Faculty: FACULTY OF TELECOMMUNICATIONS AND MANAGEMENT
Department: GENERAL ENGINEERING
Professional Field: 5.13. GENERAL ENGINEERING
Specialty: DIGITAL ENTREPRENEURSHIP AND HIGH TECHNOLOGY
Educational-qualification degree: BACHELOR

LEARNING COURSE DESCRIPTION

1. Course title: *HIGH TECH CYBER SECURITY*
2 .Course code: B.45.067.3
3. Type of the course: *Facultative*
4. Level: *Bachelor*
5. Year of study: *Fourth*
6. Semester: *Seventh*
7. Number of credits: *3*
8. Name of the lecturer: *Assoc. Prof. eng. Ivan Dinkov Ivanov, PhD*
9. Course learning outcomes

The aim of the course is to give students an overview and to form basic knowledge necessary for conducting an in-depth study of aspects of cybersecurity of high technology.

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

Basic knowledge of information security and protection, legal framework for information protection, organizational measures and technical systems and means for information protection, antivirus data protection in computer networks, basic procedures and classification of cryptographic algorithms, cryptographic algorithms, technologies for network security and cyber attacks.

Practical skills for working with configuration and work with F-Secure Client Security Premium, F-Secure Policy Manager, implementation and research of substitution and transposition cryptographic procedures, DES, AES and RSA cryptographic algorithm, implementation and research of penetration tests in local network .

Competencies: Upon completion of the course, students must have mastered the basic concepts in the field of cybersecurity.

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 each student works independently. Before each practical session, students are informed about the need for preliminary preparation on the topic.

11. Prerequisites:

*Students should have k*nowledge of "Fundamentals of Information Technology" and "Fundamentals of Programming" and others. disciplines from previous semesters.

Courses using the discipline are all disciplines in the remaining semesters requiring knowledge and skills in the field of cybersecurity.

12. Course contents:

The course addresses the main legal, technical and organizational aspects of information security in today's digital world, enabling students to deal with future cases and developments in the field of cybersecurity.

13. Bibliography

Basic literature:

1. **Nancy R. Mead, Carol C. Woody.** Cyber Security Engineering, ISBN-13: 978-0-134-18980-2, 2017.
2. **Пролетарский А.В., Суров А.М., Смирнова Е.В., Руденков Н.А.** Технологии защиты информации в компьютерных сетях (2-е изд.) 2016.
3. **Dr. Erdal Ozkaya.** Cybersecurity: The Beginner's Guide, Packt Publishing (May 27, 2019).
4. **Charles J. Brooks,** Christopher Grow, Philip Craig, Donald Short. Cybersecurity Essentials 1st Edition, Sybex, 2018.
5. **Zach Codings,** Computer Programming And Cyber Security for Beginners, Independently published (December 4, 2019).

Additional literature:

1. **Brian Walker,** Cyber Security: Comprehensive Beginners Guide to Learn the Basics and Effective Methods of Cyber Security, Independently published (June 20, 2019).
2. **Elijah Lewis,** Ethical Hacking: A Comprehensive Beginner's Guide to Learn About the Effective Strategies of Ethical Hacking, Independently published (January 11, 2020).
3. **Elijah Lewis,** Cybersecurity: A Comprehensive Beginner's Guide to learn the Realms of Cybersecurity from A-Z, Independently published (January 11, 2020).

14. Assessmentmethodsandcriteria:

The course ends with an *ongoing assessment.* The individual and team work of the student during the exercises and the passed online tests is taken into account.

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

30% of the final grade is formed by the results of the current electronic tests, 20% is formed by the implementation of the practical exercises and 50% by the final test. The current tests and the final test are electronic and are published in the e-learning system of VUTP. These include open and closed questions. Some of the questions are related to solving cases in order to check the creative application of the acquired knowledge.

2. Formation of the final mark

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-point Scale 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*

1