HIGHLY QUALIFIED INFORMATION SECURITY PERSONNEL TRAINING IN RUSSIA

V.Gorbatov, A.Maluk, N.Miloslavskaya, A.Tolstoy

Moscow Engineering Physics Institute (State University)

{milmur; ait}@mephi.edu

Abstract: Highly qualified personnel training is one of the priority national tasks in the field of education, which is aimed at supporting the specified level of the personnel potential for fulfilling scientific research and teaching in the system of higher education. Extensive experience in that field has been accumulated in Russia. The general organizational requirements of the existing Russian system as a whole, as well as intensional peculiarities of candidate and doctor of sciences in scientific specialties' related to information protection and information security training are posed in this report.

Key words: highly qualified personnel training, security education, information security, thesis requirements, Russia

1. THE SYSTEM OF HIGHLY QUALIFIED PERSONNEL TRAINING IN RUSSIA

The process of highly qualified personnel training is carried out in large research institutions, leading universities and other institutions of higher education. The basis of training is formed by the system of state certification which is organized by the social-state authority, namely Higher certification committee of the Russian Federation (HCC of Russia), operating at the Ministry of Education of the Russian Federation. The HCC of Russia issues normative documents regulating activities in the considered field of educational services, creates social boards carrying out the main certification procedures, and adopts final decisions on giving the corresponding

qualification to candidates.

Russian system of certification is based on the two-stage technology of giving qualifications by results of successful defense of scientific-qualification grace papers (theses): “candidate of science” (the first stage) or “doctor of science” (the second stage). To pass the second stage it is obligatory to defend the candidate of science grace thesis first.

According to the HCC of Russia a candidate’s thesis should either include a solution of an essential problem in the given area of knowledge or state scientifically founded technical, economical or technological innovations having vital importance for the country’s economy.

Doctor thesis should include either results of scientific research a collection of which could be qualified as a new scientific achievement, or solution of a big scientific problem having significant social-cultural or economic significance, or state scientifically founded technical, economical or technological solutions whose implementation would bring an important contribution to country’s economy development.

An obligatory condition of presenting a candidate of science grace thesis is successful sitting for at least the following three examinations: scientific specialty, philosophy, and foreign language.

As a rule, highly qualified personnel training, involving realization of specific scientific-research work, education, and sitting for disciplinary examinations similar to the candidate level, is carried out by including candidates in post-graduate studies founded at leading scientific institutions, universities and other educational-scientific centers. Duration of post-graduate studies is three years internally and four years without isolation from the main job (by correspondence course). State budget form of training at the expense of state financial support and contract form of training at the expense of candidate’s funds are distinguished depending on the method of payment. Carrying out post-graduate student training, being one of the forms of educational services, requires obtaining a license from the Ministry of Education of Russia.

Each thesis is implemented within a definite scientific field whose list totals 25 titles. For example, in the field of information security it could be physico-mathematical sciences, technical sciences, and legal sciences. These titles are accordingly added to the scientific degree (e.g. candidate of technical sciences, doctor of physico-mathematical sciences).

2. THESIS REQUIREMENTS

The HCC of Russia determined that a person competing for a candidate or doctor scientific degree should hand in his thesis to the corresponding

board in the form of a specially prepared typescript or a published monograph.

The thesis should be written by the author himself, include a collection of new scientific results and statements proposed by the candidate for the public defense, have inner uniformity and be evidence of the author's personal contribution to science.

The new proposed by the author solutions should be consistently argued and critically evaluated in comparison with other known solutions.

A thesis having applied significance should include information about practical use of scientific results obtained by the author, whereas in a thesis having theoretical significance – recommendations for use of scientific conclusions.

The main scientific results of a thesis should be published in scientific editions recommended by the HCC of Russia.

3. HIGHLY QUALIFIED PERSONNEL TRAINING IN THE FIELD OF INFORMATION SECURITY

There is only one specialty related to information security in the list of scientific specialties approved at the level of public administration authorities: "Methods and systems of information protection, information security". That specialty requirements are formulated in the so called "specialty passport". That document approved by the HCC of Russia establishes the list of problems which should be solved by the candidate in his scientific research corresponding to this specialty, determines the role (significance) of the specialty, indicates the fields of science to which belongs the specialty, and defines its place among other specialties.

Scientific research dealing with the problems of analysis, development, use and perfection of methods and means of information protection in the process of its gathering, storage, processing, transfer, and distribution as well as technical, organizational, and legal support of state, community and personality information security relate to the considered specialty "Methods and systems of information protection, information security".

Scientific research within that specialty should be important for solving methodical, scientific-technical and organizational-legal problems on the basis of design of new and development of existing methods and means of information protection to ensure information security of technical, social-economical, biological and other systems of any kind and different areas of application, to perfect and develop the corresponding legal regulation as well as forms and methods of confrontation with violations in the informational realm.

Here is a list of fields of research which may be carried out within the concerned specialty:

- analysis of fundamental problems of information security in the process of formation of modern informational society, providing the balance of personal, social and governmental interests in the informational area;
- methods, models and means research and development for detection, identification and classification of threats of information security violation of objects of different kinds and classes;
- analysis and scientific reasoning of public and local authorities' main lines of activities in providing the information security of the Russian Federation, including development and perfection of monitoring system of the Russian Federation's information security status;
- study and prediction of consequences of modern information technologies incorporation and wide proliferation, including development of personality and society informational-psychological security methods and models;
- scientific reasoning and development of organizational-legal mechanisms for securing constitutional rights and freedoms of citizens in the informational area, with these rights and freedoms regulating creation and use of informational resources, means of information protection, assessment, standardization, information and informational resources quality certification and control, high-technology area crimes prevention and investigation, federal, subjects' of the Russian Federation and local authorities cooperation in the informational area, countries' cooperation for providing collective information security;
- protectability analysis of information circulating in the various existing systems of documents circulation. Development of methods and means of information protection in the systems of electronic documents circulation including cases of use of digital signatures and other cryptographic methods and means for providing electronic payment and electronic commerce systems' information integrity;
- design of measures and mechanisms for information security policy formation and support for objects of all hierarchy levels of different control systems;
- development of general theory of information security and information protection with various technical, organizational and legal methods and means including foundations and project solutions (technical, mathematical, organizational, legal, etc.) for prospective means of information protection and information security creation;
- analysis and risk management, evaluation of possible damage as a result of information security breach, and vulnerabilities of systems of any kind and field of application including models and methods of evaluation of

information protectability and information security of objects of various classes, information security systems' and complexes' efficiency;

- development of theory of conflict functioning of informational-telecommunicational systems (ITCS) of any kind and field of application;
- research of new physical processes and effects allowing to increase the ITCS security;
- development of technologies of ITCS users' and subjects' identification and authentication, access control, antivirus and ITCS destructive software influence protection;
- creation of computational systems, models, methods and means of providing stability and protection for data object, database and metadata creation at various stages of their lifecycle. Research and development of methods and means for protecting ITCS data and knowledge bases;
- synthesis of integrated ITCS information security systems including means of automated design targeted at their security increase;
- research and development of models, methods and means (complexes) of passive and active information counteraction to information security threats in networks, including such open networks as the Internet, providing inner audit and monitoring of status of ITCS being under the influence of information security threats, ITCS information security management;
- research and creation of models of technical covert channels, design of the corresponding counteraction means. Development of methodology of technical information protection for objects of any kind and field of application;
- design of methods and systems of technical information protection including the necessary algorithmic support, analysis and synthesis of analogous and digital signal processing means for the sake of objects' information security;
- creation of quantitative methods and models of legal and normative base analysis and evaluation. Research of offense dynamics, development of forms and methods of crime control in the field of information security and information protection.

4. HIGHLY QUALIFIED PERSONNEL TRAINING EXPERIENCE IN MEPHI

Highly qualified personnel training in the field of information security has been launched in the Moscow Engineering Physics Institute (State University) (MEPhI). Post graduate courses in specialty “Methods and systems of information protection, information security” and a board for

candidate and doctoral thesis protection in two fields of science – technical and legal – are available in the university. In future it is planned to broaden the board privileges by adding the physico-mathematical sciences branch. The post graduate studies are attended by graduate students of the MEPhI's Information Security Faculty, who successfully finished the full educational course and obtained the higher education in the specialty “Complex maintenance of automated system information security” or “Jurisprudence”.

Other theses prepared in different scientific and educational centers lacking dissertation boards are also accepted for defense.

A list of several theses' topics defended recently is given as an example in the conclusion:

1. Research and development of algorithms of secure information access in data storage networks.

2. Research of information protection means' trustworthiness in automated systems of depository services.

3. Development of algorithms for software cryptographic transforms' modeling and analysis.

4. Research and development of design methods of complex object security systems.