cyber security relating to the technical part of this issue. The number of studies that highlight scientific and organizational issues of implementing projects on cyber security is much smaller. The main organizations-participants of scientific projects on cyber security are the state and scientific institutions, as well as business organizations.

An analysis of the regulation of information security at the state level in economically developed countries, performed in [3], revealed that the safety rules may be comprehensive or partial, strategic or tactical, reactive or proactive. Some countries define security goals only; others have efficient mechanisms of risk management in this area. There are different approaches to determining the protection of personal data and privacy. These national differences are influenced by cultural norms of the society and have different advantages and disadvantages. This causes complexity in the implementation of international projects in this field.

The formation of systems of information security in business organizations is described in many papers, for example, [4] proposed methodology to assist companies in evaluating their compliance with the international standards of ISO, as well as in planning and implementation of actions necessary to ensure certification by these standards. It may be a prerequisite for participation in the projects of cyber security.

Scientific institutions are also important participants in certain projects as the sources of creation of new information and development of new products and services through effective use of information. Article [5] deals with the problems of infrastructure, operation, use of information, in accordance with the standards of information security of research institutions. The implemented method of risk analysis allows comparing security systems of different universities, which may determine the degree of their readiness to participate in the project activities of cyber security.

In [6], it is noted that the implementation of measures on cyber security must be supported by the scientific approach to the standardization of these processes, both in the field of information technology and in the field of project management.

The use of value-oriented approach to the projects implementation is considered in [7], where models of development of an organization and its corporate systems of project management, based on the value approach under conditions of turbulence, are presented. Paper [8] is also of interest since it offers a value-homeostatic approach to the assessment of project decisions, taking into account priority of expected values and the values that are contributed by participants, as well as compliance of the values, formed by a project, with participants' expectations. Article [9] in this field contains a value-oriented analysis of decision-making in managing projects and makes it possible to take into account the level of prevailing value memes in projects at certain points of their implementation and to perform calculations of value assessment of the project product more accurately.

In addition, there are a large number of scientific papers, in which researchers put material sense to the concept of project value. This is proved by article [10], in which, based on the conducted analysis, the modern researchers' concentration on issues of maximization of commercial value was defined and further directions of business development were revealed. In [11], the difference between a value of the project and the value of project management was determined, taking into account changes in values of stakeholders in the course of project implementation. The study of value of project management itself, presented in [12], proves the existence of high-efficiency project management, but reveals the problem of different values in a project team, which corresponds to the set goal.

The overview we performed indicates that the studies, carried out in the chosen direction, are at their initial stage and are relevant for further development. There is no mechanism for managing the values of project participants, which would take into account intangible values that play a key role in international projects.

3. The aim and tasks of the study

The aim of this study is to define methods of forming the participants' values system on the example of training for the participation in the NATO grant program "Science for Peace and Security Programme (SPS), topic: Cyber security" at Chernyhiv National Technological University. The aim also includes development of the apparatus of effective cooperation of major project participants on the basis of convergence of values. This will allow ensuring compliance of the values, obtained as a result of the project implementation, with the personal planned values of each project participant, which is the key measure of its success.

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

– to identify main participants of scientific projects on cyber security and to define their values;

– to propose a method for forming a universal system of values of the project with the definition of the core of such system;

– to propose a model for determining the degree of convergence of values of project participants and to create the mechanism for making project decisions to ensure their effective interaction;

– to develop recommendations concerning a response of the project manager to the changes in the values of participants, taking into account the degree of their convergence.

4. Materials and methods of examining the problem of the formation of the system of values of participants on the example of international scientific project of cyber security

Since the concept of "value" is associated with the axiological category "evaluation" – measurement (appreciation or rejection), the value of a project product is usually determined by the ouput it produces and passes onto a product while meeting the requirements contained in the project mission. In the

practice of project management, the value of a project product and the value of project management are distinguished. Both of these assets can be used to gain certain benefits.

There are two necessary conditions that warrant creation of the project value. The first one is the practical ability of the project manager to complete the project in accordance with the plan; the second one is finding a way to harmonize (balance) the project value for all stakeholders through the properties of a project product. The first condition is mandatory, whereas the second one is a sufficient condition for creating the project value.

Taking into account the individuality of perception and life experience, it is possible to argue that each person has its own unique model of perception and information processing depending on what this person finds valuable in this world.

Therefore, at the present stage of development of project activity, the main factor of the project success is active participation of stakeholders in approving and making key decisions in the course of project implementation. Each stakeholder, as well as the project team, expresses different values that define different objectives and outcomes of the project. In addition, over the life cycle of the project there appear turbulence and migration of values of stakeholders, and in the project situations it is necessary to make decisions on the basis of project indicators, which should reflect harmonized value of all stakeholders.

In this case, it is determined in [13] that the provision of information security must be implemented not only with the help of technical and technological means, but also through the formation of culture of information security of participants of information processes, based on their values.

Paper [9] contains a formulated scientific fact that in project situations, stakeholders form a vision of a variant of project continuation without necessary regard to strategically-service values of the project, taking practically only personal values as a basis. This fact puts forward new problems to the project team, which should contribute to more grounded scientific approach to decision making by stakeholders of the project, otherwise there is a real threat to its successful implementation.

Practical experience also proves that the majority of stakeholders cannot establish their own system of values independently, so there is a need for active participation of the project team that shapes and directs such a system in accordance with the overall project strategy, which requires special methods and models.

It is known that success of a project depends on making project decisions by a project team and approving them by key participants. This can be achieved through ensuring the convergence of values of all participants of the project.

The lack of convergence of values in a project could lead to such consequences as delays and overexpenditures, connected with delays in the process of making constructive decisions. The manager and the project team should develop an ongoing process of tracking the convergence of values and focus on timely response to any deviations.

In international projects, it is possible to form and examine values in three categories:

– the values contributed to project by its participants (competence, experience, investments);

– the values of project itself, which are formed from the totality of values of participants of the project, taking into account synergic effect;

– the values that the project participants and consumers gain from its implementation.

5. Results of studying and forming a model for the system of values of participants on the example of international scientific project of cyber security

In the process of preparation for the participation in the NATO grant program "Science for Peace and Security Programme (SPS), topic: Cyber security", the key potential participants of the project were defined. They were selected on the basis of the main goals of cooperation between NATO and partner countries in the field of cyber security, namely:

– improving the efficiency of NATO and partner countries in the field of protection of crucial communication and information infrastructures against cyber attacks;

– laying the foundations for support measures in cases of cyber attacks;

– provivion of assistance in restoring normal functioning of a correspondent infrastructure after cyber attacks.

The formed system of values of participants of the international scientific project on cyber security is shown in Fig. 1. Taking into account scientific orientation of the given project, it is proposed to create a management system of this project on the basis of leading universities, which have experience and capabilities to carry out scientific research in the field of cybersecurity.

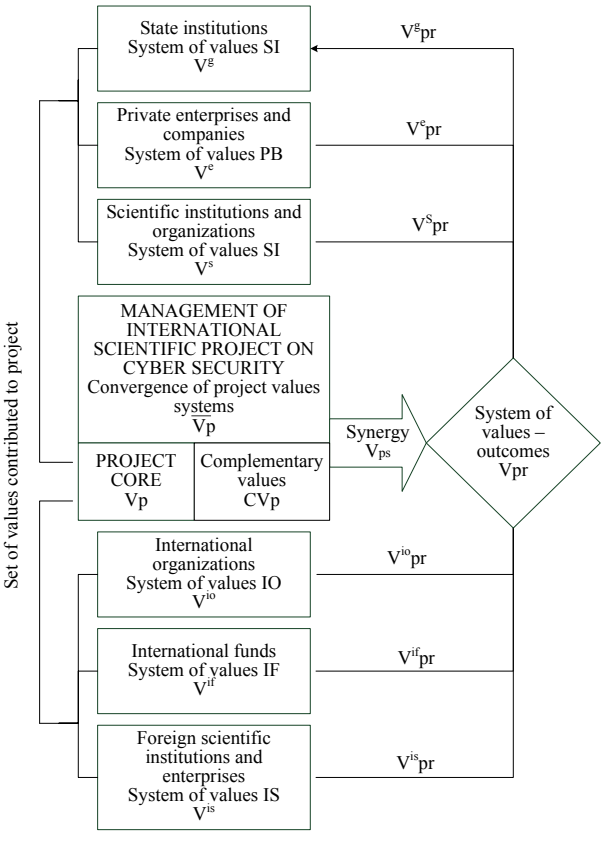

Fig. 1. Model of creating the system of international scientific project participants' values system

The values of the key stakeholders are given in Table 1. It is clear that it is difficult to consider all values of participants, so only those, which provide for the possibility to execute projects within the framework of international programs of cyber security, were selected in the table.

Taking the example listed in Table 1, we will construct a model for the project values and identify its common values.

Table 1

Values of the international scientific project on cyber protection's (security) stakeholders

Values of State (V^g)	Values of organization (V^e)	Values of international organizations (V^{io})	Values of international funds (V^{if})	Values of scientific institutions (V^s)	Values of international scientific institutions and organizations (V^{is})
V^g_1 – increasing resources of all entities on the territory of the state; V^g_2 – territory and resources safety from all external claims; V^g_3 – strengthening instruments capable of providing safety ; V^g_4 – increasing life quality of all entities on the territory of the state; V^g_5 – protection of living environment on the territory of the state.	V^e_1 – values, for the sake of which organization was created; V^e_2 – increasing over time of all kinds of resources that are under control of organization; V^e_3 – defense of own development under conditions of competitive economic environment; V^e_4 – desire to find loyalty of consumers, state and humanity as a whole.	V^{io}_1 – consistent and harmonious development; V^{io}_2 – providing global product safety; V^{io}_3 – contribution to solving problems connected with global economic crisis; V^{io}_4 – providing political dialogue on international economic and financial issues; V^{io}_5 – saving system of stability of international trade; V^{io}_6 – contribution to development of economically poor regions and countries.	V^{if}_1 – support of international cooperation and connections in area of scientific and technical development, socio-economic policy. V^{if}_2 – financing and support of international projects and developments; V^{if}_3 – strengthening development of democracy and civil society.	V^s_1 – uniformity in assessment authenticity of scientific research; V^s_2 – scientific research should become common gains; V^s_3 – responsibility for scientific research and developments to society; V^s_4 – regulation of activity that accompanies knowledge production, complying with ethical norms of conducting research; V^s_5 – formation of own image as social institution; V^s_6 – orientation to consumer needs	V^{is}_1 – organization of communication process among scientific organizations in various countries; V^{is}_2 – cooperation of scientists of various countries; V^{is}_3 – pursuit of integration of international information streams into united system of knowledge.

First, the system of project values V^0_p is formed at the intersection of sets of values of project's stakeholders, who define the unity in pursuit of the project implementation.

$$V^0_p = V^g \cap V^e \cap V^s \cap V^{io} \cap V^{if} \cap V^{is}, \quad (1)$$

where

$$V^g = \left\langle V^g_1, V^g_2, V^g_3, V^g_4, V^g_5 \right\rangle;$$

$$V^e = \left\langle V_1, {}^eV_2, {}^eV_3, V_4 \right\rangle;$$

$$V^{io} = \left\langle V^{io}_1, V^{io}_2, V^{io}_3, V^{io}_4, V^{io}_5 V^{io}_6 \right\rangle;$$

$$V^{if} = \left\langle V^{if}_1, V^{if}_2, V^{if}_3 \right\rangle;$$

$$V^s = \left\langle V^s_1, V^s_2, V^s_3, V^s_4, V^s_5 V^s_6 \right\rangle;$$

$$V^{is} = \left\langle V^{is}_1, V^{is}_2, V^{is}_3 \right\rangle.$$

This system forms the core of the project. The formation of such core can take place only with the active participation of the project manager, since not all project participants have a clearly formed list of values of the organization, and participation in the project can lead to the creation of new values that the heads of organizations and institutions may not be aware of.

So, the formed core of values is necessary to evaluate in terms of its completeness to ensure implementation of international projects on cyber security.

6. Discussion of results of modeling. Determination of the degree of convergence of project participants and methods for ensuring their effective interaction

It should be noted that similar elements that are at the intersection of the systems can have the same name but be completely different by the semantic content. For example, the value of "security" is located at the intersection of all sets, but has a different degree of value to participants. The approximation of these concepts in the project is not simple averaging of their point-scoring assessment, but can take place through evaluation of the degree of convergence of these concepts for various participants [14]. In this case, the degree of convergence can be defined using Euclidean distance. To do this, it is possible to perform the normalization of indices of the system elements, or to carry out point-scoring assessment of a value in terms of significance for each participant. It is also necessary to take into account the value of each element for a project, and then assessment of degree of convergence (Con) can be performed through Euclidean distance to the core of the project.

$$Con = \sqrt{\sum_{i=1}^{N} (A_i - B_i)^2}, \quad (2)$$

where A_i and B_i are the degree of value of the i-th element for two different project participants; N is the number of project participants.

Then, after forming the core of the project, the degree of convergence can take into account the weight of each factor for the project (balanced convergence Con_{bal}).

$$Con_{bal} = \sqrt{\sum_{i=1}^{N} k_j (A_i - B_i)^2}, \quad (3)$$

where k_j is the value of the i-th element for the project.

The value of certain element k_j for the project can be determined by using such parameters as degree of influence on the outcome of the project and elasticity. The project team may conduct such assessment using the method of paired comparisons.

Experimental evaluation of degree of convergence of participants of the project of preparation for the international program of cyber safety is shown in Fig. 2.

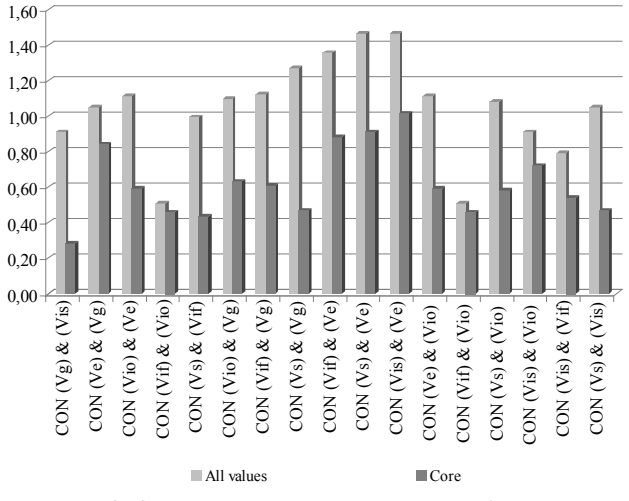

Fig. 2. Cyber security project participants' values convergence

We can see from the diagram given in Fig. 2 that even at the initial stage of the project of preparation for the implementation of programme on cyber security, there is a high degree of discrepancy between the values of business enterprises and organizations and the values of scientific organizations. It is clear that this is caused by essential differences in such values as gaining profit and replenishing resources. In this case, convergence in the core of values shows more convergence between the values of the state and scientific institutions. Here the project manager must work better to ensure interaction between commercial organizations and state authorities and scientific institutions.

Resulting indicators of degree of convergence consequently will require constant monitoring and adjustments with the aim of convergence of values of the project participants to ensure a high level of motivation and successful project implementation. In this case, the value of the index of convergence degree can be characterized as it is listed in Table 2. The table also contains recommendations for the actions of the project manager in the identified situations. The limits for these indices are established considering the specifics of projects of cyber security.

Further formation of the values' core can take place with the use of the method of structural matrices [15], which is based on the statement that any system is a set of input, core and output. In addition, useful factors and obstacles are distinguished at the input.

Table 2

Determining a degree of cyber security project participants' values convergence

Limits of value of index CON	Degree of participants' values convergence	Recommended actions for project manager
$0 \le Con < 0,4$	high	– formation of project documentation by defined values; – development of measures for providing support for values at this level throughout project life cycle
$0,4 \le Con < 0,6$	medium	– specifying assessment of values by project participants; – reporting common values of other stakeholders to all participants; – adjustment of system of values of the project
$0,6 \le Con < 0,8$	low	– partial change of project participants; – identification of new (hidden, implicit) goals of participants, which can be the basis for successful cooperation.
$0,8 \le Con \le 1,0$	critically low	– change of project participants; – change of common values of project

The matrix of influences in Fig. 3 is plotted on the basis of the values, defined for the examined project taking into account the overall system (Table 1) and the cores of values of the project (1). Other factors are distributed between the input and the output. If the distribution into these groups is possible, this is a systems organization, if not – these are indirect links. Only direct links are specified in the matrix.

	Factors (1)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Accretion resources	1					←		←							
2	Safety	→	2		←	←	←	←	←						←	
3	Methodological innovations			3												
4	Increasing quality of life	→	→		4		←		←							
5	Environmental protection					5										
6	Gaining profit	→		→	→		6	←	←							
7	Loyalty of environment							7								
8	Sustainable development			→	→		→		8							
9	System's stability			→	→		→		→	9						
10	Establishing effective interaction		→								10				←	
11	Universality	→										11				
12	Certainty of genuine knowledge and experience			→									12		←	
13	Openness		→		→	→		→						13		
14	Responsibility		→			→									14	
15	Integration							→								15

Fig. 3. Interconnections in the system of cyber security project participants' values

We will divide all selected values into three groups:

1st group includes the values that influence other values of the examined process, but are not exposed to influences (3, 5, 7).

2nd group includes the values that not only influence others but are also exposed to influences (1, 2, 4, 6, 8, 14).

3rd group includes the values that are exposed to influences, but do not affect other values (9, 10, 11, 12, 13, 15).

Then we relocate elements of the matrix so that the diagonal elements, which belong to the first group, are located in the first diagonal minor of the matrix, those belonging to the second group – in the second minor, those belonging to the third group – in the third minor.

In our case, the matrix will take the form, presented in Fig. 4.

		$\bar{x}_{in}$			$\bar{x}_{cond}$											
Factors (2)		3	5	7	1	2	4	6	8	14	9	10	11	12	13	15
3	Methodological innovations	3														
5	Environmental protection		5													
7	Loyalty of environment			7												
1	Accretion resources				1			←	←							
2	Safety		→	→	→	2	←	←	←	←						
4	Increasing quality of life				→	→	4	←	←							
6	Gaining profit	→		→	→		→	6	←							
8	Sustainable development	→					→	→	8							
14	Responsibility		→			→				14						
9	System's stability	→					→	→	→		9					
10	Establishing effective interaction					→				→		10				
11	Universality				→								11			
12	Certainty of genuine knowledge and experience	→								→				12		
13	Openness		→	→		→	→								13	
15	Integration			→												15
																$\bar{x}_{out}$

Fig. 4. Formation of the core of values of project on cyber security

It is clear that elements of links of the second minor create closed contours on the matrix, and the values corresponding to these elements will constitute the "core of the system". The values that belong to the first minor constitute "inputs" of the system, and those belonging to the third minor constitute the "outputs" of the system. In turn, values of the inputs and outputs may belong to the cores of other subsystems, which, together with the examined system, create a system of the higher level.

Thus, we obtained the core of the system, which consists of the values of augmenting resources, security, enhancing life quality, gaining profit, sustainable development and responsibility. Input values x_3, x_5, x_7 can be considered not only as resources, but also as obstacles, which, in fact, are limitations of the project. For the examined project, these factors are limitations.

Taking into account the fact that informational or organizational and technical systems are under consideration, project managers may, in the defined order, change links independently, on the basis of their own experience and results of discussion of these factors with stakeholders. In our case, we see that other 3 subsystems that make up the values 2 and 4; 4 and 6; 6 and 8, 6 and 1, 2 and 14 are distinguished inside the core. In this case, there is a question of importance of the links between factors 1 and 6, because for the subsystem of factors 6 and 8, one input for entering of this subsystem to the core is enough.

The defined core will require further comparison with the demands and capabilities of all participants of the project on cyber security.

After initial harmonization of the system of values of the project, in order to ensure its further development, new necessary components of the systems of values of participants are added to the defined set. As a result, a complementary system of project values CV_p is formed:

$$\begin{aligned} CV_p = \Big\{ & \Big\{ v^g : v^g \in V^g \wedge v^g \notin V_p^0 \Big\}, \\ & \Big\{ v^e : v^e \in V^e \wedge v^e \notin V_p^0 \Big\}, \\ & \Big\{ v^{ph} : v^{ph} \in V^{ph} \wedge v^{ph} \notin V_p^0 \Big\}, \\ & \Big\{ v^s : v^s \in V^s \wedge v^s \notin V_p^0 \Big\}, \\ & \Big\{ v^{io} : v^{io} \in V^{io} \wedge v^{io} \notin V_p^0 \Big\}, \\ & \Big\{ v^{if} : v^{if} \in V^{if} \wedge v^{if} \notin V_p^0 \Big\}, \\ & \Big\{ v^{is} : v^{is} \in V^{is} \wedge v^{is} \notin V_p^0 \Big\} \Big\}. \end{aligned} \quad (4)$$

In the process of project implementation, there is a transformation (correction) of the values of project participants into the outcome. A system of values $\overline{V}_p$ that contains those elements of the overall system of values of participants, for gaining of which the project was implemented:

$$\begin{aligned} V_p = \Big\{ & \Big\{ v^g : v^g \in V^g \wedge v^g \notin V_p^0 \wedge v^g \notin CV_p \Big\}, \\ & \Big\{ v^e : v^e \in V^e \wedge v^e \notin V_p^0 \wedge v^e \notin CV_p \Big\}, \\ & \Big\{ v^{ph} : v^{ph} \in V^{ph} \wedge v^{ph} \notin V_p^0 \wedge v^{ph} \notin CV_p \Big\}, \\ & \Big\{ v^s : v^s \in V^s \wedge v^s \notin V_p^0 \wedge v^s \notin CV_p \Big\}, \\ & \Big\{ v^{io} : v^{io} \in V^{io} \wedge v^{io} \notin V_p^0 \wedge v^{io} \notin CV_p \Big\}, \\ & \Big\{ v^{if} : v^{if} \in V^{if} \wedge v^{if} \notin V_p^0 \wedge v^{if} \notin CV_p \Big\}, \\ & \Big\{ v^{is} : v^{is} \in V^{is} \wedge v^{is} \notin V_p^0 \wedge v^{is} \notin CV_p \Big\} \Big\}. \end{aligned} \quad (5)$$

As a result of project implementation, there are also new project values V_{ps} that appear due to synergy. Therefore, the outcome of project implementation will be the system of values V_{pr}, which will be effective only inder condition of constant monitoring of convergence of values over entire life cycle:

$$V_{pr} = V_{ps} \cup V_p. \quad (6)$$

The effectiveness of project implementation in the system of values can be determined by ratio:

$$V_{pe} = (V_p^0 \cup CV_p) \cap V_{pr}. \quad (7)$$

The given model of formation and transformation of the system of values of the project participants makes it possible to support decision making process on the project, taking into account the values of all project participants, and, due to its constant alignment, to maintain a high degree of interest of participants in successful project implementation.

To do this, it is necessary to implement the following logical steps:

– to determine the degree of project participants' values convergence;

– to form requirements to the level of convergence of project values and to make changes in the documentation for the project;

– to carry out regular monitoring of changes in the degree of convergence of the project values over its life cycle;

– to implement timely actions in case of deviations.

Thus, the research we conducted demonstrated the possibilities of forming a universal system of values of international projects on cyber security for establishing effective cooperation of all stakeholders. Comprehensible mathematical apparatus of the proposed method for determining convergence of values of the project provides for the opportunity for its application by the project manager of any level. Results of the study might be used in other projects of varying complexity.

Further research in this direction might be aimed at exploring changes in the convergence of values during project implementation and at developing measures to control the overall system of values of the project in accordance with these changes.

7. Conclusions

1. Defining the key participants of international scientific projects on cyber security and their values is the basis for further modeling of the universal system of values of the project, ensuring effective interaction between them and enhancing a general culture of information security.

2. The proposed method for the formation of values of the project requires active participation of the manager to ensure effective interaction between all participants. This is especially true for international projects that have maximum number of differences. Selecting the core of the system using the methods of structural matrices provides for the possibility to ensure completeness of the overall system of values that will actually allow implementing the project on cyber security.

3. The model for determining a degree of convergence of values of participants of the project on cyber security allows us to monitor the process of definition, transformation and change of the values during project implementation and is the basis for building up an effective system of monitoring the convergence of values of the project participants.

4. The given recommendations that address a response of the project manager to changes in the values of participants with regard to a degree of their convergence should significantly enhance efficiency of the processes of project planning and make it possible to take timely and necessary decisions on establishing (renewing) efficient interaction between all project participants.

References

1. Kundenko, A. Crisis management of small and medium businesses in regional economic policy system [Text] / A. Kundenko // The Economic Annals – XXI Journal. – 2015. – Vol. 5-6. – P. 108–111.
2. Dorosh, M. Project management in cybersecurity research in Ukraine [Text] / M. Dorosh, V. Lytvynov, M. Saveliev // Information models & analyses. – 2015. – Vol. 4, Issue 4. – P. 324–335.
3. Johnson, J. A comparison of international information security regulations [Text] / J. Johnson, S. J. Lincke, R. Imhof, C. Lim // Interdisciplinary Journal of Information, Knowledge, and Management. – 2014. – Vol. 9. – P. 89–116.
4. de Revista, G. Da Tecnologia e Sistemas de Informação [Text] / G. de Revista // Journal of Information Systems and Technology Management. – 2005. – Vol. 2, Issue 2. – P. 121–136.
5. Yilmaz, R. A Comparative Analysis of University Information Systems within the Scope of the Information Security Risks [Text] / R. Yilmaz, Y. Yalman // TEM Journal. – 2016. – Vol. 5, Issue 2. – P. 180–191.
6. Podhorec, M. Cyber security within the globalization process [Text] / M. Podhorec // Journal of defense resources management. – 2012. – Vol. 3, Issue 1. – P. 119–126.
7. Bushuev, S. D. Mehanizmyi konvergentsii metodologiy upravleniya proektami [Text] / S. D. Bushuev, N. S. Bushueva, S. I. Neizvestnyiy // Upravlinnya rozvytkom skladnykh system. – 2012. – Vol. 11. – P. 5–13.
8. Teslya, Yu. N. Tsennostno-gomeostaticheskiy podhod k otsenke resheniy po proektu [Text] / Yu. N. Teslya, I. I. Oberemok, N. V. Oberemok // Upravlenie razvitiem slozhnyih sistem. – 2016. – Vol. 25. – P. 73–79.
9. Molokanova, V. M. Tsinnisno-oriyentovanyy analiz pryynyattya rishen' v upravlinni proektamy [Text] / V. M. Molokanova // Upravlinnya rozvytkom skladnykh system. – 2016. – Vol. 25. – P. 32–37.
10. Martinsuo, M. Value management in project portfolios [Text] / M. Martinsuo, C. P. Killen // Project Management Journal. – 2014. – Vol. 45, Issue 5. – P. 56–70. doi: 10.1002/pmj.21452
11. Zhai, L. Understanding the value of project management from a stakeholder's perspective [Text] / L. Zhai, Y. Xin, C. Cheng // Project Management Journal. – 2009. – Vol. 40, Issue 1. – P. 99–109. doi: 10.1002/pmj.20099

12. De Oliveira, W. A. Creation from organizational project management: a case study in a government agency [Text] / W. A. De Oliveira, C. F. De Muylder Malue // Journal of Information Systems and Technology Management. – 2012. – Vol. 9, Issue 3. – P. 497–514.
13. Lytvynov, V. V. Formuvannia i pidvyshchennia kultury informatsiinoi bezpeky orhanizatsii [Text] / V. V. Lytvynov, O. V. Trunova, M. M. Voitsekhovska // Stvorennia ta modernizatsiia ozbroiennia i viiskovoi tekhniky v suchasnykh umovakh, 2016. – P. 163–164.
14. Bushuyev, S. D. Formuvannya innovatsiynykh metodiv ta modeley upravlinnya proektamy na osnovi konverhentsiyi [Text] / S. D. Bushuyev, M. S. Dorosh // Upravlinnya rozvytkom skladnykh system. – 2015. – Vol. 23. – P. 30–37.
15. Shatihin, L. G. Strukturnyie matritsyi i ih primenenie dlya issledovaniya sistem [Text] / L. G. Shatihin. – Moscow: Mashinostroenie, 1991. – 256 p.

UDC 621:681.65
DOI: 10.15587/1729-4061.2016.85204

SYNTHESIS OF INTEGRAL QUALITY INDEX OF PARAMETRIC SYSTEM STATE IN CONDITIONS OF SITUATIONAL UNCERTAINTY

V. Skachkov
Doctor of Technical Sciences,
Professor, Senior Researcher*
Scientific Research Laboratory
Military Academy
Fontanskaya doroga str., 10, Odesa, Ukraine, 65009
E-mail: v_skachkov@ukr.net
V. Chepkyi
PhD, Associate Professor, Senior Researcher*
E-mail: viktor2011@mail.ru
S. Volkov
PhD, Associate Professor**
E-mail: greyw@ ukr.net
V. Pavlovich
Postgraduate student**
E-mail: pavidlovi4@gmail.com
*Scientific Research Laboratory
Military Academy
Fontanskaya doroga str., 10, Odesa, Ukraine, 65009
**Department of computer and
information-measuring technology
Odesa State Academy of Technical Regulation and Quality
Kovalska str., 15, Odesa, Ukraine, 65020

Запропоновано ступінь невизначеності стану параметричної системи чисельно оцінювати середньою кількістю інформації на виході досліджуваної системи, використовуючи модифіковану метрику Шеннона. На основі інформаційно-ентропійного підходу синтезовано інтегральний показник якості стану системи, отримані загальна і часткова аналітичні форми його представлення. Оцінено втрати інформації про поточний стан параметричної системи в умовах впливу зовнішніх збурень і розширення спектру внутрішньосистемних збурень, включаючи також багатопараметричний вектор адаптивного управління

Ключові слова: інформаційно-ентропійний підхід, інтегральний показник, зовнішні збурення, внутрішньосистемні збурення, ситуаційна невизначеність, інформаційні втрати

Предложено степень неопределенности состояния параметрической системы численно оценивать средним количеством информации на выходе исследуемой системы, используя модифицированную метрику Шеннона. На основе информационно-энтропийного подхода синтезирован интегральный показатель качества состояния системы, получены общая и частная аналитические формы его представления. Оценены потери информации о текущем состоянии параметрической системы в условиях воздействия внешних возмущений и расширения спектра внутрисистемных возмущений, включая и многопараметрический вектор адаптивного управления

Ключевые слова: информационно-энтропийный подход, интегральный показатель, внешние возмущения, внутрисистемные возмущения, ситуационная неопределенность, информационные потери

1. Introduction

Evaluating the quality of parametric systems' condition involves the necessity to solve multi-criteria (vector) optimization problems. The most difficult are multi-criteria problems to be solved in terms of situational (a priori) uncertainty; they belong to the class of ill-posed problems as viewed by Hadamard and Tikhonov [1–4]. In these problems, minor variations of the observed sample implementations $u_i(t)$, where i=1, 2,..., η, lead to unintended results.

Situational uncertainty in assessing a parametric system is determined by the effect of unplanned destabilizing factors