FACULTY OF COMPUTER SCIENCE AND ENGINEERING

CURRICULUM

Confirmed:
Dean:

CS319

INFORMATION SECURITY

Updated: protocol № 7/30.01.2019

Lecturer: Assoc.Prof. Veselina Zhecheva, PhD

ANNOTATION

The course aims to clarify and expand in the necessary depth concepts from the field of information security, the main threats and vulnerabilities, as well as prevention and protection methods. The discipline ends with the defense of a coursework and an exam.

BASIC PURPOSES

The main goal of the course is to develop students' knowledge and skills for analysis and assessment of information security in computer networks and systems.

After studying the course, the student will:

• know the main problems related to the security of the contemporary systems;

• analyze and assess security threats and risk;

• can apply methods and means to increase information security;

• has expertise to further develop their qualification on the subject.

PREREQUISITES

Students should have a very good level of computer literacy, a very good idea of the structure and organization of processes on the Internet, as well as the corresponding very good mathematical knowledge to analyze the problems related to information security. The course requires prior knowledge of Programming, Operating Systems, Web technologies and applications, and Mathematics. Knowledge of computer networks and communications is useful. The knowledge obtained from the course is used as a basis for the course Security of corporate networks in the master's program.

STATUS AND STRUCTURE

PROGRAMME	status	ECTS	Full time				Part time			
			л	с	у	общ	л	с	у	Общ
Computer Science	Mandatory	4	20	20		40	10	10		20
Software Engineering	Mandatory	4	20	20		40	10	10		20

COURSE CONTENT

Topic 1. Introduction. Problems facing the information security in a networked environment. Tasks and elements of information security. Security aspects. System objects and subjects.

Topic 2. Defense design and creation process. Vulnerabilities and threats. Types of threats. Passive and active attacks. Threats related to the confidentiality and integrity of information.

Topic 3. Security policy. Types of security policies. Assessing the value of information. Risk analysis.

Topic 4. Defense mechanisms. Identification and authentication mechanisms. Two-factor and multi-factor authentication. Use of a trusted third party.

Topic 5. Defense mechanisms. Access control mechanisms. Partition mechanisms in the system. Communication mechanisms. Breach detection and incident recovery mechanisms.

Topic 6. Malware. Malware types and origins. Viruses, worms, Trojan horses. Spyware and adware. User activity tracking software. Spam. Extortion related attacks.

Topic 7. Malware. Fraud related attacks. Tracking attacks. Exploits. Denial of service attacks. Full exhaustion attacks. Dictionary attacks. Extortion related attacks. Attacks related to the manipulation of industrial systems.

Topic 8. Security software. Antivirus programs. Firewalls. Firewall architecture. Types of architectures. Minimum level of protection.

Topic 9. Encryption. Basic concepts. Types of algorithms. Hash functions. Digital signatures and digital certificates. Standards. Basic encryption programs.

Topic 10. Intrusion detection systems. Purpose and main applications. Types of breach detection and prevention systems.

Topic 11. Virtual private networks. Tunneling and Encapsulation, Technical Concepts and Implementation. Secure protocols.

Topic 12. Standards for information security. Monitoring and auditing of the system.

SEMINARS

Topic 01. Hacker attacks. The simplest attack. The massed attack. Hyperlink scams.

Topic 02. Kerberos keys. Getting to know Kerberos. The Kerberos protocol. The Kerberos database.

Topic 03. Internet trade protection. Basic questions. Digital cache. Credit cards.

Topic 04. Use of audit (surveillance) as protection. Types of monitoring tools. Monitoring in Linux. Monitoring in Windows.

Topic 05. Computer viruses. Basic mechanism of operation. Types of computer viruses. Virus scams.

Topic 06. Security of browsers. Types of vulnerabilities. Types of protections.

Topic 07. Security policy planning. Types of security policies. Specific rules. Violation reactions.

PLANNED LEARNING ACTIVITIES AND TEACHING METHODS

Training methods:

Face-to-face lectures and seminars

Visual learning

Practical Education

Interactive learning

E-learning through the Moodle platform

Teaching tools:

Self-paced work

Educational video materials incl. video presentations

Practical tasks

Programming tasks using application software

Use of electronic resources in the Moodle platform: theoretical materials, presentations, sample programs, tests and tasks for self-paced work on each topic

COURSEWORK

The course assignment is assigned to each student and contains tasks on analysis and assessment of current information security problems. It is chosen by the student and consulted with the teacher. Each student presents his course assignment and receives a grade characterizing the level of mastery of the learning material.

ASSESSMENT METHODS

- Each student develops a personal course assignment, representing a study of a specific problem in the field of information security. The task includes independent development of a certain topic from the subject of the discipline. The implementation and protection of the development are evaluated - up to 30 points. The criteria for evaluating the development are: originality, thoroughness of the research, complexity of the topic, presentation of the development.
- For original ideas presentation - up to 10 items.

- Up to 6 points are awarded for attendance and participation in the exercises.
- The exam is written and is a test with open-ended questions, which is evaluated with a maximum of 54 points. The final evaluation includes the total of ongoing control of the seminar exercises, an evaluation of the course work and an evaluation of the written exam. To form the grade, the student collects points, the maximum value of which is 100. The final grade is formed by distributing the points on the scale:

1. Face-to-face assessment..... .... 16 points

1.1. Control work - 10 points

1.2. Seminars - 6 points

(presence and participation in seminars)

2. Outside classroom employment .... … 30 points

2.1. Course assignments – 2 pcs. - 20 points

2.2. Homework - 10 points

3. Final exam……..... .... 54 points

The student must have a minimum of 14 points from the control during the semester and a minimum of 22 points from the examination procedure in order to form a comprehensive assessment. The final grade is formed by distributing the points on the scale:

• from 54 to 60 points - Medium (3);

• from 61 to 70 points - Good (4);

• from 71 to 80 points - Very good (5);

• from 81 to 100 points - Excellent (6).