Information Security Specialist Training for the Banking Sphere

Andrey P.Kurilo, Natalia G.Miloslavskaya and Alexander I.Tolstoy

[1] The Central Bank of Russia,
[2] Moscow Engineering Physics Institute (State University), Moscow, Russia
+7 495 324-9735, ait@mephi.edu, tolstoy@mephi.ru

Abstract. On the basis of analysis of the Standard of the Central Bank of Russia "Ensuring Information Security for Organizations of Banking system of the Russian Federation. Basic principles." there have been defined the qualification requirements for the specialists with higher education in the field of information security who could be claimed for work in the banking sphere.

Keywords: information security, expert training, banking sphere, Russia

1 Introduction

Banking institutions are one of the most sensitive objects for which information security (IS) maintenance requirements are very real. Damage from breaking the security of banking information (confidentiality, integrity, and availability) could have a wide range of consequences ranging from financial loss of individuals to financial crisis of an individual state.

The banking system of the Russian Federation is formed by the Central Bank of Russia, different credit organizations (for e.g., the Savings Bank, the Vneshtorgbank, the Vnesheconombank, regional banks etc.), and representative and branch offices of foreign banks. These organizations solve different business problems and have different structures (for e.g., have or have not regional branches).

The joining factor for different banking objects is the banking information and banking information technologies. The peculiarities of the banking information and technologies allow us to allocate banking organizations into a separate groups of information objects that require separate approaches to IS. These approaches apply to the whole object and its separate systems (like automated banking payment systems, information banking systems, telecommunication banking systems). Compounding the variability in requirements, IS employees require specialized training in the field of IS.

Training of specialists with higher education in the field of IS is carried out by over 100 Russian universities. Analysis of the experience collected within training of IS specialists in one of the leading Russian universities – the Moscow Engineering Physiscs Institute (State University), which has the Information Security of Banking Systems Department at the Information Security Faculty – allow forming the basic requirements to the level of preparation of specialists for the banking sphere.

To form such kind of requirements it is expedient to examine the types and tasks of professional activities of the university graduates and to formulate their qualification characteristics. The following sections formulate the qualification characteristics of IS specialists for banking institutions.

2 Defining Qualification Characteristics

The basic qualification characteristics of a specialist with higher education are formulated on the basis of his/her special (professional) competences. Special qualitites of a graduate are his/her abilities to solve definite problems and carry out specific work within his/her line.

Thus formulating the qualification characteristics is possible only when considering separate typical objects where IS tasks are carried out with specialists in the IS field. Such kind of qualification characteristics could be formulated on the basis of expert estimations of either leading IS specialists or definite organizations. Unfortunately the second approach cannot be easily implemented in practice because of lack of distinct system which would allow joining forces of separate typical organizations for working out concrete qualification requirements.

It is necessary to note that this drawback concerning banking instituations of Russia has been overcome with adopting the Standard of the Central Bank of Russia (SCBR) “Ensuring Information Security in Organizations of Banking System of the Russian Federation. Basic principles.” in 2006 [1]. There is enough information within the Standard to formulate the qualification requirements for specialists, ensuring functioning of the banking information protection systems.

3 Initial data for formulating the qualification characteristics

It is possible to formulate qualification characteristics on the basis of:

- topics worked out by students within a specific banking organization during their practice and preparation of graduate qualification paper (diploma project);
- functions of IS specialists working within concrete banking objects.

Under the first qualification characteristic, the Russian universities allow up to one year for practicing and preparation of the graduate qualification paper for training IS specialists. For example, the MEPhI students have their 10th and 11th semesters for that which lasts for 1 year. Experience of graduating higher education specialists collected since 1995 allow grouping practice and diploma project topics in the following way:

- development of information protection technologies;
- design of information protection means;
- administering separate IS technologies;
- administering IS subsystems;
- IS subsystem design for a concrete automated system;

- IS management system design of an object as a whole.

It is worth noting that for banking information objects the most typical or the topics that deal with administering separate information technologies and IS technologies, design and administering IS subsystems of concrete automated systems and design of IS management systems for an object as a whole.

Developing of specialized information protection means for banking information objects is not actual.

Considering the second qualification characteristic, to define functions of IS specialists working within banking objects it is necessary to define a place of IS at those objects, role of IS service and line of activities of such specialists. Such information could be obtained upon analysis of the SCBR. Before analyzing the document, it is expedient to characterize that Standard in general.

4 General Characteristic of the SCBR "Ensuring Information Security for Organizations of the Banking system of the Russian Federation. Basic principles."

The SCBR consists of three main parts:

1. Forming the goals of ensuring IS of banking organizations in the Russian Federation (RF) (is based upon defining initial conceptual scheme (paradigm) of IS, basic principles of IS, model of threats and IS violators and forming IS policy of an organization).

2. Implementation of the goals of ensuring IS of an organization. This part of the SCBR defines the role of IS management processes in an organization.

3. Control of progress in reaching IS goals of an organization is based upon checks and evaluation of organization's IS (monitoring and audit) and defining maturity of organization's IS management processes (defining maturity model).

When developing the SCBR a large number of international (14) and Russian (11) standards and normative documents were used. Moreover, a certain number of the Russian standards have foreign prototypes. Such as "ISO/IEC IS 27001-2005 Information technology. Security techniques. Information security management systems. Requirements" and "ISO/IEC IS 27002-2007 Information Technology. Code of practice for information security management."

The structure of the SCBR is the following:

- Scope of implemetation.
- Normative links.
- Terms and definitions.
- Notations and abbreviations.
- Initial conceptual scheme (paradigm) of ensuring IS of banking organizations in the RF.
- Basic principles of ensuring IS of banking organizations in the RF.
- Threat model and IS violator model of banking organizations in the RF.
- IS policy of banking organizations in the RF.
- IS management system of banking organizations in the RF.

- Check and evaluation of IS of banking organizations in the RF.
- Model of maturity of IS management processes of banking organizations in the RF.
- Standard's line of development.

Analysis of these sections of the SCBR allow us to get initial information for formulating qualification characteristics of IS specialists for banking organizations.

5 The Role of IS at the Object

The Standard defines the role of IS at the banking object as (section 5.2 of the Standard): *IS processes are a type of supplementary processes implementing support (ensuring) for the processes of the main activities of the organization for it to be able to reach the maximum result possible. It is also defined that organization's activities is carried out through 3 groups of high level processes: main processes (main business processes), supplementary processes (processes maintaining specific tasks) and organization management processes.*

Thus all the processes related to ensuring IS at an information object should add to the main business of the organization. As a result, when training IS specialists peculiarities of protection objects should be taken into consideration and that should be reflected at the qualification characteristics.

IS goal at an object is to build an optimal protection system which would ensure the required level of protection for information resources. That level is defined on the basis of analysis of IS risks which should be adjusted with the main sphere (business) of an organization (section 5.1 of the Standard).

Along with that, one has to note that any coordinated activity of an organization is forming risks whose essence is natural vagueness of the future. This is objective reality and those risks could be lowered only to the level of vagueness of subjects characterizing the nature of business. The remaining part of the risk defined by the factors of the environment of organization's processes for which organization cannot influence at all, should be accepted. In this case ensuring IS at an object should lower risks to a certain level.

6 IS Service Role at an Object

To specify the role of IS service in an organization it is necessary to define subjects that could interact with each other in situations when IS risks could appear. The standard defines the following subjects for that: owner of information assets of the organization and violator trying to influence those assets.

Information assets of the Russian banking system are defined by the Standard as different types of banking information (payment, financial and analytical, official, management, etc.) at all phases of its lifecycle (generation, processing, storage, transfer, termination).

Role of the IS service in an organization is defined by the tasks which are carried out within the conditions of opposition of the owner and violator for the control over information assets.

Ensuring IS at an object is the process that should be efficiently managed. The main role of IS service if defined by the organization's IS strategy which lies in *deployment, exploitation and perfection of the IS management system (ISMS)* (section 5.17 of the Standard).

IS management is a part of the overall corporate organization's management which is oriented for reaching organization's goals through ensuring protection of its information resources. ISMS of organizations is a part of the overall management system based on the business risk approach whose goal is to create, implement, operate, monitor, analyze, support and rise IS of an organization (ISO/IEC IS 27001).

7 IS Specialist Line of Activity

Upon defining the main lines of activities of IS specialists in a banking organization it is necessary to take the following quotations from the SCBR into consideration:

- *The most correct and efficient way of minimizing risks of IS breach for an owner is to develop an IS policy upon en exact forecast which is also based on analysis and evaluation of IS risks, and implement, operate and perfect the ISMS of an organization* (section 5.8 of the Standard). *Such kind of forecast could and should be built upon the experience of the leading specialist of the banking system and in accordance with international experience in the field* (section. 5.10 of the Standard).
- *IS policy of banking organization of the RF is built upon principles of ensuring IS of banking organizations of the RF, models of threats and violators, identification of assets being subject to protection, risk evaluation taking into account peculiarities of business and technologies and interest of a specific owner* (section 5.9 of the Standard).
- *Following IS policy is also an element of corporate ethics. That is why the level of IS within an organization is seriously influenced by team relations and also by team and owner (or management representing owner's interest) relations. Thus such kind of relations should be managed* (section 5.11 of the Standard).
- *Ensuring IS of an organization includes implementation and support of the process of perception of IS and IS management* (section 5.16 of the Standard). Perception of IS ensures the basis for ISMS's functioning. Here efficiency means relation between the achieved result and the spent resources.
- *To implement tasks of deployment and operation of the ISMS of an organization it is recommended to have IS service as part of the stuff* (section 9.7.1 of the Standard).
- To administer IS subsystems in centain automated banking systems the Standard assumes availability of specialists acting as IS administrators (section 8.2.9.5 of the Standard) and formulates basic requirements for such specialists.

Taking all this into consideration and the place and role of the object's IS service, it is possible to formulate the basic line of activities and qualification characteristics of an IS specialist working in banking organizations.

8 Basic Lines of Activities and Qualification Characteristics

The basic lines of activities of IS specialists in banking organizations are defined by their professional activity. Taking into consideration the requirements of the Standard and the topics of the graduate qualification papers allows to define the main types of professional activity:

- technological (ensuring functioning of the main IS technologies);
- organizational-technological (ensuring functioning of ISMS).

Qualification requirements are defined by the types of tasks carried out by the specialists and requirements for the level of knowledge and skills. There are the following tasks solved (special competence):

- formation of goals of ensuring IS at the object on the basis of identification of object's assets, risk analysis, evaluation of IS risks, definition of basic principles of ensuring IS and formulation of object's IS policy.
- implementation of goals for ensuring IS at the object on the basis of deployment, operation and perfection of ISMS.
- control over achievement, if IS at the object goals on the basis of the processes of monitoring, conducting self-evaluation of level of object's IS and definition of level of maturity of object's IS management.

Further, IS specialists should –

know:

- normative basics, related to ensuring IS;
- principles of ensuring IS;
- methods of IS risk analysis;
- basic methods of IS management;

be able to:

- define model of threats and model of IS violators;
- develop an IS policy;
- conduct IS risk analysis at the object;
- develop, deploy, operate, perfect ISMS;
- administer IS subsystems of certain information technologies and automated systems;

have an idea of:

- methods of building object management systems;
- methods of system monitoring and audit;
- peculiarities of psychology and ethics of team relations.

An example collection of activities that should be carried out by an IS specialist working in an IS service of a banking organization is (section 9.7.1 of the Standard):

- manage all the plans of ensuring organization's IS;
- develop and propose modifications to the IS policy;

- modify existing and adopt new normative and methodical documents for ensuring organization's IS;
- choose means of management and ensuring IS of an organization;
- control users and first of all users who have maximum privileges;
- control activity related to access and use of anti-virus tools and other means of IS;
- monitor events related to IS;
- investigate events related to violations of IS and if needed propose application of sanctions against people, who have done unlawful activity, for example, infringed requirements of instructions, manuals, etc. for organization's IS;
- participate in activities for recovery of operational capacity of automated systems right after faults and accidents;
- create, support and perfect ISMS of the organization.

9 Conclusion

On the basis of analysis of the Standard of the Central Bank of Russia "Ensuring Information Security for Organizations of Banking system of the Russian Federation. Basic principles." the qualification requirements for specialists with higher education in the field of IS have been defined. These qualifications must be met prior to working in the banking sphere. These qualification requirements have universality and do not depend upon national peculiarities of banking systems. Additionally, the process of formulation of qualification requirements could be used for definition of qualification requirements for specialists dealing with other typical objects. Higher education institutes can use the defined qualification requirements for specific training plans and contents of training.

References

1. The Standard of the Central Bank of Russia "Ensuring Information Security for Organizations of Banking system of the Russian Federation. Basic principles." STO BR IBBS-1.0-2006.

This Page intentionally Left Blank