Forming the Abilities of Designing Information Security Maintenance Systems in the Implementation of Educational Programmes in Information Security

Vladimir Budzko, Natalia Miloslavskaya, Alexander Tolstoy

Forming the Abilities of Designing Information Security Maintenance Systems in the Implementation of Educational Programmes in Information Security

Vladimir Budzko, Natalia Miloslavskaya and Alexander Tolstoy

The National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), 31 Kashirskoye shosse, Moscow, Russia

{NGMiloslavskaya, AITolstoj}@mephi.ru

Abstract. The paper shares the NRNU MEPhI's experience in forming the abilities to design the Information Security Maintenance Systems (ISMaS) in training Bachelors, Masters and Engineers in the field of Information Security (IS). It is proposed to form their abilities and teamwork skills when executing a course project by a team of students under supervision of their Professor within the framework of the "IS Management" discipline. Course projects help to reinforce the students' theoretical knowledge and develop their ability to apply this knowledge to the solution of practical problems. They are assigned at a group basis and in our case are aimed at designing the ISMaS of a particular object, which automates the implementation of a separate organization's process. A brief description of the process model for ensuring IS of such objects is given and the regulations for implementing the course project are presented in detail, indicating the types of abilities that are gained at each stage.

Keywords: information security, professional competencies, abilities, system, processes, educational programme

1 INTRODUCTION

The implementation of educational programmes in the field of information security (IS) is aimed at the formation of specific professional competencies. This approach is consistent with the set of requirements that employers place on professionals in any field of professional activity, including IS [1-4]. A competency is traditionally referred to a combination of observable and measurable knowledge, skills and abilities, as well as individual attributes and work experience that contribute to enhanced employee performance and ultimately result in organizational success [5]. Knowledge is the cognizance of facts, truths and principles gained from formal training and/or experience. A skill is a developed proficiency or dexterity in mental operations or physical processes that is often acquired through specialized training; using the skills results in successful performance. An ability is the power or aptitude to perform physical or mental activities that are often affiliated with a particular profession. The ability to

adfa, p. 1, 2018.

apply knowledge and skills in a productive manner, which can be characterized by such behavioral attributes as aptitude, initiative, willingness, communication skills, team participation, leadership and others, shows the professional's effectiveness.

The goal of this paper is to describe our experience in forming the students' abilities and teamwork skills based on the implementation of a comprehensive course project for developing the IS Maintenance System (ISMaS) for a specific object to be protected. To achieve this goal, the process model of ensuring IS is considered, the regulations for the course project implementation are described and the results of implementing these regulations are analyzed on the example of training Bachelors, Masters and Specialists in the field of IS at the NRNU MEPhI (Russia).

2 RELATED WORK

The efforts to develop a common approach to the formulation of requirements for IS competencies are being made worldwide for a long time. For example, an attempt to define a set of information and its structure, which created a basis for understanding terms and competencies in a particular knowledge area, was made in [6, 7]. The first steps to develop a common point of view refer to the World International conferences on IS Education (WISE) in the late 1990s – early 2000s. As a continuation, we have already presented our analysis of the three current basic approaches (American, Australian and European) [5, 8]. At the same time, several models of competency requirements for different organizations (such as CISA, CISSP, GIAC, etc.) have been developed for the certification of IS professionals.

For all available information sources, a common feature is answering "What is the formulation of a specific attribute of a specific professional competence?" question. They do not answer "How to form a professional competence?" question. We see two reasons why. On the one hand, the formation of the level of such attributes as "knowledge" and "skills" is well tested in the framework of traditional training forms: lectures, classes (seminars and labs) and students' independent work [5]. For example, for the "knowledge" attribute, one can use the recommendations of the SANS Institute [9]. On the other hand, there are some difficulties in the formation of the "skills" attribute in the framework of the typical educational process. The latter factor confirms the relevance of the results presented here. They should be considered as a continuation of our research on IS professional competencies presented in [5].

As for the other universities, which teach the full-time (not online) "IS Management" discipline, one can name the Norwegian University of Science and Technology (Norway), the City University of London (UK), the University of Pretoria (South Africa), the Eastern Kentucky University (USA), etc. But their Professors' publications do not describe any detail of the formation of abilities within this discipline.

3 IS ENSURING PROCESS MODEL

In this paper, the term "*IS of an object*" refers to the state of the object's security against threats in the information sphere (formed on the basis of [10-13]). The *object*

itself can be an information asset, IT or informatization object (object of applying IT to the main business processes of a particular organization such as an information system, automated system, automated process control system, etc.). To ensure this state is possible when performing specific actions, corresponding to a set of processes. This involves the following important terms. *Ensuring object's IS* (EIS) refers to the processes of maintaining the secure state of the EIS object. The *IS maintenance system* (ISMaS) is a set of corresponding EIS processes and IS controls, as well as the resources supporting them. In the Russian language the "maintenance" term is essentially broader than "management" as it means "ensuring" in all its possible senses, including corresponding system, staff, tools, documentation, procedures, etc.

Herein, the key terms are "a process" and "the process approach" [14]. A *process* is a set of interrelated and/or interacting activities, which are used to obtain the intended result. The *process approach* relates to a situation, where successive and predictable results are achieved more effectively and efficiently, and the activities are realized and managed as interrelated processes within a coordinated system. To structure all the processes, the cyclic Shewhart-Deming model or the Plan-Do-Check-Act (PDCA) cycle is traditionally used [15]. The PDCA cycle's application in various fields allows the effective management of activities on a systemic basis. This cycle can be applied within each organization's high-level process, as well as the separate production processes, and also the complete system of processes. It is closely connected with the planning, implementation, management and continuous improvement of both the organization's business processes and other processes related to its activities, including the EIS processes.

Each process as an integral part of the ISMaS must be appropriately managed. Any managerial action is also a process. It is aimed at ensuring the proper completeness and quality of the process, to which the managerial action is directed. Therefore, two groups of processes should be identified: the processes ensuring IS and the processes of their management. Their connectivity allows combining them into two systems: the IS System (ISS) (integrates the processes ensuring IS) and the IS Management System (ISMS) (integrates the management processes) [16, 17]. The *ISS* is a set of EIS processes, IS controls and resources needed to implement them. The *ISMS* is a set of management processes aimed at ensuring the completeness and quality of EIS processes (designed to plan, implement, monitor and improve the EIS processes), IS controls and resources supporting them. The ISMS should be considered as a part of the object's management system and it is aimed at planning, implementing, monitoring and improving the ISMaS. The PDCA cycle is applicable for both ISMaS management as a single process and for managing a separate ISS process.

The first group of ISMS processes forms four directions: planning, implementing, monitoring and improving the ISMaS as a single process. In this paper, only the "Planning" IS management processes are considered to determine the input and output data for separate components of the object's ISMaS as a single process. This direction unites all the processes which are necessary for the transition to the "Implementation" direction. In its essence, the "Planning" direction provides the ISMaS development.

In accordance with the recommendations of [10, 18-21], eight related subprocesses performing the ISMaS planning can be proposed (Fig. 1): "Object description", "Asset

identification", "IS threat analysis", "Choice of IS threats", "IS threat description", "IS risk treatment", "IS Policy development", "Development of internal IS documents". In [13] we describe all of them in detail and so do not repeat this here. The connection between these subprocesses is due to the fact that the results of implementing any of them in the form of output data are the input data for the subsequent subprocess.

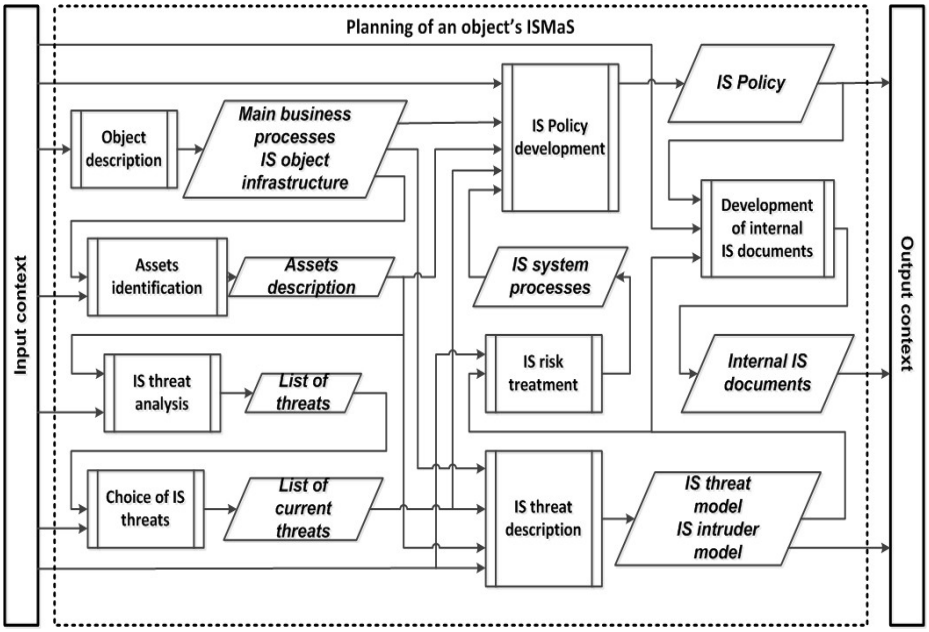

Fig. 1. Structural diagram for "Planning" of the ISMaS as a single process

The final result of designing the ISMaS for an individual object is its project documentation as a set of internal documents. An exemplary list of documents is the following [13]: "The list of the object's assets to be protected", "The list of the object's current IS threats", "The object's IS threats model", "The object's IS intruders model", "The object's IS risks registry", "The object's IS Policy", "The private IS policies related to the specific EIS processes at the object".

To obtain abilities in designing the ISMaS, a student must participate in designing all ISMaS subprocesses (Fig. 1).

4 OUR REGULATIONS FOR FORMING THE ABILITIES

Within the educational process for a specific curriculum, the ISMaS processes can be studied within the "IS Management" discipline. Traditional forms of discipline mastering (lectures, seminars) do not allow to fully form the abilities of each student to develop all the above-mentioned ISMaS subprocesses. In this case, an additional educational form such as an execution of a course project entitled "Designing the ISMaS for a specific object" is proposed. The number of subprocesses (8) requires a team of

executors (students) to perform the course project successfully. Our regulations of the course project's implementation is shown in Fig. 2. Let us consider them in detail.

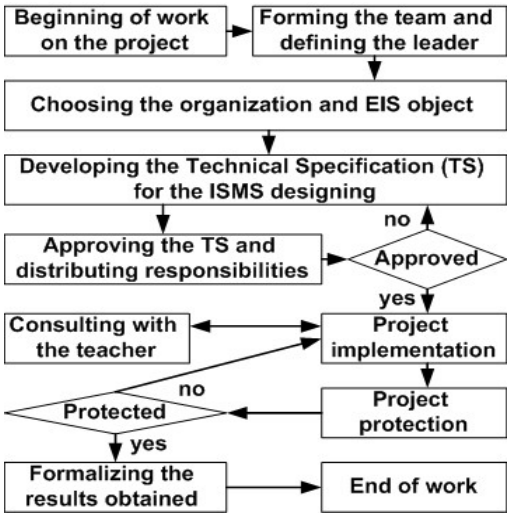

Fig. 2. The regulations for forming the abilities

1. *The beginning of work on the project* is determined by the completion of study the modern EIS approach, based on the process model. At the lectures students gain knowledge on the basics of IS management, and at the seminars they form their abilities and skills to apply the process approach to the ISMaS development. Thus each step of the regulations forms certain abilities corresponding to this particular step.

2. *The forming of the teams for individual course project's execution*. Students are distributed to separate teams voluntarily, taking into account the relations established in their groups. The number of students in one team is determined by the specifics of curriculum for training professionals (this issue is discussed in Section 5), qualification requirements for graduates, as well as the requirements of the discipline's syllabus. It is necessary to determine a team leader, whose duty is to coordinate work of all team members. The choice of the team leader is best entrusted to the team members. If there is a problem with this choice, it is made by their teacher.

3. *The choice of an organization and EIS object* is carried out by each team independently within the parameters set by their teacher with his/her consultative support. Students get the main recommendations for that at the seminars. For the given approach, students are recommended to choose as their EIS objects some organization's part, which deals with automated information processing under IS threats in the information sphere. For the selection of such EIS objects, students must know how to use IT for automated information processing.

4. *The development of the Technical Specification* (TS) for the ISMaS design. In the TS, the ISMaS requirements, structure and project documentation, which should be developed as a part of the course project, are defined taking into account the organization's peculiarities (its main business processes) and the EIS object (IT used). In

this case, students should know the basic requirements for the TS writing and have the ability to use the relevant regulatory documents. In the collective implementation of this stage, students will gain the abilities in developing the TS document (the initial ISMaS design stage). At this stage, the precise duties and tasks for each team member are formulated.

5. *The TS approving and the distribution of responsibilities* are carried out at the seminar in the form of a talk with a slideshow by the leader of each team in the presence of students of the entire group, from which the separate teams are formed. During such seminars, the teacher organizes the active participation of all the students in discussing the results of the TS development by formulating questions to the acting team leader and making their comments. Based on the discussion of a specific TS and taking into account the comments made, the teacher decides whether to approve the TS or not. If the TS is not approved, the team should return to the TS development with its subsequent presentation. At this stage, students gain the abilities of public protection of their decisions, as well as the abilities to participate in discussions.

6. *The project implementation* consists of the steps, within which each team member performs his tasks in accordance with the TS approved at the previous stage and the structure of the associated ISMaS design subprocesses defined above (Fig. 1). The connections and recommended order of this process implementation are important.

The subprocess A "Object description" [13]. The results of its implementation are the descriptions of the organization's main business processes and the EIS object's infrastructure. Understanding the importance of the reliability and completeness of the description of the organization and the EIS object allows recommending all team members to take part in the implementation of this subprocess. At the same time, students gain the abilities in the analysis of specific EIS objects.

The subprocess B "Asset identification" [13] is intended for the description of the EIS objects, ensuring IS of which should be done by the ISS processes. Such objects are assets that are valuable to the organization and relate to the EIS object and to the main organization's business processes. Assets include information assets (open (public) information and restricted access information) and assets related to the processing environment (software and hardware components of the EIS objects). The subprocess's input data is the output of the previous subprocess A. The output of the subprocess can be issued as a separate document: 1) Linking the asset to a specific main business process implemented by the organization and to the EIS object's infrastructure; and 2) The asset description (its type, vulnerabilities and IS properties to be protected with their priorities if possible). During the subprocess implementation students gain the abilities to identify the objects (assets) to be protected and describe there IS-related characteristics.

The subprocess C "IS threat analysis" [13] is intended for the formation of a preliminary list of IS threats typical for the EIS object as a part of the organization. Each IS threat is associated with a separate asset and with the possibility of disrupting its IS properties that can cause damage to the organization. The subprocess's input data is the output of the subprocess B. Within the subprocess, the expert assessments based on the experience of ensuring IS for similar objects, as well as the expert assessments of applicability of typical IS threats listed in some normative documents or published

in various sources are used. The expert assessment of this information allows determining a preliminary list of IS threats for the selected EIS object. The output data of the subprocess can be documented as "The preliminary list of IS threats to the assets of the EIS object". During the subprocess implementation students develop the abilities to assess IS threats specific to the selected EIS object, using various sources.

The subprocess D "Choice of IS threats" [13] generates a list of current IS threats specific to the EIS object of a particular organization. The subprocess's input data is the output of the subprocess C. For the selection of IS threats, the methodology for assessing the IS risks is used. Students get recommendations for using specific methods at the seminar, taking into account the provisions of ISO/IEC 27005 [21]. This method allows to determine the value of acceptable risk of violating the organization's main business processes (the so-called "risk appetite"), to assess the risks for each IS threat from the preliminary list of IS threats (subprocess C), and form a list of current IS threats, for which their risks exceed the risk-appetite. The result of the subprocess implementation is documented as "The list of current IS threats to the EIS object". Students develop the abilities to assess the risks of implementing IS threats for the selected EIS object.

The subprocess E "IS threat description" [13] is intended for the development of the IS threat and IS intruder models for the EIS object. The subprocess's input data is the output data of the subprocesses A, B and D. The description of IS threats to the assets of the EIS object can be performed in accordance with the recommendations [21], which for each IS threat from the list of current IS threats assume the definition of IS threat sources and method of its implementation, the asset (assets) to which this IS threat is directed, and the consequences of its implementation for these assets, as well as the damage to the main organization's processes. Within the subprocess, the quantative value of risk for each IS threat must be calculated. This description should be done in "The IS threats model for the EIS object". If the IS threat's source is an intruder, the IS threat description should be supplemented with his description. At the same time, for each IS intruder its type (external/internal), the asset affected by him, the level of access to the assets and the way of influencing them, his motivation, qualifications and resources available should be determined. The description of IS intruders is presented in "The IS intruders model for the EIS object". It should be noted that the structures and contents of both models must be consistent and not contradictory to each other. When implementing the subprocess, students gain the abilities to develop the models of IS threats and intruders for the selected EIS object.

The subprocess F "IS risk treatment" [13] is designed to select IS controls, which implement separate EIS processes related to the ISS and reducing IS risks to an acceptable level. The subprocess's input data is the output of the subprocess E. Within the subprocess, for each current IS threat the EIS processes (the ISS is formed) and the IS controls, which form these processes, are selected with the assessment of residual IS risks. The process of their selection continues until the residual IS risk will be not higher than the risk appetite. The results of the subprocess implementation are formalized in "The IS risks registry", where the selected EIS processes, IS controls and the levels of initial and residual risks are shown for each IS threat. During the subprocess implementation, students gain the abilities to select the specific processes,

IS controls for the real-world EIS objects, as well as the abilities to use some methodology for assessing the IS risks.

The subprocess G "IS Policy development" [13] is aimed at the development of the "The object's IS Policy" document (this is the output of the subprocess) as a normative document, which defines the requirements for EIS, the system of measures or the procedures for actions, as well as the responsibility of the organization's employees and control mechanisms for the defined area of EIS. The subprocess's input data is the output data of the subprocesses A, B, D, E and F. During the seminars, students develop the ability to define the structure and formulate the requirements for the IS Policy's content. When implementing the subprocess, the abilities to develop the "The object's IS Policy" are gained.

The subprocess H "Development of internal IS documents" [13]. The subprocess's input data is the output data of the subprocesses E, F and G. The nomenclature of the documents being developed is defined in "The object's IS Policy" and the TS for the ISMaS development. This set of documents should contain normative documents with the requirements for all EIS processes, as well as the implementation, operation, monitoring and improvement of the ISMaS. The results are presented as the private IS policies, regulations, instructions, etc.

7. *The project protection* is carried out at the seminar at least 4 weeks prior to the last class of the semester in the form of a talk by all team members performing the course project, with a slideshow in the presence of students of their group. During such seminars, the teacher organizes the active participation of all students in discussing the results of the project by formulating questions and commenting. Based on the results of the discussion of a particular course project and taking into account the comments made, the teacher decides whether to approve or not the project's results. In the second case, the team must return to the course project's implementation with subsequent re-protection, but exactly in the time limits of the semester, during which the course project is carried out. At this stage, students gain the abilities of public protection of their decisions, as well as the abilities to participate in their discussion.

8. *The formalization of the project results obtained* is the final stage. Every team prepares a Report consisting of separate Chapters, containing reports of each team member reflecting his/her contribution to the overall course project. In the "Introduction" section, the team leader characterizes and assesses the contribution of each team member to the course project's implementation. In each section, its executor should provide information on how the specific process has been implemented, which normative documents have been used, and how its connections with the other subprocesses have been taken into account. If the result of execution of a part of the course project is a draft of some internal IS document, then it must be written in accordance with the existing norms for such type of documents. In general, the Report should be written taking into account the requirements for design documentation. The Report is supplemented by a slideshow, used by students during their course project protection. Taking into account the results of the TS approving and the protection of the course project's results, as well as the quality of the Report and the activity of students in the course project's implementation, the teacher assesses the work of each student performing the individual course project.

After all the students expressed a unanimous opinion that this method of consolidating the theoretical knowledge obtained was very useful and interesting for them.

5 OUR EXPERIENCE IN FORMING THE ABILITIES

The described approach in forming the abilities in ISMaS designing has been tested for 3 years at the NRNU MEPhI within the following curricula in IS: for Bachelor (annual recruitment of 1 student group (B1) of 20 students); Masters (4 groups of 20 students each) and Specialists (Engineers) (4 groups of 20 students each).

Bachelors' training is conducted according to the "Automated Systems Security" educational programme. Masters' training is conducted in four programmes: "Application of Cryptology Methods in ISMS" (M1); " IS Maintenance for Key Information Infrastructure Systems" (M2); "Business Continuity and IS Maintenance" (M3) and "Information and Analytical Support of Financial Monitoring" (M4). Training of Specialists is conducted in two specialities: "IS of Automated Systems" (ISAS) and "Information and Analytical Security Systems" (IASS).

The NRNU MEPhI carries out training within the framework of the approved educational standards, competence models of graduates, curricula and programs of educational disciplines. The educational standards and competence models of graduates formulate professional competencies related to the ISMS design. According to them, a graduate after graduation should have the following abilities [5]:

- *Bachelor*: To participate in the IS policy implementation; To conduct analysis of the source data for designing the EIS subsystems and tools; To formalize working technical documentation taking into account existing normative and methodical documents;
- *Master*: To assess risks, formulate an IS Policy for the objects to be protected; To develop the EIS systems, complexes, tools and technologies; To carry out the justification of composition, characteristics and functionality of the EIS systems and tools for the objects to be protected on the basis of the Russian and international standards; To organize IS management; To develop drafts of organizational and administrative documents, business plans in the field of professional activity, technical and operational documentation for the EIS systems and tools;
- *Specialist (ISAS)*: To develop and analyze design solutions to ensure IS for automated systems (ASs); To develop an IS policy for AS; To participate in the design of the ISMS for AS; To develop proposals for improving the ISMS for AS; To develop drafts of documents regulating the EIS activities for AS; To participate in the formation of the organization's IS Policy and to monitor the effectiveness of its implementation; To manage IS for AS;
- *Specialist (IASS)*: To identify the main IS threats, to build and investigate the intruders models for computer systems; To carry out the selection of technology, tools, computer facilities and EIS tools for the creation of special Information and Analytical Systems (IASs); To develop drafts of normative, methodological, organizational and administrative documents regulating the functioning of special IASs and their EIS tools.

Each of the above curricula contains the "IS Management " discipline. But its content differs in accordance with a different set of professional competencies. As a result, a different set of abilities must be formed when training Bachelors, Masters and Specialists. Thus, the course projects as the obligatory part of the different curricula relate to the implementation of a limited set of ISMS design subprocesses (or to the partial design of the ISMaS). From the analysis of their lists of professional competencies it follows that the formation of the abilities while training Bachelors, Masters (M1 and M4 programmes) and Specialists (IASS speciality) can be limited to the development of IS threats and intruders models for a particular EIS object. A full set of subprocesses should be included in the course projects for training Masters (M2 and M3) and Specialists (ISAS speciality). In this case, it was considered advisable to develop within the course projects only one private IS Policy for the M2 programme (for example, the IS Incident Management Policy), 2-3 private IS policies for the M3 programme (for example, the IS Incident Management Policies, Internal/External IS Audit or IS self-assessment Plan, Continuity Policy for the EIS object) and 3-5 internal IS documents for the ISAS speciality (for example, the Regulations on the implementation of specific IS controls).

Table 1 shows the relationship of the listed ISMaS design subprocesses with the course projects for the given curricula ("+" and "-" mean that the subprocess is included or not included in the course project respectively; "+", "++" and "+++"reflect the different number of internal IS documents for subprocess H).

Table 1. ISMaS design subprocesses in different NRNU MEPhI's curricula

Subprocess	*Curriculum*						
	Bachelor	*Master*				*Specialist*	
	B1	*M1*	*M2*	*M3*	*M4*	*ISAS*	*IASS*
A "Object description"	+	+	+	+	+	+	+
B "Asset identification"	+	+	+	+	+	+	+
C "IS threat analysis"	+	+	+	+	+	+	+
D "Choice of IS threats"	+	+	+	+	+	+	+
E "IS threat description"	+	+	+	+	+	+	+
F "IS risk treatment"	-	-	+	+	-	+	-
G "IS Policy development"	-	-	+	+	-	+	-
H "Development of internal IS documents"	-	-	+	++	-	+++	-
Number of team members	3	3	5	6-7	3	6-8	3

Our analysis of the content and scope of students work in the implementation of individual subprocesses allows recommending the following distribution of the subprocesses according to the executors (E) of the course projects (members of one team): E1: A and B; E2: C and D; E3: E; E4: F and G; E5: H: Development of one private IS Policy; E6: H: Development of several documents for the implementation of various IS controls. The number of internal IS documents, being developed by one executor, must be agreed with the teacher in advance. With this in mind, the recommended number of executors in the team implementing the course project will depend on the subprocesses, the implementation of which is included in it. The corresponding numbers are given in the last line of Table 1.

6 CONCLUSION

Studies aimed at applying modern methods of forming students' professional abilities in a certain field of activity are relevant not only for science, but also of great practical importance. Their usage makes it possible to increase the effectiveness of educational process and to provide graduates of educational institutions with all necessary conditions for the acquisition of modern professional competencies. In this paper, we shared our experience in the development and practical use of the regulations for forming the abilities to design the ISMaS for individual objects and teamwork skills (for example to break the task down into steps, plan a strategy, manage time, handle issues that only arise in groups such as delegate responsibilities, listen to alternative ideas, resolve conflicts and reach consensus, coordinate efforts, integrate the contributions of multiple team members, etc.) based on the implementation of the course projects. For that purpose, we created the different versions of regulations, allowing to take into account the peculiarities of curricula for training professionals in the field of IS of various levels (Bachelors, Masters and Specialists).

Our approbation of these versions revealed certain findings that must be taken into account when improving the educational process at the NRNU MEPhI. The most important of them is the significant increase in the study time attributed to the students' independent work, which is needed for the course project's implementation. Secondly, the teacher's role in individual consulting of students is expanded. Thirdly, it is necessary to create conditions for teamwork of students to perform their course projects and publicly protect the results obtained, taking into account the combination of features of teamwork and individual responsibility for their part of the whole work.

In this regard, there is a need to develop tools that improve the efficiency of ISMaS design processes for individual objects. For example, the creation of databases of typical assets' vulnerabilities of considered objects to be protected, IS threats, EIS processes and organizational and technical IS controls, the development of templates for documents related to the ISMaS design, as well as the use of visualization tools for the ISMaS design processes (such work has already been started by us in [13]).

Further development of this work is aimed at the improvement of our educational process, taking into account the identified factors, as well as the development of tools for designing the ISMaSs.

Acknowledgement. This work was supported by the MEPhI Academic Excellence Project (agreement with the Ministry of Education and Science of the Russian Federation of August 27, 2013, project no. 02.a03.21.0005).

7 REFERENCES

1. EN 16234-1:2016 "e-Competence Framework (e-CF) – A common European Framework for ICT Professionals in all industry sectors – Part 1: Framework" and CEN/TR 16234-2:2016 "… Part 2: User Guide".
2. Newhouse W., Keith S., Scribner B., Witte G. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. August 2017. URL: https://doi.org/10.6028/NIST.SP.800-181 (accessed: 22.06.2018).

3. Cybersecurity Curricula 2017. Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. Version 1.0. Report by ACM, IEEE, AIS, IFIP. 31 December 2017. URL: http://cybered.acm.org/ (accessed: 22.06.2018).
4. 2016 Cybersecurity Skills Gap. ISACA. http://www.isaca.org/cyber/PublishingImages/Cybersecurity-Skills-Gap-1500.jpg (accessed 22.06.2018).
5. Miloslavskaya N., Tolstoy A. Designing Degree Programmes for Bachelors and Masters in Information Security. In: Bishop M., Futcher L., Miloslavskaya N., Theocharidou M. (eds) Information Security Education for a Global Digital Society. WISE 2017. IFIP Advances in Information and Communication Technology, Vol. 503. Springer. Pp. 14-26.
6. Bishop M., Engle S. Software Assurance CBK and University Curricula. 10th Colloquium for Information Systems Security Education. University of California at Davis, USA (2006). URL: http://nob.cs.ucdavis.edu/bishop/talks/2006-cisse-1/swacbk.pdf (accessed 22.06.2018).
7. Theoharidou M., Gritzalis D. Common body of knowledge for information security (2007). IEEE Journal Security & Privacy. Vol. 5, iss. 2, pp. 64-67.
8. Miloslavskaya N., Tolstoy A. ISO/IEC Competence Requirements for Information Security Professionals. In: Bishop M., Futcher L., Miloslavskaya N., Theocharidou M. (eds) Information Security Education for a Global Digital Society. WISE 2017. IFIP Advances in Information and Communication Technology, Vol. 503. Springer. Pp. 135-146.
9. Yusof A. Ways To Become An Effective Information Security Professional - From A GIAC Wannabe Perspectives. SANS Institute InfoSec Reading Room. Version: 1, 2001. URL: https://www.sans.org/reading-room/whitepapers/infosec/ways-effective-information-security-professional-giac-wannabe-perspectives-601 (accessed 22.06.2018).
10. ISO/IEC 27000:2018 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary.
11. Kissel R. Glossary of Key Information Security. Terms. NIST Interagency/Internal Report (NISTIR). 7298rev2. May 2013. URL: https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=913810 (accessed 22.06.2018).
12. GOST R 50922-2006 Information security. Main terms and definitions (In Russian).
13. Miloslavskaya N.G., Tolstoy A.I. Visualization of Information Security Management Processes. Scientific Visualization Journal. 2017. Vol. 9, N 5, pp. 117-136. URL: http://sv-journal.org/2017-5/10.php?lang=en (accessed 22.06.2018).
14. ISO 9000:2015 Quality management systems -- Fundamentals and vocabulary.
15. Deming W.E. Out of the Crisis. Cambridge, MA: MIT, 1986.
16. Bank of Russia Standard STO BR IBBS-1.0-2014 Information Security Maintenance for Organizations of the Banking System of the Russian Federation. General Conditions (In Russian).
17. GOST R 57580.1-2017 Security of financial (banking) operations. Protection of information of financial organizations. Basic composition of organizational and technical measures. URL: http://www.cbr.ru/eng/analytics/Gubzi_docs_en/st-10-14_en.pdf (accessed 22.06.2018).
18. ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements.
19. ISO/IEC 27002:2013 Information technology -- Security techniques -- Information security management systems – Code of practice for information security controls.
20. ISO/IEC 27003:2017 Information technology -- Security techniques -- Information security management systems – Guidance.
21. ISO/IEC 27005:2011 Information technology -- Security techniques -- Information security risk management.