ITMO University

Foundations of information security

Course Workload		Assessment form (examination/ graded test/ ungraded test)
ECTS	Hours	
3	108	Exam

This course is an introductory course for a cycle of professional disciplines in Information Security sphere. It is intended to introduce students of the master's program who have not received basic degree in the field of Information Security as well as to determine the future directions of master's training and dissertation and the choice of specialization.

Course structure:

1. Scientific and methodological, organizational and legal bases of information security

---

1.1. The concept of information security. Computer information security as an integral part of information security.
1.2. Types of possible violations of information system security. The concept of information security of the Russian Federation. The place of information security in the national security of the country.
1.3. Organizational support for the protection of confidential information. The main regulatory and reference documents on the protection of state secrets and information security in the Russian Federation.
1.4. Types of confidential information. State, commercial, professional and official secrets. Personal data. The main organizational methods and means of protecting confidential information.

2. Technological foundations of the design and operation of secure information systems

---

2.1. Types of threats of information system security. Taxonomy of information security violations. Random threats. Deliberate (intentional) threats. Technical channels of information leakage.
2.2. The concept of unauthorized access to information. The intruder's model. Types of malicious software. Requirements for software and hardware protection against unauthorized access. Features of protection against unauthorized access for computer equipment and automated systems.

2.3. Access control system. Security classes of computer equipment. Security classes of automated systems. Security requirements for automated systems designed to process classified information. User identification. The concept of system policy. Password management systems. User authentication. Biometric systems.
2.4. Methods and means of ensuring data integrity. Data archiving and backup. Types of archives. Software tools for creating and maintaining electronic archives. Methods of data backup. Schemes of rotation of information media. Comparative characteristics of backup storage devices. RAID technology. Software tools for data backup and recovery.
2.5. Uninterruptible power supplies. Classification and application features.
2.6. Computer viruses. Features of computer viruses compared to other types of malicious software. Classification of computer viruses. Variants of software implementation of computer viruses. Means of detecting and countering computer viruses.
2.7. Classification of antivirus software. Principles of anti-virus programs. Modern antivirus software.

3. Basics of cryptography

3.1. Cryptographic systems. Main principles of cryptography. Types of cryptographic systems. Symmetric cryptosystems. Asymmetric cryptosystems.
3.2. Key management. Foreign and domestic encryption standards. Modern cryptographic software tools.
3.3. Digital signature. Legal basis for the use of a digital signature. Technology for creating and applying a digital signature. Organizations issuing electronic certificates.
3.4. Steganographic systems. Principles of steganography. Types of steganographic systems. steganographic software

4. Promising directions for the development of information security systems

4.1. Prospects for the development of information security systems. Advanced trends and solutions in the field of information security. Soft information security. Non-classical directions of ensuring information security of business processes.