

PROJECT MANAGEMENT IN CYBERSECURITY RESEARCH IN UKRAINE

Maria Dorosh, Vitalii Lytvynov, Maxim Saveliev

Abstract: *This paper presents an approach to cyber security research project management. The paper includes the Project Management Office model and conception that can be created in educational and research institution like University. The organization structure of the cyber security research project and the peculiarities of university team organization on cyber security research project are shown.*

Keywords: *project management, cyber security, educational and research projects.*

ACM Classification Keywords: *K.6.1 Management of Computing and Information Systems - Project and People Management*

Introduction

The formation of information society influences the dynamic development of various types of cooperation realised by means of modern information technologies. These changes are aimed at large-format expansion of multi-vector information consulting environment that initiates and supports innovations, and promotes the development of project approach in the process of creation and implementation of strategic development projects and programmes [Chukhrai, 2015].

The synthesis of advanced information and communication technologies and the rapid development of computer technology play a great role in this process: they have caused the creation of fundamentally new global substances –information space and information society, which have practically unlimited potential and play a significant role in the economic and social development of any country in the world.

However, the development of information and communication technologies leads to the emergence of new threats at the level previously unknown to mankind. On the one hand, it provides an access to restricted information, the use of which can cause economic damage such as terrorism, sabotage and diversion to individual companies as well as society in general. On the other hand, it gives the opportunity to misrepresent real and public data, the usage of which can negatively influence economics and society in general. Thus, it is cyber security that is the main factor of sustainable development of modern information society.

Cyber security has become an important research policy in universities and research institutes all over the world. This article presents the information about approaches to cyber security research project management in Ukraine.

Analysis of Recent Researches and Publications

The analysis of publications dealt with the research on the development of special methods and models for providing cyber security [Stasiuk, 2012], [Okhrimenko, 2012] proves that uncontrolled dissemination and unrestricted use of information- and cyberspace by the world's leading countries in the form of arena of action in the course of modern information resistance have led to the following negative results: the majority of other countries (including Ukraine) are characterised by technological lagging and inequality in the sphere of information, nano-, bio-, telecommunication and other high technologies; information flows are duplicated and excessive IP are accumulated by the main subjects of information activity in these countries; public and military authorities of these countries lack qualitative information exchange; information sphere (infosphere) of these countries is not protected from the negative influence of internal and external cybernetic attacks (cyber-attacks) and threats (cyber threats) which can be deliberate, accidental, natural or artificial in their nature, etc. [Buriachok, 2011].

It should be noted that there are no publications dedicated to the project approach, use or creation of new modern methods of project management in the sphere of development and implementation of cyber security systems. That is why it is very urgent for Ukraine and the majority of other countries in the world to carry out research aimed at developing new or improving existing ways of organizing reconnaissance and delivering attacks on IT and cryptosystems, as well as means of resistance to outside influence from possible cyber-attacks and cyber threats.

Taking into consideration the information mentioned above we can introduce the purpose of our study: to present the peculiarities of project management in the sphere of development and implementation of cyber security systems as well as development of new approaches to the formation of such project management system.

In order to reach this aim the following tasks should be completed:

- - to analyse the state and prospects of international cooperation in the course of implementing projects connected with the creation and development of an entire cyber security system;
- - to create such project management system on the basis of higher education institutes of Ukraine;
- - to define the peculiarities of managing project team on the basis of higher education institutes.

Review of Ukraine-NATO Cooperation on Cyber Security Researches

Recent events taken place in Ukraine have influenced Ukraine to become an active participant in international discussions concerning the whole sphere of international relations on which information technologies are able to influence.

It is known that the main world leader in the sphere of development and implementation of cyber security programmes is the North Atlantic Alliance; and Ukraine was the first among non-aligned countries that began to consult with the North Atlantic Alliance on cyber security issues and announced that the country was interested in the development of universal international legal documents concerning this area. At the end of 2008 the Security Service of Ukraine initiated the establishment of the Working Subgroup on Cyber Defence under the aegis of the Ukraine-NATO Joint Working Group on Military Reform (JWG MR); this fact should have been the first step towards the development of cooperation between Ukraine and NATO in this sphere.

On 2 April 2009 the NATO headquarters spread the enclosed document under the title "Framework for Cooperation on Cyber Defence between NATO and Partner Nations". This document was a logical continuation of a number of former doctrinal documents which defined NATO's policy on cyber defence. Thus, NATO has created political and legal background and determined appropriate framework for establishing practical cooperation with partner nations, including Ukraine, interested in it.

According to the mentioned document, an essential element of NATO policy in the sphere of cyber defence is the principle that Allies have the prime responsibility for protecting their national communication and information systems, but at the same time NATO must have the ability to support Allies who are victims of a cyber-attack of national significance. Partner nations are urged to take necessary measures in order to harmonize national legislation in the sphere of cyber security in accordance with international norms such as the Council of Europe's Convention on Cyber Crime.

During 2009-2011 Ukraine actively cooperated with NATO. There were five stages of consultations of the Working Subgroup on Cyber Defence under the aegis of JWG MR in the "ad hoc" format. On the fourth stage, which took place in October 2011 in Yalta, the current state of development of the Strategy of Ukraine in the Sphere of Cyber Defence Project was discussed, but it was neither accepted nor executed. The last stage of consultations took place in 2013 in Yalta. After that, Ukraine had no opportunity to perform its activity in this sphere due to a number of objective and subjective reasons [Kandaurov, 2011].

Today the activity on cyber security and information defence is defined, first of all, in the Doctrine of Information Security of Ukraine and the Law on Fundamentals of National Security of Ukraine, and depends on the contradictions between the capabilities of existing methods and techniques of searching, collecting and getting information, as well as protecting our country's IP from foreign cyber influence, on the one hand, and user requirements for providing informational support, for example, to the administrative Board of the Ministry of Defence, the Armed Forces of Ukraine and our state in general, on the other hand.

One of the main drawbacks on the way of problem solving is that the legislation of Ukraine and the majority of other countries of the world has not given fixed definitions of the following notions: cyber-attack, cyber security, cyber influence, cyber warfare, cyber defence, cyber weapon, cyber operation, cyberspace, cyber reconnaissance and other terms that could be taken into account, for example, in the foreign policy activity of countries on the mentioned issues.

For the introduction of this terminology and determination of priority directions of activity in this sphere it was suggested to renew the development of the Cyber Security Strategy of Ukraine Project (2015-2018). This project defines:

- - basic terms and definitions;
- - threats in the sphere of cyber security;
- - main principles of cyber security of Ukraine;
- - main directions of resistance to threats in the sphere of cyber security;
- - system of cyber security of Ukraine;
- - stages of Strategy realization.

Therefore, cyber security requires taking coordinated measures and introducing integrated approaches under the aegis of the state and in close cooperation with the private sector and civil society, without which it is impossible to solve this problem. Furthermore, one country cannot resist cybercrime alone. The effective cooperation between various countries both at the state level and the level of cooperation between government organizations and representatives of the business sphere in the field of IT-technologies is necessary.

Scientific institutions, in particular higher education institutes, should play a leading role in providing scientific support in the process of realizing such a strategy. They can take an active part in the development, planning and implementation of projects involving international partners for the creation of

new approaches to project management in the sphere of development and implementation of cyber defence systems.

In June 2015 an international Cyber Security: Ukraine and the World forum was held in Kiev under the aegis of the Ukrainian Public IT Alliance Organization and the American Chamber of Commerce in Ukraine: the heads of services on security and protection of information of public authorities, bank, financial and corporate sectors discussed the risks of threats and presented new achievements and technologies in the sphere of cyber security. The Concept of Interuniversity Cyber Security Centre was presented on the forum as a project the main task of which is providing and improving the level of cyber security as a component of information security and national security of Ukraine. The project was presented by Kharkiv Zhukovskiy National Aerospace University "KhAI" and Kharkiv V.N. Karazin National University. This concept includes informational, educational, research, technological and communication components, but it does not define the project component and has no management system determined for the implementation of further development and practical application of this concept.

Unfortunately, the management systems of higher education institutes still use old management methods, despite the fact that new requirements for the development of education and society have changed and considerably expanded the directions of activity of all departments of educational institutes. The situation is that teachers and researchers teach their students and develop new systems in the sphere of management, technology and engineering, but they have no opportunity to use them within university. It concerns project management just as well.

At present project activity is carried out at all levels of management in various areas at universities. For example, the following projects can be executed within any Subdepartment:

- carrying out scientific and methodical seminars within the Subdepartment;
- organization and carrying out conferences;
- publication of the collective monograph;
- assisting in licensing particular specialities;
- implementation of some parts of projects (sub-projects) carried out at the university, etc.

In order to carry them out functional structures of project management are used, when a project coordinator is a director or employee of the structural subdivision who is responsible for the project

implementation. However, such a structure has its own drawback: coordinators in project management lack professional skills and knowledge. Of course, it does not mean that it is obligatory to get professional project managers involved in project management, but it demands the creation of a united project management office that will assist in training, consulting and strategic higher education institute project portfolio management.

Conception of Project Management Office (PMO) for Cyber Security Research in University

The main function of the project management office should be to establish the cooperation between stakeholders of projects and maintain effective communication in order to achieve synergistic effect and open new opportunities. This function can be realised by means of modern information technology applications.

Conceptual scheme presenting project management at institutes of higher education (Fig. 1) includes project management office functioning. This model is based on the following five elements of project activity [Neizvestnyi, 2005]:

- systematic approach;
- project life cycle;
- intellectual space of knowledge about project;
- project stakeholders;
- use of general management skills.

The scheme presents project management office built on the basis of the Kerzner project management maturity model [Kerzner, 2003]. This model includes different convergence layers used to connect other parts of a project; these layers make it possible to create innovative management methods and models.

Media convergence layer contains the approximation, agreement of various requirements, restrictions and possibilities concerning a project that are specified by stakeholders and environment. The systematic presentation of a project being formed by stakeholders, the core of values of all members should be defined and fixed in the form of project documentation, and innovative methods of convergence of project participants' values should be applied.

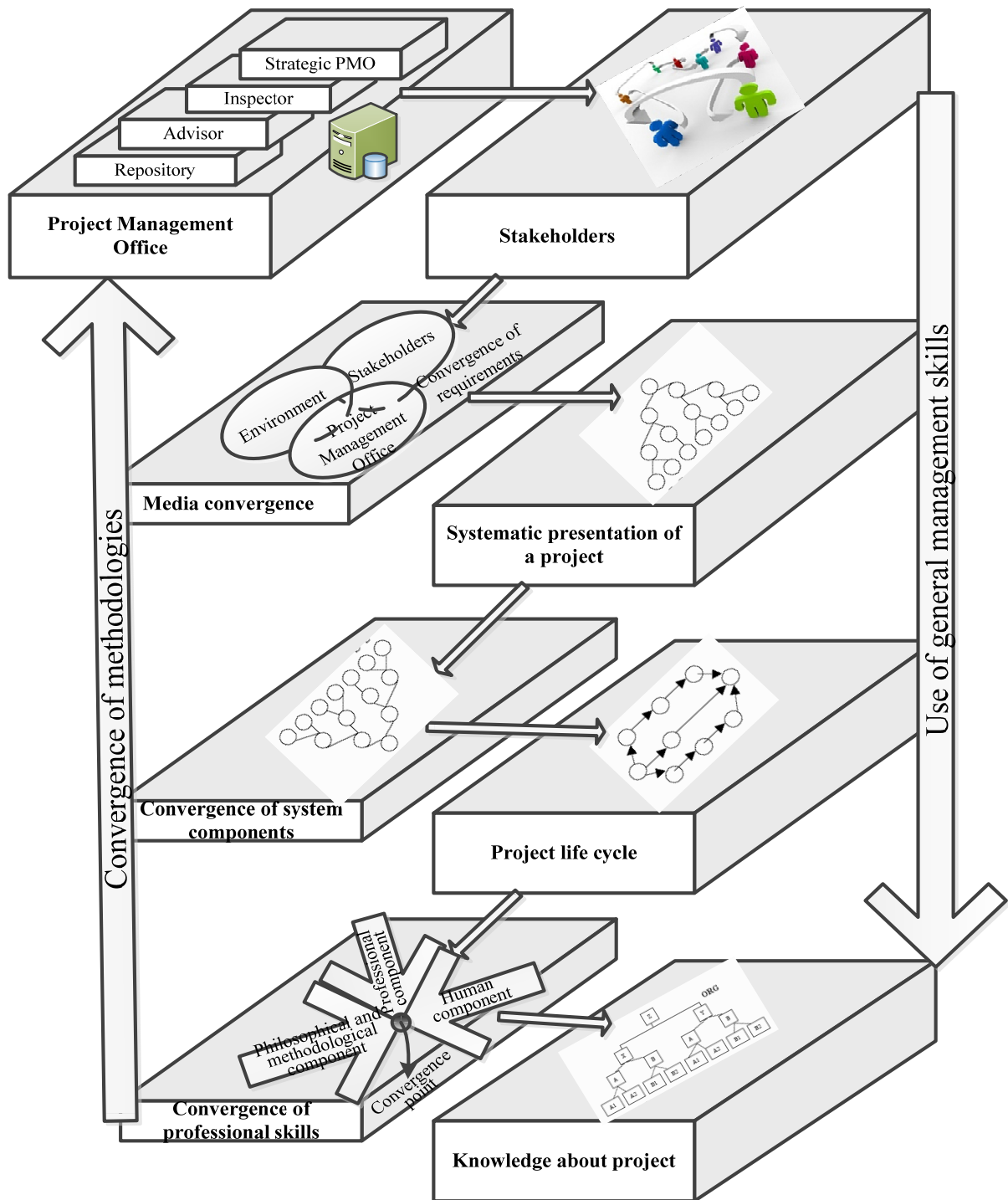


Fig. 1. Conceptual Scheme Presenting Project Management at Institutes of Higher Education

Convergence of system components layer contains the integration processes of coordinated informational, organizational, logistical and administrative components of a project and a basic institution (institute of higher education). Of course, it is not desirable to integrate these systems fully, because it can make it complicated to control the main parameters of the project during its implementation. It is necessary to separate the projects of different functional subdepartments of institute of higher education, though the same resources can be used by them.

Convergence of professional skills layer combines competencies that are peculiar to various types of professional activity involved in the project. In addition, it is necessary to take into consideration the combination of professional, philosophical, methodological and human components of a modern specialist. These components are the basis for convergence of methodologies which makes it possible to introduce innovative project methods and models.

It is also necessary to take into consideration the fact that project team and stakeholders responsible for cyber security projects constitute a virtual, motivational space, in which stakeholders devote themselves to their project, being in different geographical, cultural, special and organizational environments, and cooperate sharing their points of view on the project content, planning, control and communication within that project. The quality of an intellectual space influences significantly the project execution.

In addition, cyber defence projects are carried out under the aegis of international organizations, within which misunderstandings and contradictions caused by cultural peculiarities of participants from different countries often arise. Thus, using convergence methods will help to overcome these problems and lead to understanding between project participants.

It is known that all members of a project team cooperate with each other virtually through the Internet. That is why the effectiveness of communication within modern virtual project team depends on understanding project objectives and the fact whether the project participants are interested in working on it. First of all, a great attention is paid to correct professional communication skills regardless of geographical, temporary or cultural environment to which the project team members belong. In general, the configuration of relations between them forms the essence of project intellectual space.

Project Approach in the Process of Preparation for Participation in the International Cyber Security Program in Chernihiv National University of Technology.

Let us consider the peculiarities of using project approach in the process of preparation for participation in the International Cyber Security Program in Chernihiv National University of Technology.

The main objectives of cooperation between partner from different countries in cyber defence sphere are as follows:

- to improve the ability of partner nations to protect their critical communication and information infrastructures against cyber-attack;
- to provide a basis for support measures in cases of cyber-attack;
- to help restore normal functioning following such attacks.

Many specialists working in Chernihiv National University of Technology have been already engaged in the implementation of grant projects and programmes; their experience shows that there is a great need for a comprehensive and serious preparation for their implementation. The University is going to participate in the the NATO Science for Peace and Security grant programme and preparation has been started since October 2015.

First of all, the project team was formed, and its organizational structure which includes both external and internal project members was developed (Fig. 2).

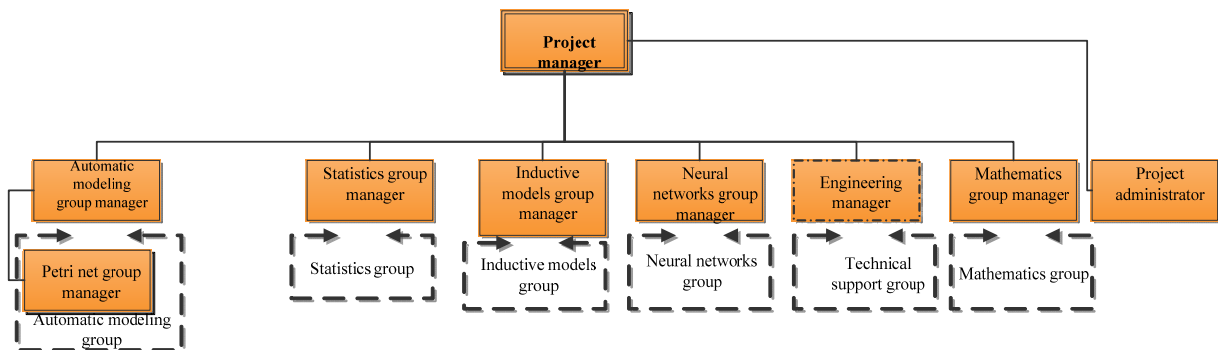


Fig. 2. Organizational Structure of Project Preparation for Project Cyber Security Execution

The project is managed by the project manager, and the organizational administrator carries out organizational activity. Also functional project groups were formed according to the areas of research. Experts, scientists, postgraduate students as well as students from different courses are members of such groups. In this case, the involvement of students plays an important role in the educational and methodological process, as such an activity teaches to solve real problems, bring them to completion, and work in team; it also helps coordinate and plan one own's activity.

In addition, the project scheduling being conducted makes it possible to control the process implementation and draw a conclusion about the effectiveness of some phases execution.

At present phase of the project implementation we can determine that:

- Project implementation by University teams always pursues two objects: first of all, acquiring new knowledge and mastering skills by project participants; secondly, successful project implementation in spite of fixed project restrictions (time-frame, money, quality). At the same time, students, postgraduate students and faculty will constitute the basic human resource of the project.
- In the process of such projects implementation the students lack the necessary knowledge, postgraduate students lack experience, and the faculty is limited to existing teaching load norm and bureaucratic procedures.

There are some more obstacles on the way of successful project execution:

- Time limitation. As a rule, students' projects are carried out within one semester (12 – 16 weeks). During this time it is difficult to form a team and conduct a quality work.
- Behavioral problems. Being students, young people have not formed professional relationship towards work and colleagues. They tend to form groups according to their personal preferences. Conflicts unknown to a teacher and project manager influence negatively the formation of groups.
- Restrictions in choosing research problem. As a result the students have no motivation to carry out a project.

We can distinguish the following two types of project work:

- project work carried out by the students of the same year of studying,
- general project work carried out by the faculty (students can be involved just as well).

In the first case, team members are characterized by approximately equal knowledge and ambition. In order to set up such a group Agile Scrum model was used. One of the main problems is to appoint a leader who forms the team and defines its activity. That is why this role is performed by teachers, but senior students are also given some tasks to be done.

In the second case, there is an absolute project leader. The team members carry out project tasks according to their functional abilities.

Thus, practical implementation of professional project management in higher education institutes gives the opportunity to use innovative scientific achievements of leading scientists involving students and postgraduate students to work in team, such an approach can significantly improve the efficiency of learning process and reduce the gap between theory and practice.

Conclusion

Finally, we can draw the following conclusions:

- the analysis of the state and prospects of further international cooperation in the course of implementing projects connected with the creation and development of an entire cyber security system has shown the necessity to continue active cooperation with NATO in cyber defence of Ukraine issues;
 - the suggested conceptual scheme presenting cyber security project management is supposed to be used at institutes of higher education; it contains all the components necessary for the development of innovative project management methods and models on the basis of project management office;
 - the results of practical application of professional project approach have revealed the main specific features of human resource management in such projects, that can become the basis for the development of new management methods and models at present.
-

Bibliography

- [Chukhrai, 2015] . Chukhrai N.I., Nowakowski I.I. (2015). Project management as a basis for effective development of the information society. Bulletin of National Technical University "KPI". Collected Works. Series: Strategic management, portfolio management, programs and projects, №2 (1111), 3-8. (in Ukrainian).
- [Stasiuk, 2012]. Stasiuk A.I., Korchenko A.A. (2012). Basic model parameters to build systems detect attacks. Scientific and technical journal "Protecting information", № 2 (55), 6-18. (in Russian).
- [Okhrimenko, 2012] .Okhrimenko A.A., Korchenko A.O. (2012). Model identification spoofing attacks on information systems resources. Information Technology and Data Protection: Third International Scientific Conference [Abstracts], 210. (in Ukrainian).
- [Buriachok, 2011]. Burachok V.L. (2011). Estimation algorithms degree of security specific information telecommunication systems . Scientific and technical journal "Protecting information", №3, 21-30. (in Ukrainian).
- [Kandaurov, 2011]. Kandaurov S. M. (2015) The question of cyber security. Interaction between Ukraine and NATO in the field of cyber security. Internet resource: <http://www.uan.ua/ua/content>. (in Ukrainian).

[Neizvestnyi, 2005]. Neizvestnyy S.I. (2005). Project Management : a tutorial, IT, 221. (in Russian).

[Kerzner, 2003]. Kerzner H. (2003). Strategic planning for project management using a maturity model. Publisher: DMK Press, IT Co., 320. (in Russian).

Authors' Information



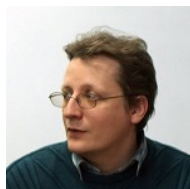
Maria Dorosh – PhD in PM, Chernihiv, National University of Technology, 95,
Shevchenko street, Chernihiv-27, Ukraine, 14027; e-mail: mariyaya5536@gmail.com

Major Fields of Scientific Research: Project Management



Vitalii Lytvynov – Dr. Sc., Prof. Chernihiv, National University of Technology, 95,
Shevchenko street, Chernihiv-27, Ukraine, 14027; vlitvin@ukrsoft.ua

*Major Fields of Scientific Research: modeling of complicated systems, computer
aided management systems, decision support systems*



Maxim Saveliev – Institute of Mathematical Machines and Systems Problems,
Ukraine;
e-mail: mcsim@sitex.com.ua

*Major Fields of Scientific Research: Software Engineering, Automated System Life
Circle Models, Requirements Evolution, System Analysis, System-of-Systems*