

Faculty: FACULTY OF TELECOMMUNICATIONS AND MANAGEMENT
Department: INFORMATION TECHNOLOGIES
Professional Field: 5.3 COMMUNICATION AND COMPUTER TECHNOLOGY
Specialty: CYBER SECURITY OF HIGH TECHNOLOGIES
Educational-qualification degree: PROFESSIONAL BACHELOR

LEARNING COURSE DESCRIPTION

1. Course title: PRACTICE ON INFORMATION AND TECHNOLOGICAL SECURITY

2. Course code: P.18.014.2

3. Type of the course: elective

4. Level: Professional bachelor

5. Year of study: 1

6. Semester: 2

7. Number of credits: 3

8. Name of the lecturer: Assoc. Prof. Dr. Eng. Ivan Ivanov

9. Course learning outcomes:

The aim of the course is to provide students with basic knowledge in the field of cyber security in a systematized form.

Students who have completed their studies in the discipline must acquire:

Basic knowledge of cyber space, goals and measures guaranteeing cyber security, cyber attacks, cyber security and cyber resilience, organizational measures and measures for the protection of information, technical systems and means of information protection, signaling and security systems, fire alarm systems, anti-virus protection of data in computer networks.

Practical skills for specifying cyberspace, analyzing cyber security goals and measures, analyzing information protection contours, developing organizational measures and measures for information protection, developing a plan for technical systems and means of information protection, configuring of alarm and security systems, configuration of fire alarm systems, detection and removal of virus infections.

Competences: After completing the course, students must have mastered the mechanisms and tools for achieving information-technological security.

10. Teaching methods:

The lectures are conducted by acquainting the students with the material provided in the curriculum. The lectures are illustrated with graphic and video material, with illustrative examples and tasks, which are presented through presentations with a multimedia projector.

The practical exercises are conducted in the laboratories of the department, equipped with modern computers and network devices, and each student works independently.

Before each practical session, students are informed about the need for preliminary training on the topic.

11. Prerequisites:

Students should have a thorough knowledge of security fundamentals. The knowledge acquired in the disciplines Basics of security and standards for information security and Basics of electrical engineering is essential.

12. Course contents:

The course examines current topics related to the specification of cyber space, analysis of cyber security goals and measures, analysis of information protection contours, application of basic cryptographic procedures, development of organizational measures and information protection measures, development of plan for technical systems and information protection means, configuration of alarm and security systems, detection and removal of virus infections.

13. Bibliography

Basic literature:

1. National cybersecurity strategy "Cyber-resistant Bulgaria 2020".

- Ivanov I.. Fundamentals of Cryptography, VUTP Publishing House, 2021.
- Vacca J.R. Computer and Information Security Handbook, Third Edition 3rd Edition, Morgan Kaufmann, 2017.
- Andress J. The Basics of Information Security, Second Edition: Understanding the Fundamentals of InfoSec in Theory and Practice 2nd Edition, Syngress, 2014.
- Conklin W. A, White G, Cothren C, Davis R, Williams D, Principles of Computer Security, Fourth Edition (Official CompTia Guide) 4th Edition, McGraw-Hill Education, 2015.

Additional literature:

- Ivanov I. Manual for laboratory exercises on information security and protection and administration and protection of communication and computer networks, ed. center-VU KTP, Sofia, 2013, ISBN: 978-954-9332-88-9.
- Partyka T. JL, Popov I. I. Information security: textbook / T. JI. Partyka, I. I. Popov. — 3rd ed., revised. and add. — M.: FORUM, 2010.
- Gribunin V, G, Chudovsky V. V, Kompleksnaya sistema zashtiya information na przes, Publishing center "Academy", 2009.
- Meeuwisse R, Cybersecurity for Beginners, Cyber Simplicity Ltd, 2017.
- Kim D, Solomon M, Fundamentals of Information Systems Security 3rd Edition, Jones & Bartlett Learning, 2016.14.

14. Assessment methods and criteria:

The evaluation of the discipline is formed through a point system, the maximum number of points that students can receive is 100 (see table 1). Knowledge, skills and competence are evaluated by conducting written control works to check the theoretical and practical assimilation of the learning material, the performance of the students during the practical exercises, as well as their ability to independently solve the tasks set in the practical exercises. The discipline ends with a written exam.

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*