Designing Competency Models for Cybersecurity Professionals for the Banking Sector

Andrey Vybornov, Natalia Miloslavskaya, Alexander Tolstoy

Designing Competency Models for Cybersecurity Professionals for the Banking Sector

[1]Andrey Vybornov, [2]Natalia Miloslavskaya and [2]Alexander Tolstoy

[1]Bank of Russia, 12 Neglinnaya Street, Moscow, Russia
[2]The National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), 31 Kashirskoye shosse, Moscow, Russia

{NGMiloslavskaya, AITolstoj}@mephi.ru, vao1@mail.cbr.ru

Abstract. The research results for the main stages of designing competency models (CMs) for cybersecurity (CS) professionals are presented. A strategy for designing such models was formulated. The CS-related terminology and conceptual framework were clarified. Areas, objects, and types of professional activity (PA) as a whole for CS professionals and the banking sector, in particular, were determined. It is proposed to use the role and process models to determine the tasks that employees of banking organizations should solve. The practical issues of developing CMs, which allowed to determine the order of their development and the typical structure, as well as to formulate recommendations on the content of a specific CM, are considered.

Keywords: Design, Cybersecurity, Space, Environment, Competency, Model, Professional, Bank, Processes, Management, Knowledge, Skills, Role

1 INTRODUCTION

At present, we witness a growing need for professional staff in the rapidly developing field of Cybersecurity (CS). The modern approach to determining qualification requirements for such personnel is based on the formulation of professional competencies (PCs) as the ability to solve assigned tasks and perform certain work within the framework of professional activity (PA) [1, 2]. Moreover, it was recognized that it is correct to form a set of PCs in the form of competency models [3-5].

Currently, there are a large number of definitions of the "competency" term [1-6]. For completeness of the research topic discussion, we will focus on the following definition: competency is a certain personality characteristic, which is necessary to perform certain work and which allows its holder to obtain the necessary work results [6]. Competency traditionally refers to a combination of observable and measurable indicators: knowledge (K), Skills (S), and Abilities (A) (together denoted by KSA).

A model is a logical description of components and functions, which display the essential properties of a simulated object. Competency models (CMs) are structured sets of necessary, identifiable, and measurable competencies [6]. Existing approaches

to the development of competency-based models take into account the PA scope (fields and types), as well as the focus of the application of such models.

For CS, the most interesting is the CM presented in the report of Apollo Education Group, Inc and the University of Phoenix [5, 7] and based on tools developed by the Department of Labor (US). The CM is presented in the form of organizational structure [8, 9], divided into nine levels forming three clusters.

Cluster 1: Fundamental competencies unite three levels (groups) of competencies. Levels 1 to 3 at the bottom represent a group of basic competencies, which are required from almost any person as a workforce. Together they reflect skills, which are common to all PA fields and types. At level 1, there are competencies of personal effectiveness/qualities, such as integrity, reliability, and adaptability, which are formed at an early age in the family, at school or through connections with religious or other community-based values. Level 2 consists of academic competencies, which are usually formed through formal education (primary, secondary, higher). Level 3 includes competencies in the workplace, such as teamwork, planning, and organization, which are necessary to perform certain job functions.

Cluster 2: Industry competencies unite two levels of competencies. Levels 4 and 5 include general PCs related to a specific PA field without reference to a certain profession or roles. Level 4 contains the general PCs relate to the formation of concepts related to the entire PA field. Level 5 includes general PCs that are associated with the formation of concepts relating to specific sectors of the PA field.

Cluster 3: PCs unite three levels of competencies. PCs are located at levels 6 through 8. They relate to special PCs and reflect a specific PA type with a focus on a particular profession and the performance of specific professional roles. To do this, it is necessary to form special PCs related to special knowledge for a specific PA type (level 6), special skills and abilities to perform certain roles (level 7), requirements for performing specific roles (level 8) and management processes when performing them.

The organizational structure of the CM presented above is universal. Its effectiveness can only be tested when developing specific CMs.

Thus, the main goal of the paper is to design CMs for CS PA and the types of professional activities that are associated with professions being in demand in banking institutions when implementing specific roles to ensure CS. This goal can be achieved by solving the following tasks: developing a CM design strategy, clarifying the CS term, defining on this basis the PA fields, objects, types, and tasks for banking organizations, determining the CM types applicable in this case, defining the requirements for the CM structure and content, and considering practical issues of developing a CM for professionals in CS for banking organizations. Key findings conclude the paper.

2 COMPETENCY MODEL DESIGN STRATEGY

When developing CMs, it is necessary to solve the strategic tasks presented on Fig. 1.

Task 1: Setting the goal of developing a specific CM. It is primarily determined by the practical significance of the developed model's usage in a specific field of activity. Currently, the following areas of CM use can be distinguished.

1. The area of an educational activity (academic education). The purpose of developing CMs is to create a regulatory framework for improving the quality and effec-

tiveness of training professionals in various PA fields with a variety of PA types, objects, and tasks, for which graduates of educational institutions should be trained. In the CM, the universal (personal, general educational), general and special PCs, which should be formed after graduation, should be defined. At the same time, general and special PCs should be consistent with the requirements of the labor market (organizations-employers). The process of training professionals has certain "inertia". Therefore, CMs developers should predict the needs of the labor market for several years to come. For example, this period in the bachelors' training is 3-4 years, and in the masters' training is 2-3 years. It should also be noted the nature of the professional training at the academic education level, which does not allow the formation of a wide range of practical skills that affect the content of CMs.

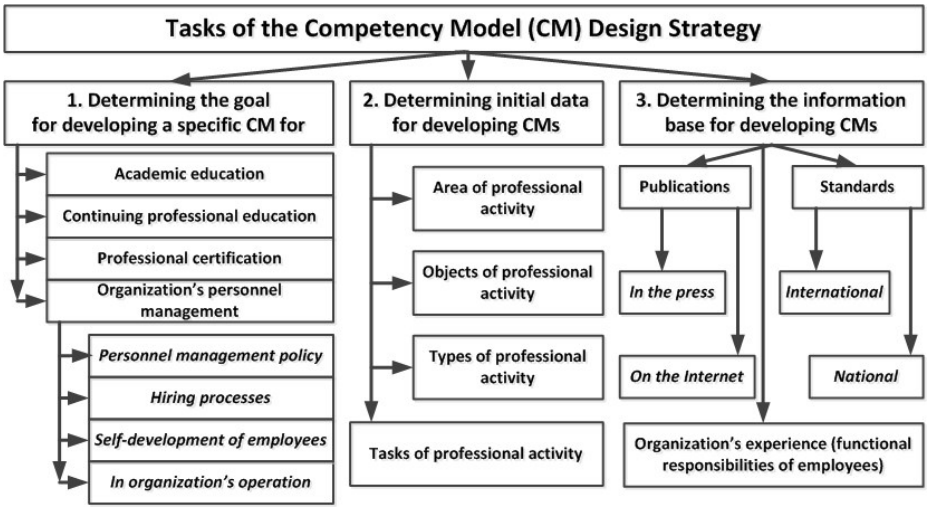

Fig. 1. The structure of the tasks of the Competency Model Design Strategy

2. The area of continuing professional education. The purpose of developing CMs is to create a regulatory framework for improving the quality and effectiveness of the implementation of professional refresher courses and retraining programs in a specific field and for specific PA objects, types, and tasks. Continuing education is aimed at developing a certain special PC (to acquire additional practical skills and the corresponding knowledge). Retraining is aimed at the formation of a new special PC (to acquire new skills and the corresponding knowledge). CMs should include general professional (for retraining programs) and special professional (for professional refresher courses and retraining programs) competencies, which should be formed among students who have been trained in these programs. Moreover, CMs should be coordinated with specific organizations that are either employers or centers for independent certification of specialists in a specific PA field.

3. The area of activity of a particular organization for work with its personnel. The CMs developing purpose is to create a regulatory framework for improving the quality and effectiveness of personnel management. In this case, the CM can be developed and applied for the following organization's personnel management processes:

- Development and implementation of an organization's personnel management policy. At the same time, this policy can be developed as a separate document or part of a document related to the policy of managing a specific process (for example, a CS ensuring policy). The use of CMs simplifies greatly the work to strengthen the organizational culture, helps to create clear guidelines that indicate what is expected from its employees, and gives it the added benefit of improving professional development programs. In this case, when developing CMs for a specific PA field (determined by the specifics of a particular organization), it is advisable to determine the PA object, type, and tasks in the framework of the description of the roles that an employee should fulfill and which should be related to the relevant competencies. The role-based approach should be fixed in the personnel management policy, which should imply the order of their development and connection with CMs, as well as the principles of the role formation and distribution (assignment). An important feature of the organization's personnel management is the establishment of a procedure for the development and use of competency and role models in the case of the organization growth that is associated with changes in its business, as well as the PA field, objects, types or tasks;
- Personnel management during their hiring (hiring processes). CMs provide clear criteria for selecting candidates based on requirements for knowledge and skills levels, as well as existing work experience. These requirements should be included in the CMs that distinguishes them from the CMs developed, for example, in educational institutions;
- Personnel management during the organization's operation. Together with role models, CMs can be used during periodic certification of employees to determine whether their competencies correspond to the roles performed, as well as to identify the opportunities for specific employees in their career growth. It is also important to draw up and implement plans for raising awareness, modernizing the existing PCs of employees, or creating new PCs for them. The latter is important in the context of the development of the organization noted above;
- Improving the professional level of the organization's employees on an individual basis. Based on the provisions of CMs, the employees can independently form a required level of knowledge and skills. This may be due to the desire to maintain constantly the roles assigned to them in the best way or with plans to apply for the roles related to a higher position.

4. The areas of professional certification. The goal is to increase the effectiveness of independent certification centers that implement certification programs for professionals in a particular field and related specific PA objects, types, and tasks. The implementation of certification programs is aimed at determining the level of knowledge and skills of specific specialists. This work can be carried out within the framework of an order of specific organizations of employers, companies-developers of specific devices and systems, or with the individual application of specific professionals who want to receive a certificate confirming a certain level of their PCs. The effectiveness of certification centers is determined by many factors; a particular factor is a focus on modern CMs developed in educational institutions and organizations-employers.

The features of the first problem solution discussed above allow us to conclude that there are a large number of CM types that differ not only in the goals of their development but also in the source data necessary for the development of a specific CM.

Task 2: Defining initial data. It includes the description of a specific field, as well as specific PA objects, types, and tasks. In some cases (e.g., personnel management), it is possible to describe the source data in the form of role models. Further, the solution of this problem for the selected field will be considered.

Task 3: Defining the information base necessary to determine the source data and formulate the relevant competencies. This information base can include publications, including on the Internet, reflecting the experience of developing CMs (among them are publications containing general recommendations on the development of CMs [4, 8-12], recommendations on CMs in the information security (IS) field [1-3, 6], information on PCs in the field of CS [5, 7, 13-16]), standards, including those containing recommendations on competencies in the IS field at the international [17] or national [18, 19] levels, and the experience of organizations in their personnel management (documented functional responsibilities and job descriptions of employees).

Special attention should be paid to the experience of Russia in developing a competency-based approach for formulating requirements for the professional qualifications. Professional standards for various PA fields were developed and implemented. Among them, there is a group of six IS professional standards. They 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 [18]. These professional standards are used by organizations to create and implement their personnel management systems. A group of seven Federal Educational Standards (FESs), related to the training of bachelor, masters, and specialists (engineers), is linked directly to these IS professional standards. They formulate general and general PCs and normalized the development of special PCs.

3 CYBERSECURITY AND PA FIELDS

The ISO/IEC 27032:2012 with the guidelines for CS defines the CS as a "preservation of confidentiality, integrity and availability of information in the Cyberspace. Besides, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved" [20]. It is a security in the Cyberspace. In turn, the Cyberspace refers to a "complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form". This standard is in the conceptual field, which constitutes the methodological basis of the provisions of the standards of the ISO/IEC 27000 series related to IS. This area is associated with concepts such as asset, threat, vulnerability, and risk [21], which is related directly to the field of CS.

An analysis of these definitions shows the following. The CS definition complies fully with the IS definition. The difference lies in clarifying the CS scope (the Cyberspace). From the CS definition, it follows that the concept of an interaction environ-

ment is associated with it. It should be noted that the "space" and "environment" terms are not synonymous. Therefore, clarification of the definitions of these terms is required. ISO/IEC 27032 connects directly the environment of interaction to the Internet, which does not contradict the IS field.

The features highlighted above show that there is no clear distinction between CS and IS concepts at present. It can be assumed that the CS term refers to a narrower conceptual field than the IS term. In our opinion, all the problems of providing security services can be solved within the framework of security management. Despite this conclusion, the fact that the CS term has found very wide use today can be stated [22, 23]. In this case, it seems very important to make the following clarifications. Firstly, the CS term alone (as well as the IS term) does not have a clear definition. If we connect CS with the CS space and environment, then it is necessary to consider the conceptual area in the context of specific objects (so called CS objects). Secondly, when formulating the definition of the CS object term, it is necessary to take into account the modern approach to providing IS, the methodology of which is presented in the ISO/IEC 27000 standard series. In this case, the following definitions are proposed.

The CS space is a collection of CS objects that takes into account their relative position and has its structure (Fig. 2). As a rule, the CS space is a virtual space in which the position of a CS object is specified by a logical address. In some cases, it may be appropriate to determine the position of the CS object in real space. In the general case, CS objects can be represented in the structure of CS space, having their addresses, which are needed to determine the relative position of the CS objects. In Fig. 2, CS objects are combined into groups (parties) representing individual organizations.

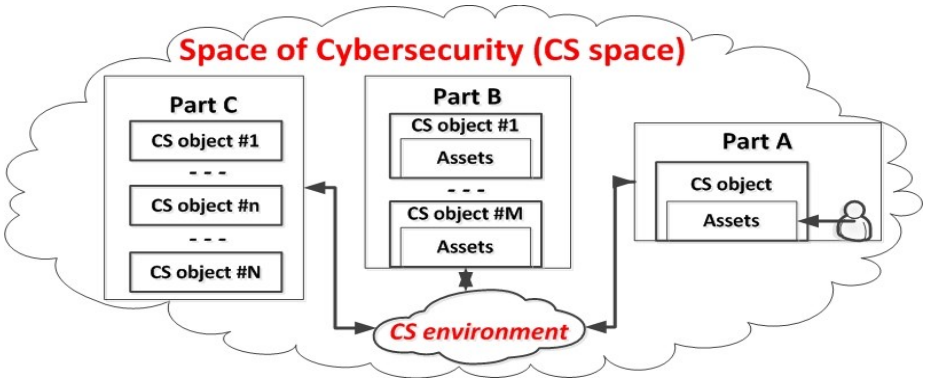

Fig. 2. The structure of the CS space and environment

The CS environment is a virtual environment implemented based on the Internet technology, ensuring the interaction of CS objects and having its structure. This structure corresponds to the situation that is associated with the provision of CS during the interaction of CS objects. In this case, it is important to identify stakeholders [20], which are organizations or persons with their CS objects that interact with each other using the Internet technology. A typical case is the presence of the following parties of the interaction presented on Fig. 2. Party A (provider) is an organization (person) that provides its services based on the operation of a specific CS object. Party B (con-

sumers) is organizations (persons) that consume these services (there may be several), using their CS objects. In the general case, the number of such organizations (persons) or CS objects will be from 1 to M. Party C (external intruders) is organizations (persons) that by organizing the interaction of their CS objects with the CS objects of the provider or consumer will realize threats aimed at the assets of the CS objects of Parties A and B. In general, the number of such organizations (persons) or CB objects related to Party C will be from 1 to N. The interest of the parties to interact will be different: Parties A and B have a common interest in preserving their assets, and the purpose of Party C is to harm Party A and/or Party B.

It should be noted that there is a possibility when a threat may come from the organization's employee - the provider, who has authorized access to the assets of the CS object and uses its capabilities to harm the organization. This corresponds to the source of threats inside the organization - the provider or the internal intruder.

The CS object is a real object implemented using IT and the Internet technology.

The CS framework is a combination of the CS space and environment.

An object's CS refers to a property inherent in the object to maintain the state of object's asset protection when there are threats in the CS framework, which corresponds to the value of damage (or risk) associated with the possible implementation of these threats, not exceeding a predetermined level. At the same time, the state of asset protection is determined by their properties: confidentiality, integrity, availability, authenticity, non-repudiation, etc.

Ensuring the object's CS refers to an activity of forming the necessary properties of an object in the CS framework.

Thus, it is possible to formulate a definition of *the PA field* (in the broad sense) as a field of science, engineering, and technology, covering a set of problems associated with ensuring CS of objects. This definition is of a general conceptual nature and has no practical significance.

The terminology analysis of the object's CS concept and the structural features of the CS space and environment allows us to draw the following conclusion about the absence of a single PA field related to CS. This means that professionals are needed in various fields for solving problems in CS, taking into account the specifics of a particular field and the CS framework.

For further applicability, including the development of CMs, it is appropriate to identify at least three PA fields (they reflect the narrow sense of this concept):

- Areas of science, engineering, and technology covering problems associated with:
  - IT implemented taking into account the requirements for ensuring CS. This area includes IT professionals with competencies in CS;
  - The processes of ensuring CS in key systems of information infrastructure of organizations. Professionals in CS with competencies in IT belong to this area;
- Separate areas of engineering and technology, in which it is necessary to implement separate processes for ensuring CS when using IT while solving basic professional problems. This area includes professionals in a specific field of activity with additional competencies in IT and CS.

4 CS OBJECTS AND PA TYPES IN BANKING SECTOR

To describe the CS objects, it is necessary to determine the basic technological processes (TPs) implemented in banks. There are two groups of them: main and auxiliary. The first group includes banking TPs that carry out operations to change and/or determine the state of the organization's banking assets used in the operation or necessary for the implementation of banking services [24]. Operations on the assets of a banking organization can be performed manually or be automated (for example, using IT). Depending on the type of activity, there are banking payment and information TPs. *Banking payment TPs* (BPTPs) are a part of banking TPs that implement banking operations on information related to the transfer of funds from one account to another and/or control of these operations. In this case, the information contained in the documents refers to the payment information, based of which operations related to the transfer of funds from one account to another, are performed [24]. *Banking information TPs* (BITPs) are banking TPs that carry out operations to change and/or determine the state of information necessary for the functioning of a banking organization and which is not payment information. Non-payment information may include, for example, data from statistical reporting and on-farm activities, analytical, financial, and background information [24].

Automation of banking TPs is carried out, as a rule, with the help of automated banking systems (ABS), which are complexes consisting of personnel and automation tools that implement information and telecommunication technologies for performing the established functions of TPs. There are two groups of ABS: automated banking payment (ABS1) and bank non-payment (ABS2) TPs. The difference lies not only in the processing of different types of information (payment and non-payment), but also in the fact that they have different structures. The ABS1 may have in its structure executing devices (ATMs, payment acceptance devices) and remote access devices for clients when receiving banking services (smartphones, laptops, personal computers). The ABS2, as a rule, does not have logical (in some cases physical) connections with the ABS1, it does not have executing devices in its structure and can use remote access technologies only for employees of a banking organization.

In the banking structure, there may be several ABS1 and ABS2. The second group includes TPs that implement auxiliary functions. Taking into account the specifics of the area under consideration, these TPs include CS ensuring processes integrated into specific systems. The CE Ensuring System (CSES) consists of two systems: Information Protection System (IPS) and CS Management System (CSMS) (Fig. 3).

The IPS combines the following processes [25]: P1. Securing information during access control: 1.1. Management of accounts and rights of entities of logical access; 1.2. Identification, authentication, authorization (access control) in the implementation of logical access; 1.3. Protection of information during physical access; 1.4. Identification, classification and accounting of resources and access objects. P2. Securing computer networks: 2.1. Segmentation and firewalling of computer networks; 2.2. Identification of network intrusions and attacks; 2.3. Protection of information transmitted over computer networks; 2.4. Wireless Security. P3. Monitoring the integrity and security of the information infrastructure. P4. Protection against malicious code.

P5. Prevention of information leaks. P6. IS incident management: 6.1. Monitoring and analysis of IS events; 6.2. Detection of IS incidents and response to them. P7. Protecting the virtualization environment. P8. Prevention of information during remote logical access using mobile (portable) devices.

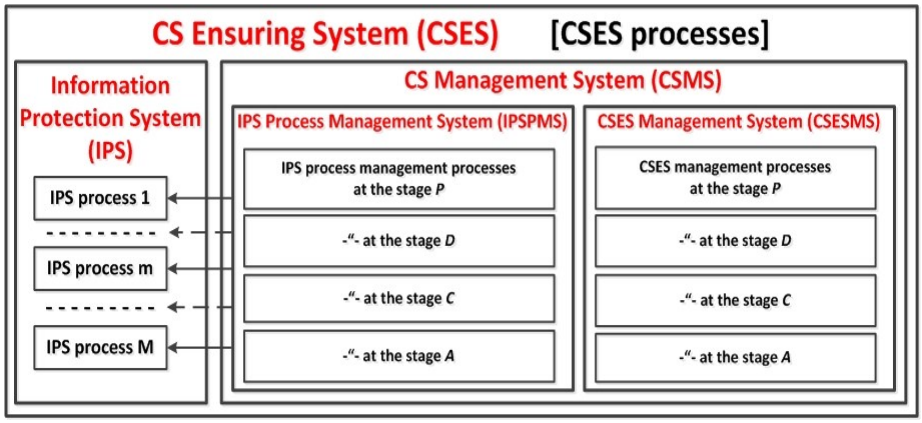

Fig. 3. The structure of the CSES

The CS Management System (CSMS) consists of two systems (Fig. 3): the IPS Process Management System (IPSPMS) at the design (P), implementation (D), control (C) and improvement (A) stages of the specific IPS process and the management system for the entire CSES (CSESMS) at the stages P, D, C and A according to the cyclic Plan (Plan) - Implementation (Do) - Check (Check) - Action (Act) model [21].

The management processes of the CSES include: *At the stage P*: identification of assets to be protected, description of CS threats, assessment of CS risks and selection of information protection processes and measures, development of a CS ensuring policy and development of internal organization documents related to ensuring CS; *At the stage D*: implementation of a CSES; *At the stage C*: carrying out various types of management of the CSES (processing the data of monitoring the IPS processes, conducting an internal and external audit of the CSES, conducting a self-assessment), *At the stage A*: development and implementation of measures to improve the CSES processes, including the IPS processes and the CSES management processes.

When creating a CSES, it is important to identify assets to be protected. For a banking organization, such assets will be objects that have value and are located in its location. Moreover, it is important to describe (identify) those assets that are used or consumed in the implementation of banking TPs. In this case, they are considered in the form of resources related to a particular banking TP. A banking organization has the following assets (resources) related to the scope of ensuring CS [25]: Information assets, which include payment and non-payment (financial, analytical, official, managing, personal data, etc.) information divided into two groups (public information and with a limited access) with different IS requirements; Assets related to the information asset processing environment (ABS automation systems (tangible objects): objects of storage, transmission, processing, destruction, etc.); Financial (monetary)

funds of the bank; Employees (personnel) of the bank; Banking TPs (payment and information); Banking products and services provided to customers; Intangible assets (reputation, image of the bank).

The above analysis of the processes in banking structures allows us to determine:

- CS objects: ABSs that implement various banking TPs;
- The PA objects of bank employees: CS objects (ABSs), CSES processes and measures that implement these processes, assets (resources);
- PA types: operational (implementation of the IPS processes), organizational and managerial (implementation of the CSESMS management processes), design (participation in the ABS and CSES design).

It should be noted that the distinguished PA objects have features characteristic of CS: the space of their existence can be physical and virtual, and the interaction environment is predominantly virtual.

5 CYBERSECURITY PA TASKS IN BANKING SECTOR

To determine PA tasks in banking organizations, an employee role-based approach can be used [24, 26]. This approach is based on the concept of the role as a predetermined set of rules that establish an acceptable interaction between a subject and an object [24]. Subjects include persons from among the employees of a banking organization and its customers or processes initiated by them on the implementation of actions on objects. Objects can be hardware, software, information resource, service, process, system, on which actions are performed. In this case, the role model fully complies with the consideration of the CS environment as an environment for the interaction of CS objects that can be associated with PA objects and, as a result, determine the PA tasks.

The structure of the role model of an employee of a banking organization in the field of CS can be determined by analogy with a similar structure for the field of IS [26]. For this, it is necessary to consider the specifics of an employee of a banking organization (subject) performing his duties reflected in job descriptions, which are directly related to the definition of his functions (or PA tasks), rules and restrictions when interacting with various CS objects (PA objects). From this one can form an expanded role concept as a set of functions of an employee of a banking organization, the fulfillment of which requires payback (by function - a type of work performed or planned to be performed by the employee) a set of authority. This definition allows us to propose a model for the role description, the structure of which is shown in Fig. 4. Each role can correspond to one or more functions related to ensuring CS. To perform a certain function, the CS authority is required, each of which establishes a set of rules and restrictions aimed at the CS PA objects (CS objects, assets, CSES processes).

Analysis of the role model structure allows us to conclude that there is a wide variety of roles related to the CS functions (PA tasks). Hence, it useful to classify the roles. The separation of roles into groups (categories) is possible taking into account the characteristics of assets, CS objects, and CSES structure (Fig. 5).

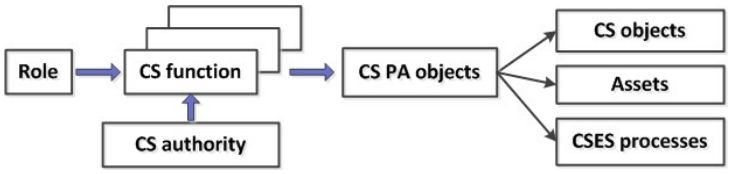

Fig. 4. The structure of the role model

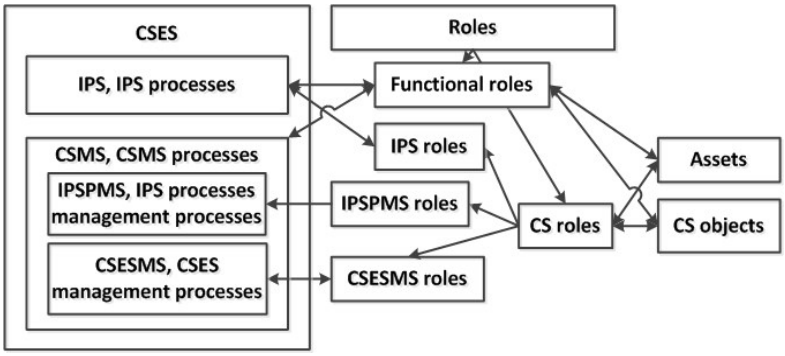

Fig. 5. The role categories

In a banking organization, two groups of employees can be distinguished whose basic job responsibilities are either unrelated or related to CS ensuring. For example, an accountant who processes banking information using automated workstations implements such IPS processes as ensuring the protection of information during access control and protection against malicious code (additional responsibilities). We will classify such roles as functional roles.

The CS unit employees perform functions related to CS ensuring (basic responsibilities). These functions include the implementation and maintenance of the IPS processes and the management processes of CSMS (IPSPMS and CSESMS). The corresponding roles will be categorized as CS roles (which, in turn, will be divided into the roles of IPS, IPSMS and CSESMS. Both role categories also include functions related to ensuring CS of assets and CS objects.

The banking organization should describe and document the roles related to CS ensuring. The processes of formation and distribution of roles refer to the processes of role management, which is a separate PA task in CS (the processes of managing CS roles belong to CSESMS). The description of the roles is the basis for the formulation of the PA tasks, which must be done when developing CMs. An example of defining roles in the field of IS can be found in [26].

6 COMPETENCY MODEL DEVELOPMENT PRACTICE

The analysis showed that the CM can be developed only for a specific PA field and application. In this case, the CM should be associated with a subject of a certain educational level (for example, a bachelor, master, specialist, engineer, etc.). Thus, the

following procedure with seven stages for developing a specific CM for CS professionals for the banking sector is proposed: 1) Solving the strategic tasks of CM developing (Fig. 1); 2) Determining its structure; 3) Filling the CM with specific content; 4) CM coordinating and approval; 5) CM implementation (usage); 6) Monitoring and analysis of the CM usage efficiecy; 7) Developing correction measures for the CM.

To maintain the necessary level of CMs usage efficiency, stages 3-7 should be performed cyclically in time during the CM life cycle. In the case of the CM development for use in educational institutions or certification centers, it is advisable to coordinate it with organizations-employers or organizations that have the right to approve at the state or international level (if any). In the Russian Federation, a system of training IS professionals has been created, which provides for the coordination of educational programs, syllabus and curricula (including CMs) at the state level. The capabilities of the system can be used to coordinate educational materials in the CS field.

The importance of the third stage of CM development should be noted. Here a typical CM structure (CM sections) can be proposed: S1. CM Goals and Purpose. S2. PA Characteristics: 2.1. PA Field. 2.2. PA Objects. 2.3. PA Types. 2.4. PA (by PA type). S3. Competencies: 3.1. General competencies. 3.2. General PCs. 3.3. PCs (by PA type). S4. Indicators of achievement of competencies: 4.1. Indicators of achievements of general PCs. 4.2. Indicators of achievement of PCs. S5. Information sources.

The specifics of the CM scope (CS professionals for the banking sector) is determined in the second section of CM. In the third section, the division of competencies into three groups (general, general professional, and professional) corresponds to the recommendations on the CM structure [8, 9], which suggest the presence of three clusters of competencies. The binding of general PCs to specific PA types partially corresponds to the division of a particular cluster into levels. The section of general competencies is present only in the CM of graduates of academic institutions (bachelors or masters) and sometimes in the CM used in personnel management. When formulating a specific competence, one should adhere to the following form: “has certain abilities” (for general competencies) or “ability to solve a specific problem” (for general professional and professional competencies). The formation of professionals' specific competency is associated with the presence of concrete KSA as indicators of specific competence. These indicators for each general professional or professional competence should be described in the fourth section. The “knowledge” and “skill” indicators are more often used for academic education. Professional's additional education and practical activities contribute to the formation of not only knowledge and skills, but also abilities.

CM developers should have certain CS competencies in the educational and practical fields that cannot be typically combined in one person. Therefore, it is necessary to recognize the fact that only a team of performers and representatives of educational centers and leading organizations in CS can develop a CM.

Currently, the National Research Nuclear University MEPhI (Moscow Engineering Physics Institute) has accumulated many years of experience in training professionals in the field under consideration when implementing Bachelor's and Master's degree programs. The relevant CMs can be found by the following link: http://eis.mephi.ru/AccGateway/index.aspx?report_param_gosn=3&report_param_ismagister=true.

7 CONCLUSION

The analysis of modern approaches to designing CMs, the specifics of ensuring CS area, as well as banking TPs and related CS ensuring processes allowed to obtain all the results presented in the paper. The validity of the results obtained is confirmed by the positive experience in the CM development in the framework of training professionals in the field in the implementation of specific educational programs at the NRNU MEPhI.

It should also be noted the features of the results obtained. Firstly, they have a novelty in terms of the integrity of the CM development process and its applicability to the banking sector. Secondly, the results obtained are systematic from the viewpoint of using various types of CMs for development, depending on the purpose of their application. Thirdly, the results obtained are universal. They may be applicable in the development of CM for professionals in other PA fields.

Besides, the development of a specific CM should be accompanied by the development of controls that are designed to determine the level of formation of a specific competency (the implementation of processes for assessing (measuring) competency indicators). This is important in the training of professionals, and in the certification and certification. Design issues for controls may be the subject of further research.

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 REFERENCES

1. Tolstoy A., Miloslavskaya N. Professional Competencies Level Assessment for Training of Masters in Information Security. In book: Information Security Education Across the Curriculum. IFIP Advances in Information and Communication Technology. 9th IFIP WG 11.8 World Conference, WISE 9, Proceedings. Vol. 453, 2015, pp. 135-145.
2. 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. Pp. 135-146.
3. Practical Information Security: A Competency-Based Education Course. Izzat Alsmadi, Robert Burdwell, Ahmed Aleroud, Abdallah Wahbeh, Mahmoud Al-Qudah, Ahmad Al-Omari. Publisher Springer International Publishing AG, Switzerland, 2018, 317 p.
4. Mansfield R. S. Practical Questions in Building Competency Models. Workitect, Inc., 2005. URL: https://pdfs.semanticscholar.org/91d6/2eceb2b4288bde92b46f4c58c9dc5bcf9827.pdf (access date 12.01.2020).
5. Competency Models for Enterprise Security and Cybersecurity. Research-Based Frameworks for Talent Solutions. University of Phoenix. Apollo Education Group. 2015. URL: http://www.apollo.edu/content/dam/apolloedu/microsite/security_industry/AEG-UOPX%20Security%20Competency%20Models%20report.pdf (access date 12.01.2020).
6. Gridin A. Competence model of a specialist in computer security. URL: https://habr.com/en/post/182176/ (access date 12.01.2020). In Russian.

7. 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 (access date 12.01.2020).
8. Introduction to the Tools. Report U.S. Department of Labor «Competency Model Clearinghouse public toolkit». URL: http://www.careeronestop.org/competencymodel/ careerpathway/cpwoverview.aspx (access date 12.01.2020).
9. Competency Model General Instructions. Report U.S. Department of Labor «Competency Model Clearinghouse public toolkit». URL: http://www.careeronestop.org/ competencymodel/careerpathway/CPWGenInstructions.aspx (access date 12.01.2020).
10. Reynolds J. Competency model? Explained – and how to build them. URL: https://www.tinypulse.com/blog/competency (access date 12.01.2020).
11. Forst S. How to build a competency model. URL: http://hq.teamfit.co/how-to-build-a-competency-model (access date 12.01.2020).
12. How to Develop a Competency Framework. URL: https://www.lucidchart.com/blog/how-to-develop-a-competency-framework (access date 12.01.2020).
13. Berry J. Competency Model for Cybersecurity. Memorandum for Chief Human Capital Officers. URL: https://www.chcoc.gov/print/2667 (access date 12.01.2020).
14. State Government Information Security Workforce Development Model. A Best Practice Model and Framework. June 2010. Final Version 1.0.
15. The U.S. National Cybersecurity Workforce Framework. URL: https://www.dhs.gov/national-cybersecurity-workforce-framework (access date 12.01.2020).
16. The Cyber Security Capability Framework & Mapping of ISM Roles. Final Report. Australian Government Information Management Office. June 2010.
17. ISO/IEC 27021:2017 Information technology — Security techniques — Competence requirements for information security management systems professionals.
18. Professional standards of the Russian Federation for information security professionals. URL: http://azi.ru/professionalnye-standarty (access date 12.01.2020). In Russian.
19. Federal Educational Standards of the Russian Federation in the Information Security Direction. URL: http://azi.ru/obrazovatelnye-standarty (access date 12.01.2020). In Russian.
20. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity.
21. ISO/IEC 27000:2014 Information technology — Security techniques — Information security management systems— Overview and vocabulary.
22. Definition of Cybersecurity – Gaps and overlaps in standardisation.- Report of European Union Agency for Network and Information Security (ENISA), v1.0. December 2015. URL: http://www.enisa.europa.eu/ (access date 12.01.2020).
23. Miloslavskaya N.G., Tolstaya S.A. Cyber Threats for Organizations of Financial Market Infrastructures. Besopasnost informachionnih technologiy. 2016. N 1. Pp. 115-126. In Russian.
24. Bank of Russia Standard STO BR IBBS-1.0-2014 «Maintenance of Information Security of the Russian Banking System Organizations. General Provisions». In Russian.
25. GOST 57580.1-2017. Security of financial (banking) operations. Protection of information of financial organizations. The basic composition of organizational and technical measures. In Russian.
26. Vybornov A.O., Kurilo A.P., Kharlamov V.P. The role model of employees of a banking institution in the field of information security. Besopasnost informachionnih technologiy. 2012. N 3. Pp. 90-102. In Russian.