Cybersecurity

National Research Nuclear University MEPhI (Moscow Engineering Physics Institute)

Degree or qualification is awarded: **Bachelor degree**

Language of study: **Russian**
Mode of study: **full-time**
Duration: **4 years**
Availability of free education: **yes**
Price: **91 000 – 110 900 rubles per semester**

Programme curator: **Vitaliy G. Ivanenko**
Tel.: **Contact name: Olga N. Petukhova, Phone number. +74957885699, ext. 8045**
E-mail: ONPetukhova@mephi.ru

Brief description of the curriculum

List of Special Subjects:

- Fundamentals of information security;
- Computer hardware in information security;
- Software and hardware means of information security;
- Cryptographic means of information security;
- Management and legal aspects of information security;
- Technical protection of information;
- Nets and systems of information transfer;
- Safety of life activities;
- Programming languages;
- Technologies and methods of programming;
- Administration of information security;
- Document flow;
- Electrical engineering, electronics and microelectronics;
- Information technologies;

- Theoretical basics of cybersecurity;
- Steganography;
- Methods and protection means fr om destructive interactions;
- Psychology in ensuring cybersecurity;
- Counteraction to internal threats;
- Information protection in electronic payment systems;
- Cloud infrastructures and services;
- Attacks on mobile phones and commuters.

Practical Research:

The training practical research is conducted during the sixth and seventh terms as theory studies.

The training practice at the institutions and laboratories takes place during the eighth term.

The institutions wh ere practical studies occur are Rosenergoatom Corp., Eleron, Center for Information Technologies and Systems, AK Central Research Institute of Control Systems, Luch Research and Production Association, Infotex, Mascom, the Dukhov All-Russia Research Institute of Automatics in Moscow and others.

Additional information

One of the priorities of the greater number of states is developing an information society on the basis of telecommunication technologies which in turn demands a complex infrastructure to provide electronic services for the population. Such a task in Russia can be quite realizable since computers, mobile means of communication, software and telecommunication systems cover practically all spheres of human activities, society and state.

Along with it, the scientific progress and development and global distribution of digital technologies, the Internet in particular, have brought about launch and propagation of cyberthreats. Now an ever growing number of criminals try to use technical potentials of computer, software and the Internet, and mobile systems. In the experts’ evaluation the rates of cyber crime in the Internet are growing fastest on the planet.

According to the data of Kaspersky Lab Ltd., up to 70 000 new malware programs appear annually. The list of potent threats includes spum, phishing, network attacks on companies, infrastructures as well as target and DDoS attacks and potential vulnerability in software. Incidents in IT security frequently result in losses of financial data (13%), intellectual property (13%), client bases (12%) and confidential staff information (12%).

Professional activity of the cybersecurity centers on the scientific area, technologies and methods related to the problems of ensuring cybersecurity and protection of information systems in different threat scenarios.

The Department Graduate must be competent in

- revealing the essence of the problems arising in the professional activity, using general science laws and applying mathematics apparatus in information professional tasks;
- interpreting the essence and significance of information in modern society, in applying information

technologies, in searching for target information in various sources and global computer systems;

- using legal recommendations in the professional area;
- managing a supporting a set of measures to ensure information security accounting for the legal justification, administrative and technological implementation and economic efficiency, possible outside penetrations, threats and level of protection technologies;
- testing objects following the requirements of state and company policies;
- participating and developing the subsystems of control, management and operation;
- participating in preliminary analyses of technical-economic feasibility to ensure cybersecurity;
- compiling technical specification taking into account current regulations for information security;
- programming solutions of common algorithms to ensure information security and applying software of system, application & special types;
- analyzing the phenomena and processes under study and design solutions;
- analyzing the information security objects and systems using national and foreign standards;
- experimenting using a prescribed procedure, processing the data, evaluating events and determining errors and credibility of the results obtained;
- searching, referencing and generalizing scientific and technical literature and recommendations on the problem of cybersecurity;
- developing technologies to improve the management system information security;
- forming and developing a set of measures (rules, procedures, practical recommendations) to manage information security.

The program realized at the department permits students later to continue studies for the qualification of Master of Science:

The customized programs are motivated by the President's Acts and decisions of Scientific and Technical Council of the Military and Industrial Complex of 2011-2013.

The major programs include "Training Specialists for Scientific Centers", "Innovation Development Program of Rosatom St. Corp." and for the priority direction "Technologies of Processing, Storage, Transmission and Protection of Information" in accordance with the Directives of the RF Security Council on the Strategy of Development of the RF Information society, the Priorities Problems in the research of Information security in the RF, the main trends of research in ensuring the RF information security, etc.

The graduates can apply for employment at Rosenergoatom Corp., Greenatom Ltd., Scientific Research Institution of Atomic Power Stations, Federal Service of Russia, Central Bank of the RF, Federal Center of Information Technologies and Systems., AK Central Scientific Research Institute of Control Systems, Inpartex Co., CryptoPro Ltd., Active Ltd., Institute of Informatics of the Russian Academy of Science, Atlas NSC, Crok Incorporated, Kaspersky Lab Ltd., Russian Savings Bank, Vneshtorgbank, Vnesheconombank, Gusprombank, Russian Standard Bank, Lins M Co., Amicon Co., Factor IT Co., etc.

Specializations within this programme

Objects of the professional activity

- computers, automated, telecommunication, information and information analytical systems, information resources and information technologies operating under cyberthreats in the IT sphere;
- technologies providing cybersecurity of various level objects (a system, a system object, and object component) related to IT used at such objects;
- control processes of information security in the objects under protection.

A great numbers of classes are conducted in specialized laboratories equipped with modern hardware and software devices

A specific aspect of the Program is that along with the compulsory disciplines students do customized programs of subjects introduced by the MEPhI at the request of employers.