



Faculty: FACULTY OF TELECOMMUNICATIONS AND MANAGEMENT

Department: INFORMATION TECHNOLOGIES

Professional Field: 5.3 COMMUNICATION AND COMPUTER TECHNOLOGY

Specialty: CYBER SECURITY IN BUSINESS

Educational-qualification degree: BACHELOR

LEARNING COURSE DESCRIPTION

1. Course title: Cyber crises and cyber threats

2. Course code: B.47.017.1

3. Type of the course: Compulsory

4. Level: Bachelor

5. Year of study: Second

6. Semester: Third

7. Number of credits: 6

8. Name of the lecturer(s): Svetlin Lazarov

9. Course learning outcomes:

The aim of the course is to provide students with basic knowledge in the field of cyber threats and cyber crises.

Students who have completed the course should acquire:

Basic knowledge of:

- Types of cyber threats;
- Mechanisms for sharing information in a cyber-incident;
- Preventing and dealing with cyber crises;
- Countering cyber threats;
- National and international response to a cyber-incident.

The practical skills that students should acquire and develop during the course are related to the specifications and counteraction of cyber threats and the management of cyber crises.

Competencies: After the successful completion of the course students shall partially mastered the theoretical and practical possibilities for action in cyber threats and cyber crises.

10. Teaching methods:

The course "Cyber Threats and Cyber Crises" is taught in the third semester according to the current curriculum through lectures grouped in two lessons per week for 15 weeks and practical exercises grouped in two lessons per week for 15 weeks.

During the lectures, students build their theoretical knowledge by participating in seminar exercises and independently preparing a response plan for cyber threats, cyber incidents and cyber crisis. The lectures are illustrated with graphic material presented through multimedia projector presentations and supplemented with examples and assignments. Seminar exercises are conducted in a departmental laboratory equipped with computers.

11. Prerequisites:

Students should have prior knowledge of Security Fundamentals and Information Security Standards, Networks and Protocols, and E-Crisis Management.

Courses using the discipline include: Information Security in E-commerce, Wireless Communications Security, E-management in Crises, Cybersecurity Policies, Hacker Attacks and Tools, Introduction to Cloud Technologies, Technical Security Systems, Criminal Justice Aspects of Cybersecurity, Protection of Classified Information, Electronic Payment Card Security.

12. Course contents:

The course curriculum presents cyber threat technology, cyber incident investigation and cyber crisis management in relation to the specifics of the specialty. *Section one* of the syllabus introduces basic concepts and defines the problem area. Methods for identifying threats, determining the type and source of the threat are presented, threat analyses are performed, and current issues and challenges in cyber terrorism and cyber culture in information networks and systems are discussed.

Section two discusses critical infrastructure protection mechanisms, SCADA system protection mechanisms, mobile cyber incidents, and incident reporting methods.

Section Three discusses crisis stages and Computer Incident Response Teams. Attention is also paid to the regulation in Bulgaria for incident response, the cyber security law and the national cyber security strategy. International cyber crisis response activities and the activities of the Cyber Security Centre of Expertise in Europe are also analyzed. Methods of testing for vulnerabilities in computer systems and networks, making recommendations for protection and maintaining and updating information systems are studied.

13. Bibliography

Basic literature:

1. National Cyber Security Strategy;
2. Cybersecurity Act;
3. The European Data Protection Regulation
4. Materials of the European Network and Information Security Agency (ENISA);
5. The Red Book. A Roadmap for Systems Security Research, SysSec Consortium, September, 2013, <http://www.red-book.eu>.

Additional literature:

1. Computer Security Fundamentals (3rd Edition) (Pearson IT Cybersecurity Curriculum (ITCC) 3rd Edition;
2. Computer Network Security and Cyber Ethics, 4th Edition;
3. Cyber-security of SCADA and Other Industrial Control Systems, Springer International Publishing AG;
4. The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities (Wiley Finance).

14. Assessment methods and criteria:

The course ends with an ongoing assessment.

1. Requirements for the assessment of the six-point system

Weight of the assessment: 50% of the test and 50% of the written work.

2. Formation of the final mark

Based on demonstrated knowledge from the test and written work.

Excellent (6) - for good knowledge of information sources, thorough mastery of key and complementary knowledge and skills, meaningful and correct understanding of the subject matter, complex problem solving skills, independent thinking and reasoning.

Very good (5) - for very well mastered key and additional knowledge, meaningful and correct understanding of the material, skills to apply what has been learned in complex cases and tasks.

Good (4) - for having mastered key and additional knowledge to solve cases and problems, but without being able to develop it to independent thinking.

Average (3) - for mastering key knowledge and solving typical problems.

The subject tests consist of 75 closed questions, with five possible answers, only one of which is correct.

Forming an assessment in the training course at each of the above stages, according to the points obtained and their ranking according to the six-point system is given in Table 1.

Table 1.

Number of points	Assessment According to the 6-pointScale System
0 – 20	Fail 2 (F)
20 – 39	Fail 2 (FX)
40 – 49	Satisfactory 3.00 (E)
50 – 59	Satisfactory 3.00 (D)
60 – 69	Good 4.00 (C)
70 – 84	Very good 5.00 (B)
85 – 100	Excellent 6.00 (A)

15. Language of instruction: Bulgarian/English