|  |  |
| --- | --- |
|   | **Course Syllabus** |

**1.** **Course Title:**

Information security technologies

**2. Academic Level:**

Bachelor

**3. ECTS Credits:**

5 ECTS

**4. Semester:**

3, autumn semester

**5. School/Department:**

[Institute of Computer Technologies and Information Security](http://ictis.sfedu.ru/)

**6. Location:**

Taganrog Campus, 2 Chekhov St., Taganrog

**7. Instructor:**

Associate Prof. Ekaterina Pakulova, email: epakulova@sfedu.ru

**8. Language of Instruction:**

English

**9. Course Description:**

The course goal is to form a system of knowledge about the problems of security of information technologies, methods and means of information security and obtaining the skills to work with them.

**10. Course Aims:**

The objectives of the course are to get knowledge about:

* possible data security threats and vulnerabilities of information systems;
* classification of information security methods and means;
* information security standardization;
* organizational and legal support of information security;
* cryptography methods and means;
* authentication methods and means;
* authorization methods and means;
* methods and means for providing security of operating systems;
* anti-malware means;
* methods and means for network information security;
* information security technical means.

**11. Specific entry requirements (if any):**

The course “Information security technologies” is based on knowledge, skills and abilities, acquired by students based on the previously obtained knowledge in the following disciplines: discrete mathematics, operation systems and algorithm development and programming.

**12. Course Content:**

**Module 1**

Part 1. Basic concepts and definitions. Information systems vulnerabilities and threats. Data protection criteria and standards.

* + - 1. Basic concepts and definitions. Information systems vulnerabilities. Information Security. Protection of information. The main components of information security. Computer security. Subject-object model. Threats and vulnerabilities of information systems. Classification of security threats for information systems. Methods for assessing security threats of computer networks. Classification of intruders. Intruder model. Classification of channels of penetration into the system and information leakage. Classification of methods and means of information protection.
			2. Data protection criteria and standards. Data protection criteria and standards. Basic concepts and principles of the Common Criteria. Security functional requirements. Security Trust Requirements. Other standards of the Russian Federation.

Part 2. Authentication methods and means. Access control. Security Policies and Models.

* + - 1. Authentication methods and means. Basic concepts in identification and authentication technologies. Password authentication. User authentication based on the handshake model. Personal means of authentication. Biometric Authentication Tools. Authentication by information associated with the subject.
			2. Access control. Security policy and model. Subject-object model. Security monitor. Security policies. Security models. Discretionary security models. Mandatory security models. Role-based security models.

Part 3. Technical information protection.

* + - 1. Technical channels of information leakage. Classification and characteristics of technical channels of information leakage. Classification and characteristics of technical channels of acoustic (speech) information leakage. Technical channels of information leakage during its transmission through communication channels. Covert video surveillance. Means of reconnaissance photography and photographic documentation.
			2. Portable technical reconnaissance equipment. Portable acoustic reconnaissance equipment. Portable means of radio and electronic reconnaissance. Espionage tools. Vehicle tracking systems. Autonomous portable technical reconnaissance equipment.
			3. Methods and means of protection against technical reconnaissance. Search for radio frequency bugging device. Methods and equipment for protecting telephone lines. Means for unauthorized access protection to acoustic information.

Part 4. Organizational and legal support of information security.

* + - 1. Organizational and legal support of information security. Basic definitions in the field of information law. Classification and types of information resources. Confidential information. National Security Information and its protection. Proprietary information and trade secrets protection. Legal protection of professional and official secrets. Legal basis of the licensing and certification system. Licensing of activities for the protection of National Security Information. Information security certification. Licensing and certification in the field of confidential information protection. Cybersecurity.

**Module 2**

Part 5. Cryptography methods and means of information security and cryptanalysis

* + - 1. Symmetric cryptosystems. Strength of cryptographic systems and algorithms. Basic methods of cryptanalysis of ciphers. The simplest ciphers and their basic properties. The main classes of symmetric cryptographic systems. Stream ciphers: basic requirements, modes of operation. Block ciphers: basic security requirements and operation modes. Basic structures of block ciphers: SP-networks and Feistel networks. The Russian standard for block encryption "Kuznechik": basic parameters, structure of the encryption round and the principle of operation, the procedure for expanding the initial key into round (working) subkeys, modes of use. Security provided by modern ciphers. The reasons for the unreliability of cryptographic systems.
			2. Hash functions. Feature assignment and basic requirements. Hash functions SHA-3 and GOST R 34.11-2012 (Streebog): basic parameters, structure, and principle of operation of the transforming function. Strong authentication methods. X.509 standard. Authentication protocols with symmetric encryption algorithms. Needham-Schroeder authentication and key distribution protocol.
			3. Asymmetric cryptosystem. Basic requirements, One-Way Functions, and Trap Functions. El Gamal and Rivest-Shamir-Adleman (RSA) asymmetric cryptographic systems. An asymmetric cryptographic system based on the Diffie-Hellman problem. Electronic digital signatures: basic requirements, electronic digital signature algorithms. Digital signatures based on asymmetric cryptographic algorithms. Digital certificates. Management of cryptographic keys using certificates. Strong authentication, based on asymmetric encryption algorithms.

**13. Intended Learning Outcomes:**

By the end of the course students should

know:

* possible data security threats and vulnerabilities of information systems;
* classification of information security methods and means;
* information security standardization;
* organizational and legal support of information security.
* cryptography methods and means;
* authentication methods and means;
* authorization methods and means;
* methods and means for providing security of operation systems;
* anti-malware means;
* methods and means for network information security;
* information security technical means;

have skills in:

* developing basic requirements for information security with modern information and communication technologies;
* task solution in information security with modern information and communication technologies.

**14. Learning and Teaching Methods:**

The discipline provides with a combination of traditional educational technologies in the form of lectures and with interactive elements, information technologies during laboratory work and control activities.

Lectures are conducted in the form of an electronic presentation of the discipline materials, which is preliminarily distributed among students. The electronic presentation covers the basic concepts of the studied discipline. As a result, before each lecture, students have the opportunity, within the framework of independent work, to get basic ideas on the topic of the lecture. At the lecture, the main provisions and basic concepts are supplemented with the necessary explanations, details, examples, and discussion of the problematic issues.

Laboratory work covers the main sections of the discipline. It is held with a variety of software tools (educational software packages, interactive platforms, software emulators) and hardware and software tools (personal authentication tools, access control tools, information leakage channel control tools). Laboratory work defense is organized in an interactive form using practical examples and situations in the field of the security of information.

Along with traditional educational technologies, for the implementation of the discipline, e-learning technologies can be used, including the ICTIS e-learning system (lms.sfedu.ru). Classroom lectures and other forms of contact work of students with a teacher can be conducted using platforms Microsoft Teams, Cisco, Skype, Google Classroom, Zoom, etc., which allows for online and offline interaction of the teacher with the students.

The main methods of current control are electronic recording and monitoring of students' educational achievements (using the service of the point-rating system; maintaining an electronic journal of progress and using other means of control using the e-learning system).

**15. Methods of Assessment/Final assessment information:**

Laboratory works, tests. Summative assessment method: graded test

**16. Reading List:**

1**.** Ali Ismail Awad, Michael Fairhurst. Information Security : Foundations, Technologies and Applications. The Institution of Engineering and Technology; 2018. Accessed May 14, 2021. <http://search.ebscohost.com/login.aspx?direct=true&AuthType=shib,sso&db=edsebk&AN=1805102&lang=ru&site=eds-live>

2. Security in Computer and Information Sciences. Springer Nature; 2018. doi:10.1007/978-3-319-95189-8. Accessed May 14, 2021.

**Additional reading list**.

1. Scholz P. Information Security: Cyberattacks, Data Breaches and Security Controls. SNOVA; 2019. Accessed May 14, 2021. <http://search.ebscohost.com/login.aspx?direct=true&AuthType=shib,sso&db=edsebk&AN=2225637&lang=ru&site=eds-live/>

2. Malcolm W. Harkins. Managing Risk and Information Security: Protect to Enable (Second Edition). Apress; 2016. doi:10.1007/978-1-4842-1455-8. Accessed May 14, 2021.

**Online resources**

1. Information security courses/ [https://www.coursera.org/courses?query=information%20 security](https://www.coursera.org/courses?query=information%20%20security). Accessed May 14, 2021

2. Blog of DANIELMIESSLER https://danielmiessler.com/. Accessed May 14, 2021.