

Faculty: FACULTY OF TELECOMMUNICATIONS AND MANAGEMENT
Department: INFORMATION TECHNOLOGIES
Professional Field: 5.3 COMMUNICATION AND COMPUTER TECHNOLOGY
Specialty: COMMUNICATION NETWORKS AND CYBERCRIME INVESTIGATIONS
Educational-qualification degree: MASTER

LEARNING COURSE DESCRIPTION

1.Course title: *Cyber operations*

2.Course code: *M.06.007.3*

3.Type of the course: *facultative*

4.Level: *master*

5.Year of study: *first year of study*

6.Semester: *first semester*

7.Number of credits: *6 credits*

8.Name of the lecturer: *Assoc. Prof. Aleksandar Tsenov, Ph.D.;*

9.Course learning outcomes:

The aim of the course is: students to become familiar with the essence, methods of implementation, the set of tools for implementing highly effective cyber operations for the protection of information, information systems and society as a whole.

Students who have completed their studies on the course should have acquired:

Basic knowledge of definition of cyber operations in specific real-life domains, stages of cyber operations, capability, knowledge and skill requirements of cyber operations teams, methods and tools for conducting cyber operations, differences between cyber security and cyber resilience

Practical skills to carry out cyber operations according to the rules defined at different stages and for different purposes

Competencies: upon successful completion of the course, students will be able to plan, execute and evaluate several types of cyber operations, in relation to specific tasks and conditions.

10.Teaching methods:

The lectures are illustrated with graphic and video material, with illustrative examples and tasks, which are presented through presentations with a multimedia projector.

Laboratory exercises are conducted in a computer class, with students developing pre-assigned tasks on the given topic.

Before each laboratory exercise, students are informed about the need for preliminary preparation on the topic.

Individual work

The VUTP e-learning site provides every student with access to lecture material, self-preparation tests and laboratory exercises, thematic plan, question card and additional materials.

Prerequisites:

Basic knowledge of computer systems, computer architectures, network architectures and operating systems

The courses using the discipline are:: *Identification of Cyber-attacks, Network Security, Information Security Management Systems, Threat Hunting with SIEM*

12. Course contents:

The course focuses on aspects of information security

Introduction to OSS / BSS

Cyber Security vs. Cyber Resilience

Stages of cyber operations

Cyber Operations Skill and Knowledge Requirements

Cyber Operations Center

Identifying different types of vulnerabilities

Design principles during system design, development and implementation to minimize vulnerabilities.

Information system security design

13. Bibliography

Basic literature:

1. Paulo Shakarian, Jana Shakarian and Andrew Ruef, Introduction to Cyber-Warfare, Syngress, ISBN 978-0-12-407814-7, DOI <https://doi.org/10.1016/C2012-0-06618-5>, Copyright © 2013 Elsevier Inc. All rights reserved, 2013
2. Stephen W. Korn, Cyber Operations: The New Balance, 54 Joint Force Quarterly 97 (2009). Web
3. David Anthony Bird (British Computer Society, UK), Real-Time and Retrospective Analyses of Cyber Security, ISBN13: 9781799839798| ISBN10: 1799839796| EISBN13: 9781799839804| Softcover: 9781799856023, DOI: 10.4018/978-1-7998-3979-8, 2020|

Additional literature:

1. Dimitri P. Bertsekas and John N. Tsitsiklis, "Introduction to Probability 2nd Edition Problem Solutions", Athena Scientific, Belmont, Massachusetts, 2019, 133 p.
1. Best Writer, The Stages of Cyber Operations, <https://strictlywriting.com/the-stages-of-cyber-operations/>, November 5, 2021
2. Cyber Operational Planning, NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES (NICCS), <https://niccs.cisa.gov/>, 2020
3. Петко Димов, Кибер информационни операции, postvai.com - Интернет списание ISSN 2535-0838, 2020
4. Оливер Фиттон, Кибер операции и серые зоны: вызовы для НАТО, Connections Q/15, No2 (2016), pp. 123-135, ISSN 1812-1098, 2016
5. Джон Хана, Кибер сигурност срещу Кибер устойчивост: по какво се различават?, <https://www.techlila.com/bg/cyber-security-vs-cyber-resilience/>, 2020
1. Silberschatz, Galvin and Gagne, Operation systems concepts, 9-th edition, 2013
2. Silberschatz, Galvin and Gagne, Important OS Papers, collection, 2015
3. Введение в Microsoft Windows Server 2019, Microsoft Press, U.S., 2019.
4. Mathers, Bill; Poggemeyer, Liza; Tobin, John, "What's new in Active Directory Federation Services for Windows Server 2016". Microsoft Docs. Windows Server, Identity and access. 2017.

14. Assessment methods and criteria:

The discipline ends with an exam.

The final grade in the discipline is formed on the basis of an exam at the end of the semester. Students have the right to be exempted from an exam based on successfully solving tasks from Control works with a score of no less than four on both controls.

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

The final grade in the course is formed on the basis of a points system and the maximum number of points that students can receive is 100. They are formed by the following activities:

- solving and timely submission of tasks for independent work - 40 points;
- active participation in practical exercises and defense of protocols - 60 points;

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-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: English