



Formation of General Professional Competencies in Academic Training of Information Security Professionals

Natalia Miloslavskaya, Alexander Tolstoy

► To cite this version:

Natalia Miloslavskaya, Alexander Tolstoy. Formation of General Professional Competencies in Academic Training of Information Security Professionals. 14th IFIP World Conference on Information Security Education (WISE), Jun 2021, Virtual, United States. pp.13-26, 10.1007/978-3-030-80865-5_2. hal-03739150

HAL Id: hal-03739150

<https://inria.hal.science/hal-03739150>

Submitted on 27 Jul 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

Formation of General Professional Competencies in Academic Training of Information Security Professionals

Natalia Miloslavskaya^[0000-0002-1231-1805] and Alexander Tolstoy^[0000-0001-9265-1510]

The National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
31 Kashirskoye shosse, Moscow, Russia
{NGMiloslavskaya, AITolstoj}@mephi.ru

Abstract. The research results of competencies and competence models of professionals in the Information Security (IS) field are presented. The group structure of competencies, which form a Competency Model (CM) for IS professional academic training, has been determined. The fundamental difference between the academic community's and the professional community's CMs is shown. The urgency of a general professional competencies' (GPCs) group formation during IS academic training is shown. A group structure model, in which specific subgroups are identified, is proposed. The relevance of the study of the first (so-called basic) level of subgroups of general educational competencies is determined. They are versatile across a variety of academic training programmes. Basic GPCs are formulated, and their characteristics are determined. The training modules, with their annotations and labor inputs, are described as parts of academic disciplines. The validity of the results obtained is confirmed by the positive experience in developing competencies and CM in the framework of training IS professionals on the specific educational programmes at the National Research Nuclear University MEPhI (Moscow Engineering Physics Institute) (Moscow, Russian Federation).

Keywords: information security, academic training, competency model, competence characteristics, knowledge, skills, competence groups, training module, academic discipline

1 INTRODUCTION

Research shows [1-6] that competencies and Competency Models (CMs) are important elements of HR systems in any professional community of educational systems, which includes the educational community and professional certification systems.

Currently, there are a large number of definitions of the "competency" term [1-6]. For completeness of the paper's topic consideration, we will focus on the following definitions:

Competency is the ability of a subject (person) to apply knowledge and skills to achieve the desired results [7];

CM is the structured sets of necessary, identifiable, and measurable competencies [1].

Existing approaches to the CM development take into account the scope (areas and types) of professional activity, as well as the application direction for such models. For example, for the cybersecurity sphere, the most interesting is the CM presented in the report of the Apollo Education Group, Inc and University of Phoenix [6, 8] and based on the CM classification developed in the Department of Labor (US). It is divided into nine levels, forming three clusters [9, 10].

An analysis of such a system of competencies shows that there can be many CMs. In this case, problems arise in the practical use of these CMs. Each problem is associated with a specific context of their application.

This paper highlights the problem associated with the coordination of CMs developed by the academic community (competencies of all three clusters and eight levels of classification [9, 10]) and CMs existing in the professional community (third cluster, 5-8 levels of classification [9, 10]).

Fig. 1 shows a structure that explains the links between competencies and CMs related to different communities.

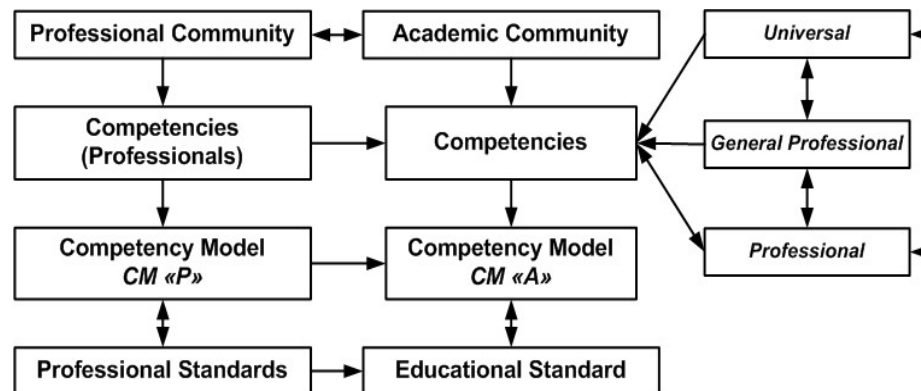


Fig. 1. The structure of links between competencies and CMs

The professional community formulates the competence requirements for professionals that are in demand in a specific professional field (for example, in the IS field) in the form of Professional Competencies (PCs) that form the basis of the corresponding CM (for example, the basis of professional standards as it is done in Russia [11]).

Academic training should be aimed primarily at satisfying the labor market in professionals with PCs formulated by the professional community. Therefore, the PCs included in the CMs related to academic training (CM "A") are directly related to the PCs from the CM "P" related to the professional community (Fig. 1).

To form specific PCs, students must have certain basic competencies. A group of universal competencies and a group of general professional competencies (GPCs) can be distinguished among them. From this follows the conclusion about significant differences between CM "A" and CM "P" (Fig. 1).

The purpose of this paper is to investigate the features of the competencies related to the academic training of IS professionals. The structure and dynamics of the formation of such competencies. The structure of groups of general PCs and PCs are

determined. The basic general PCs are formulated. The training modules designed to implement basic general PCs are described.

2 Basic concepts and definitions

Before formulating general PCs in the academic training of IS professionals, it is necessary to make the following remarks.

1. The concept defined by the "IS" term requires clarification. In the context of this paper, we will use two concepts defined by this term: in its broad and narrow senses.

IS in a broad sense is an area of professional activity as a field of science, engineering and technology, covering a set of problems associated with the provision (preservation) of specific properties of an object (called the IS properties). The definition is of a general conceptual nature and has no practical significance.

IS in the narrow sense is some entity that has practical significance, for example, for the subject of this paper, competence requirements for IS professionals. Most often this concept is defined as follows [7]: IS is the preservation of confidentiality, integrity and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

2. It should be noted that the above definition of the IS term in a narrow sense raises some questions, to which the definition does not answer. For example, storing properties of information is an information-related process. This process should involve a specific object (or environment) to which this information belongs. Nothing about this is said in the definition of the term. Thus, the existing IS term definition [7] makes it difficult to interpret it unambiguously.

In the Russian-language standard, you can find the definition of the IS regarding such an object as "organization" [12]:

IS of an organization is the state of protection of the organization's interests in the face of threats in the information sphere. Herewith, protection is achieved by ensuring a set of IS properties such as confidentiality, integrity, availability of information assets and the organization's infrastructure. The priority of IS properties is determined by the importance of information assets for the interests (goals) of the organization.

This definition uses such terms as "organization" (IS object), "state of protection", "information sphere", "asset", "threat" and "IS properties" that does not contradict the modern approach to ensuring IS, which is outlined in the ISO/IEC 27000 series.

3. As a generalization and development of such an interpretation of the IS term, it is proposed to use the following terms and definitions:

IS an object (object's IS) is the state of protection of the object's assets from threats in the information sphere, in which damage to the object's assets and the object itself will not exceed the permissible level. The state of protection is achieved by ensuring the set of IS properties of the object's assets such as availability, integrity, confidentiality, non-repudiation, reliability, authenticity, and accountability.

Information sphere is a set of information, objects, information processing objects (information systems, automated systems, information technology (IT) objects, communication networks), IT, subjects whose activities are related to the formation and

processing of information, the development and use of these technologies, IS ensuring, as well as a set of mechanisms for regulating the relevant public relations.

Ensuring object's IS is the implementation of the process (processes) of ensuring such a state of protection of the object's assets from threats in the information sphere, in which the possible damage to the object's assets and the object itself from the implementation of threats will not exceed the permissible level.

These definitions more clearly describe the concept to which the IS term refers. It allows for a well-grounded structuring and description of the competency's characteristics of IS professionals.

3 Competency model "A" and competencies structure

In the CMs of the academic community, three groups of competencies are distinguished: universal (UCs), general professional (GPCs), and professional (PCs) (Fig. 1).

The first group (UCs) includes competencies that are weakly dependent on the direction of professional training. They belong to the first cluster and the first three levels of classification [9, 10]. An example of the UCs, which a graduate of an educational institution who has mastered Bachelor's and Master's degree programmes in IS, can be found in [12].

The second group (GPCs) includes competencies that are directly related to the area of professional activity. These competencies belong to the fourth and fifth levels, united in the second cluster of the well-known classification [9, 10]. Moreover, these GPCs have a certain level of universality within a specific field of training: they will be the same for various educational programmes. The GPCs importance for a specific field of academic training explains the choice of research topic, the results of which are presented below.

The third group (PCs) includes competencies directly related to PCs described in the corresponding CM of the professional community (CM "P").

In academic training, the GPCs definition should take into account educational levels (Bachelor, Master) and the professional educational profile (PEP).

All three groups of competencies are interconnected taking into account the levels of their formation (Fig. 1).

These facts confirm the validity of the statement made that the CMs used by the academic community have significant differences from the CMs used by the professional community. It should be noted that these features can be reflected in educational standards for the academic training of IS professionals (Fig. 1), as it is done in the Russian Federation [13].

4 Structure of groups of GPCs and PCs

In the academic training of professionals (including in the IS field), not only PCs but also GPCs are important. The presence of the latter is mandatory for students in the formation of PCs.

To divide the competencies into GPCs and PCs, it is necessary to determine the separation criterion. In this case, we can propose an approach, which was used to determine the initial data for the CMs development [1]. Such initial data are the area, objects, types, and tasks of professional activity.

In addition to these initial data, the following factors must be taken into account:

1. IS as an area of professional activity (PA) is a set of sub-areas that have their own specifics in relation to PA objects, types, and tasks. Such sub-areas will include the areas of IS and information protection (IP), the area of cyber security (CS) and the area of IS of socio-technical (ST) objects, as well as other sub-areas are possible. Each sub-area of the PA defines a PEP).
2. PA objects, types and tasks can be typical for the entire area of IS (T1), typical for a certain sub-area (T2) and specific for a specific PEP.
3. Processes and measures for ensuring IS and IT are typical (T1) for the PA area (IS), typical (T2), specific for PEP.
4. The methodology, methods and techniques for ensuring IS can relate to the entire area of IS (Methodology), to a specific PA sub-area (Methods 1, 2, 3) for the sub-areas of IS, CS and ST IS) and to a specific PEP taking into account a specific PA sub-area (Techniques 1, 2, 3).
5. The formation of PCs should also be based on GPCs related to the fundamental sciences. For example, mathematics, physics and information theory, as the basis for the formation of systems thinking in trainees (F1), special chapters of mathematics, physics and electronics, necessary in some cases to understand and describe the processes and measures for ensuring IS, as well as the description of IT (F2).

The initial data and the factors highlighted above are combined and presented in Table 1.

Table 1. Selection criteria for GPCs and PCs

PA area/ sub-area	PA object, types and tasks	Processes and measures	IT	Methodology, methods and techniques	Fundamental area	GPCs / PCs
IS /	T1	T1	T1	Methodology	F-1	GPCs
/ IP	T2	T2	T2	Method1	F-21	GPCs
/ CS	T2	T2	T2	Method2	F-22	GPCs
/ ST IS	T2	T2	T2	Method3	F-23	GPCs
/ IP	PEP	PEP	PEP	Technique1	-	PCs
/ CS	PEP	PEP	PEP	Technique2	-	PCs
/ ST IS	PEP	PEP	PEP	Technique3	-	PCs

Analysis of the data from Table 1 allows us to divide the competencies into two groups (GPCs and PCs) and structure each of these groups with the assumption that these groups should be related to each other (Fig. 2). There are five subgroups in the GPCs group, each of which consists of two parts (two levels of competencies): GPC-A (GPC-A1 and GPC-A2), GPC-T (GPC-T1, and GPC-T2), GPC-P (GPC-P1 and GPC-P2), GPC-M (GPC-M1 and GPC-M2), GPC-F (GPC-F1 and GPC-F2). The first

parts include competencies that relate to the entire PA area – IS. The second parts combine the competencies related to one of the PA sub-area, which determines the PEP. Each of these subgroups (except for the GPC-F subgroup) combines competencies that reflect knowledge and skills about typical PA objects, types and tasks (GPC-A), typical IT used by typical PA objects (GPC-T), typical processes and measures to ensure IS (GPC-P), methodology (GPC-M1) and methods (GPC-M2) to ensure IS of typical objects (GPC-M).

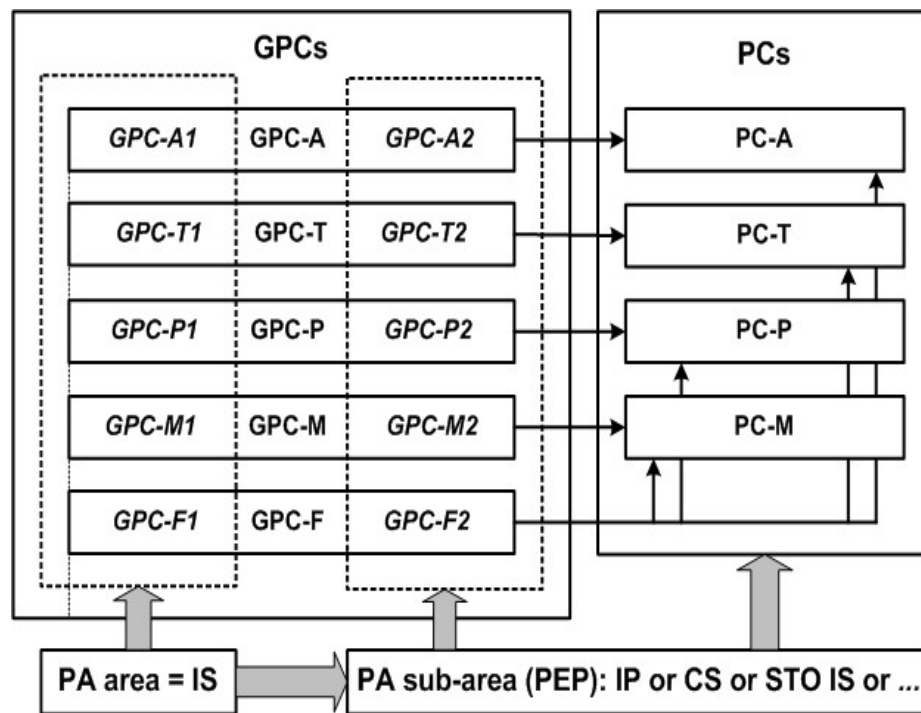


Fig. 2. The structure of groups of GPCS and PCs

The GPC-F subgroup contains competencies that are formed in the study of either the fundamental sciences, which include mathematics and physics (GPC-F1), or applied questions of mathematics, physics, electronics and electrical engineering (GPC-F2). The first level forms students' outlook and systemic thinking, and the second is necessary for the formation of PCs (Fig. 2).

The structure of the GPCs group may have some peculiarities related to the curriculum for training professionals. Firstly, the competencies related to the first level of the first four subgroups of the GPCs group will be universal in relation to educational levels (Bachelor, Master) and to the PEP in IS. Secondly, the range of second-level competencies of the first four subgroups will be different in Bachelors' and Masters' training. Thirdly, there will be no competencies of the first level subgroup GPC-F (GPC-F1) during Master's training, and the competencies of the second level of this subgroup may not exist.

The formation of PCs should take into account the selected level and profile of training of IS professionals and should be associated with specific PA objects, types and tasks, IT, processes, measures, and techniques of ensuring IS. Also, it should be borne in mind that PCs are directly related to GPCs. Based on this, we can make a reasonable conclusion that the structure of the PCs group should be close to the structure of the GPCs group (Fig. 2). The PCs group consists of four PC subgroups directly related to similar subgroups of the GPCs group. Each of these subgroups combines competencies that reflect knowledge and skills for specific PA objects, types and tasks (PC-A), specific IT used by specific PA objects (PC-T), specific IS processes and measures (PC-P), techniques of ensuring IS of specific PA objects (PC-M).

In the following, only GPCs related to the first level of subgroups GPC-A, GPC-T, GPC-P, and GPC-M will be considered. Since these competencies do not depend on the PEP for IS professionals and are common to the curricula for training Bachelors and Masters, they will be called the basic GPCs.

5 Basic GPCs

The analysis of the definitions of terms related to the IS concept in the narrow sense formulated in the paper explains why subgroups of competencies related to IS objects (GPC-A), IT (GPC-T), IS ensuring processes (GPC-P), and IS ensuring methodology (GPC-M) are identified in the structure of the GPCs group.

Let us consider the GPCs of the first level, included in the subgroups GPC-A1, GPC-T1, GPC-P1, and GPC-M1, related to the PA IS area (Fig. 2). First of all, those competencies were identified, from which the formation of the competency characteristics of the future IS professional (subgroup GPC-M1) begins – these are competencies that reflect knowledge and skills about the modern methodology of ensuring IS (competencies CM1.*). Further, the GPCs of the remaining subgroups were determined in the following order: GPC-A1 (CA1.*), GPC-T1 (CT1.*) and GPC-P1 (CP1.*). A complete list of GPCs of the first level are given in Table 2.

Table 2. GPCs of the first level (where I1 – index of the subgroup of competencies; I2 – index)

I1	I2	Competence. The graduate must be able to:
GPC-M1	CM1.1	Use effectively the terminology system related to the PA IS object
	CM1.2	Be guided in their practice by provisions from the legal and regulatory framework for ensuring IS
	CM1.3	Base their activities on modern IS ensuring methodology
GPC-A1	CA1.1	Describe typical PA areas
	CA1.2	Describe typical IS objects
	CA1.3	Describe the typical tasks of IS ensuring for typical IS objects
GPC-T1	CT1.1	Describe the typical IT used by typical IS objects
	CT1.2	Describe typical network technologies used by typical IS objects
	CT1.3	Describe typical technologies for creating and managing databases
GPC-P1	CP1.1	Describe typical IS ensuring processes that are applicable to typical GPCs
	CP1.2	Describe the standard IS ensuring measures implementing standard IS ensuring processes applicable to typical PA objects

The characteristics of GPCs of the first level are given in Table 3.

Table 3. GPCs characteristics (indicators) (where I2 – competence's index; I3 – characteristic's index)

I2	I3	Characteristics. The graduate must know (K1.*,*) / be able (S1.*,*)
CM 1.1	KM1.1	the basics of systematics (taxonomy) of IS concepts
	KM1.2	references of IS-related terms and their definitions
	KM1.3	IS-related terms and their definitions adopted by the professional community
	KM1.4	application features of IS-relates terms and their definitions
	SM1.1	to apply reasonable IS-relates terms and their definitions
CM 1.2	KM2.1	legal norms of the national legal system related to the IS field
	KM2.2	international regulatory framework related to the IS field
	KM2.3	national regulatory framework related to the IS field
	KM2.4	application features of legal and organizational norms related to the IS field
	SM2.1	to apply reasonable the legal and organizational norms related to the IS field
CM 1.3	KM3.1	fundamental security features
	KM3.2	the basics of the process approach to IS ensuring
	KM3.3	the basics of a risk-based approach to IS ensuring
	KM3.4	typical procedure for ensuring IS
	SM3.1	to define the procedure for ensuring IS of a typical PA object
	SM3.2	to define the requirements for IS ensuring stages of a typical PA object
CA 1.1	KA1.1	characteristics of PA areas
	SA1.1	to choose reasonable the PA area
CA 1.2	KA2.1	the basics of classification of PA objects
	KA2.2	typical characteristics of typical PA objects
	SA2.1	to describe a typical PA object
CA 1.3	KA3.1	typical IS ensuring tasks related to typical PA objects
	SA3.1	to formulate the requirements for ensuring IS of a typical PA object
CT 1.1	KT1.1	basic IT used in the implementation of typical PA objects
	ST1.1	to choose reasonable IT for the implementation of a typical PA object
CT 1.2	KT2.1	basic network technologies
	KT2.2	basics of classification of open information systems
	KT2.3	Internet technology basics
	ST2.1	to choose reasonable a network technology for the implementation of a typical PA object
CT 1.3	KT3.1	fundamentals of technologies for creating and managing databases
	ST3.1	to choose reasonable a technology for creating and managing a database for the implementation of a typical PA object
CP 1.1	KP1.1	fundamentals of systems engineering of IS ensuring processes
	KP1.2	features of typical IP processes
	KP1.3	features of typical IS management (ISM) processes
	SP1.1	to formulate requirements for typical IP processes
	SP1.2	to formulate requirements for typical ISM processes
CP 1.2	KP2.1	features of typical measures that implement typical IP processes
	KP2.2	features of typical measures that implement typical ISM processes
	SP2.1	to choose reasonable typical measures that implement typical IP processes
	SP2.2	to choose reasonable typical measures that implement typical ISM processes

6 Training modules for implementing basic GPCs

The basic GPCs description should be presented in the corresponding CM of the graduate being trained on a specific educational programme in IS with its curriculum. Training modules (TMs) are inserted into the curriculum separately or as part of some academic disciplines (ADs). Each TM/AD must have its syllabus and assessment of labor intensity (LI) in conventional units (CUs) (an analog of Credits). Since the implementation of a specific TM/AD is aimed at the formation of specific basic GPCs (in this case), the curriculum should establish a connection between the TM/AD and the corresponding competence.

At present, the National Research Nuclear University MEPhI (Moscow Engineering Physics Institute) (NRNU MEPhI) (Russia) has accumulated many years of experience in training professionals in this field on Bachelor's and Master's degree programmes. The corresponding CM can be found on the NRNU MEPhI website http://eis.mephi.ru/AccGateway/index.aspx?report_param_gosn=3&report_param_is_magister=true. The NRNU MEPhI carries out training within the framework of the approved educational standards, CMs of graduates, curricula and syllabus of educational disciplines. Bachelors' training is conducted under to the "Automated Systems Security" degree programme. Masters' training is conducted under four degree programmes: "Application of Cryptology Methods in ISMS"; "IS Maintenance for Key Information Infrastructure Systems"; "Business Continuity and IS Maintenance" and "Information and Analytical Support of Financial Monitoring". The papers [14] and [15] shares the NRNU MEPhI's experience in training Bachelors and Masters in IS. All these programmes are developed in accordance with the Professional standards of the Russian Federation for IS [16] and the Federal Educational Standards of the Russian Federation in the IS Direction [17]. A group of six Professional standards y formulate general and special labor functions that specific professionals can implement and requirements for the levels of knowledge and skills, corresponding to these labor functions and related to the levels of basic education and experience acquired in a practical field. These professional standards are used by organizations to create and implement their personnel management systems. A group of seven Federal Educational Standards is linked directly to these IS Professional standards. They formulate general competencies and general PCs and normalized the development of special PCs.

As a result of the generalization of this experience, the following TMs (index I4) were developed, intended for the formation of basic GPCs described: "Taxonomy Basis of IS concepts" (TBISC); "IS Legal and Regulatory Framework" (ISLRF); "Typical IS Objects" (TISO); "Fundamentals of Information Security Ensuring Methodology" (FISEM); "Information Security Ensuring Engineering" (ISEE); "Basic Information Technology" (BIT). TMs description, including an abstract (a short listing of the topics of the TM syllabus), is given in Table 4. In the curricula for IS Bachelor's and Master's training at the NRNU MEPhI, the above TMs are included in the following ADs: TBISC, ISLRF, TISO, FISEM and ISEE ($\Sigma LI=2CU$ s) and BIT ($LI=1CU$).

Table 4. Description of TMs intended for the formation of basic GPCs

I4	Abstract	LI	I2
TBISC	Taxonomy as a tool for the taxonomy of concepts. System of basic IS concepts. References to terms and their definitions. The term system for the IS field. Definitions and relationships of the concepts: "security", "IS", "IP", "cybersecurity", "socio-technical security"	0,25	CM1.1, CM1.2
ISLRF	Subject and content of the problem of legal and regulatory IS ensuring. Fundamentals of the legal and regulatory framework of IS ensuring in the Russian Federation. Technical regulation in the IS field. IS ensuring standardization: international standards, national standards, corporate standards. Features of the application of legal and organizational norms related to the IS field	0,25	CM1.1, CM1.2
TISO	Classification and general description of a typical IS object. Organization as an IS object. Information as an IS object. Classification of information. Assets of a typical IS object and their identification. Typical objects of automated information processing (information systems, automated systems, cyber security (CS) objects and socio-technical (ST) objects	0,5	CA1.2, CA1.3
FISEM	Conceptual framework for IS ensuring. PA objects and tasks of in the IS field. Fundamentals of IP methodology. Fundamental security features. Conceptual foundations of modern IS ensuring methodology (process approach; management approach; risk-oriented approach; role of IS incident management processes; management of control processes and business continuity processes).	0,5	CM1.1, CM1.2, CM1.3, CA1.1
ISEE	Process approach. Cyclic Shewhart-Deming model. IS Maintenance System of a typical object and its typical structure. Typical processes of the IP system. Typical IS Management (ISM) system of a typical object and its structure. Typical processes of the ISM system. Typical processes of the IP Management (IPM) system. Typical measures that implement typical processes of the IP system. Typical measures that implement typical IPM processes. Typical measures that implement typical ISM processes	0,5	CM1.3, CP1.1, CP1.2
BIT	Basic IT used in the implementation of standard PA objects and IS objects. The choice of IT for the implementation of a typical object. Basic network technologies. Fundamentals of classification of open information systems. Internet technology basics. The choice of network technology for the implementation of a typical object. Fundamentals of technologies for creating and managing databases. Selection of a typical technology for creating and managing databases for the implementation of a typical object	1,0	CT1.1, CT1.2, CT1.3
Total		3,0	

7 CONCLUSION

Analysis of modern approaches to the design of CMs in terms of defining competencies of various levels in the IS field, allowed us to obtain the following results:

1. The conceptual base related to the IS field was developed, which made it possible to structure the PA areas, objects, types, and tasks. These data served as the basis for the study of competencies.

2. The structure of the groups of competencies that form the CMs of IS professional academic training has been determined. Its comparison with the structure of competencies related to CMs used by the professional community is carried out. Their fundamental differences are shown.

3. The relevance of the GPCs group formation for the academic training of IS professionals is shown. A model of the structure of this group is proposed, in which specific subgroups are identified. Moreover, these subgroups are divided into levels with varying degrees of versatility. The relevance of the study of the first level of subgroups of GPCs, called basic, is determined. It is shown that they are universal for various programmes of academic training.

4. Basic GPCs are formulated and their characteristics are determined. The TMs are described as part of ADs with their definition, abstracts and LIs.

The validity of the results obtained is confirmed by the positive experience of developing competencies and CMs in the framework of training IS professionals on specific degree programmes at the NRNU MEPhI. While studying, more than half of the graduates undergo internship in the leading organizations of Russia, known in the IS field. Control over the level and quality of graduates is carried out on the basis of attracting highly qualified and eminent specialists from state and commercial organizations to the State Attestation Commission, which governs the defense of Graduation Qualifying Works. Employment of graduates is carried out in the organization of the banking sector and leading government organizations involved in various aspects of ensuring IS. For the last four years, an average of 65 students have been graduated according to the above four Master's degree programmes. These graduates are citizens of Russia and foreign countries – Belorussia, Kazakhstan and Kyrgyzstan.

The features of the results obtained should be noted. Firstly, they are new in terms of developing models that describe their structures. Secondly, these models are versatile as that do not depend on the field of academic training of professionals. Thirdly, the proposed model of the GPCs structure made it possible to substantiate the formulation of competencies and to describe their characteristics necessary for the CM development using the example of academic training of IS professionals.

The results obtained can become the basis for further research of competencies for various PA IS sub-areas, types, objects, and tasks. Moreover, methods of controlling the level of formation of a specific competence should be developed in parallel. It is important both in the training and certification of professionals.

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).

8 LIST OF ABBREVIATIONS

AD	Academic Discipline
BIT	Basic Information Technologies
CM	Competency Model
CS	Cyber Security
CU	Conventional Unit
IP	Information Protection
IPM	Information Protection Management
IS	Information Security
ISEE	Information Security Ensuring Engineering
ISLRF	Information Security Legal and Regulatory Framework
ISM	Information Security Management
IT	Information Technology
FISEM	Fundamentals of Information Security Ensuring Methodology
GPCs	General Professional Competencies
LI	Labor Intensity
NRNU MEPhI	National Research Nuclear University MEPhI (Moscow Engineering Physics Institute)
PA	Professional Activity
PCs	Professional Competencies
PEP	Professional Educational Profile
ST	Socio-Technical
TBISC	Taxonomy Basis of Information Security Concepts
TISO	Typical Information Security Objects

9 REFERENCES

1. Vybornov A., Miloslavskaya N., Tolstoy A. Designing Competency Models for Cybersecurity Professionals for the Banking Sector. In: Drevin L., Von Solms S., Theocharidou M. (eds) Information Security Education. Information Security in Action. WISE 2020. IFIP Advances in Information and Communication Technology. 2020. Vol 579. Pp. 81–95. Springer, Cham. DOI: 10.1007/978-3-030-59291-2_6.
2. Tolstoy A., Miloslavskaya N. Professional Competencies Level Assessment for Training of Masters in Information Security. In book: Information Security Education Across the Curriculum. Matt Bishop, Natalia Miloslavskaya, Lynn Fletcher (Eds.). IFIP Advances in Information and Communication Technology. 9th IFIP WG 11.8 World Conference, WISE 9, Hamburg, Germany, May 26–28, 2015, Proceedings. ISBN 978-3-319-18499-9. ISSN 1868-4238. Springer International Publishing. Volume 453, 2015, pp. 135–145. DOI: 10.1007/978-3-319-18500-2_12.

3. Miloslavskaya N., Tolstoy A. ISO/IEC Competence Requirements for Information Security Professionals. . In: Bishop M., Fitcher 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. DOI: 10.1007/978-3-319-58553-6_12.
4. Alsmadi I., Burdwell R., Aleroud A., Wahbeh A., Al-Qudah M., Al-Omari A. Practical Information Security: A Competency-Based Education Course. Publisher Springer International Publishing AG, Switzerland, 2018, 317 p.
5. Mansfield R.S. Practical Questions in Building Competency Models. Workitect Inc., 2005. URL: <https://pdfs.semanticscholar.org/91d6/2eceb2b4288bde92b46f4c58c9dc5bcf9827.pdf> (accessed: January 18, 2021).
6. Competency Models for Enterprise Security and Cybersecurity. Research-Based Frameworks for Talent Solutions. University of Phoenix. Apollo Education Group Inc. 2015. URL: http://www.apollo.edu/content/dam/apolloedu/microsite/security_industry/AEG-UOPX%20Security%20Competency%20Models%20report.pdf (accessed: January 18, 2021).
7. ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary.
8. Cybersecurity Workforce Competencies: Preparing Tomorrow's Risk-Ready Professionals. Apollo Education Group, University of Phoenix, (ISC)² and (ISC)² Foundation, 2014, 2015. URL: http://www.apollo.edu/content/dam/apolloedu/microsite/security_industry/AEG-PS-264521-CJS-STEM-CYBERSECURITY.pdf (accessed: January 18, 2021).
9. Introduction to the Tools. Report U.S. Department of Labor «Competency Model Clearinghouse public toolkit». URL: <http://www.careeronestop.org/competencymodel/careerpathway/cpwoverview.aspx> (accessed: January 18, 2021).
10. Competency Model General Instructions. Report U.S. Department of Labor «Competency Model Clearinghouse public toolkit». URL: <http://www.careeronestop.org/competencymodel/careerpathway/CPWGenInstructions.aspx> (accessed: January 18, 2021).
11. Professional standards of the Russian Federation for Information Security Specialists. URL: <http://azi.ru/professionalnye-standarty> (In Russian)
12. GOST R 53114-2008 Information Protection. Ensuring Information Security in the Organization. Basic Terms and Definitions. URL: <http://docs.cntd.ru/document/gost-r-53114-2008> (In Russian).
13. Federal Educational Standards of the Russian Federation in the "Information Security" Direction. URL: <http://azi.ru/obrazovatelnye-standarty> (In Russian).
14. Budzko V., Miloslavskaya N., Tolstoy A. Forming the Abilities of Designing Information Security Maintenance Systems in the Implementation of Educational Programmes in Information Security. In: Drevin L., Theocharidou M. (eds) Information Security Education – Towards a Cybersecure Society. WISE 2018. IFIP Advances in Information and Communication Technology, vol 531. Springer, Cham. Pp. 108-120. DOI: 10.1007/978-3-319-99734-6_9.
15. Vybornov A., Miloslavskaya N., Tolstoy A. Designing Competency Models for Cybersecurity Professionals for the Banking Sector. In: Drevin L., Von Solms S., Theocharidou M. (eds) Information Security Education. Information Security in Action. WISE 2020. IFIP Advances in Information and Communication Technology. 2020. Vol 579. Pp. 81–95. Springer, Cham. DOI: 10.1007/978-3-030-59291-2_6.
16. Professional standards of the Russian Federation for information security professionals. URL: <http://azi.ru/professionalnye-standarty> (accessed: January 18, 2021). In Russian.

17. Federal Educational Standards of the Russian Federation in the Information Security Direction. URL: <http://azi.ru/obrazovatelnye-standarty> (accessed: January 18, 2021). In Russian.