UNIVERSITY OF ECONOMICS - VARNA

FACULTY OF MANAGEMENT

DEPARTMENT OF INTERNATIONAL ECONOMIC RELATIONS

Adopted by the FC (record № 12/ 29.04.2024)
Adopted by the DC (record № 8/ 16.04.2024)

ACCEPTED BY:
Dean:
(Assoc. Prof. Dr. Dobrin Dobrev)

SYLLABUS

SUBJECT: "CYBERSECURITY AND CYBER-RESILIENCE"

DEGREE PROGRAMME: "Maritime Business and International Trade"; BACHELOR`S DEGREE

YEAR OF STUDY: 4; SEMESTER: 7

TOTAL STUDENT WORKLOAD: 240 hours; incl. curricular 60 hours

CREDITS: 8

DISTRIBUTION OF STUDENT WORKLOAD ACCORDING TO THE CURRICULUM

TYPE OF STUDY HOURS	**WORKLOAD, hours**	**TEACHING HOURS PER WEEK, hours**
CURRICULAR: incl. ● LECTURES ● SEMINARS / LAB. EXERCISES	 30 30	 2 2
EXTRACURRICULAR	180	-

Prepared by:

1. **……..**
   (Chief. Ass. Prof. Dr. M.Kamdzhalov)
2. **……**
   (Assoc. Prof. Dr. G. Marinov)

Head of department
"International Economic Relations": ……
(Prof. Dr. Vesselina Dimitrova)

I. ANNOTATION

The "Cybersecurity and Cyber Resilience" course aims to provide knowledge on contemporary threats in cyberspace and ways of protecting cyber assets. The students will be taught to evaluate cybersecurity threats using a variety of analytic techniques and methodologies. The course emphasises risk assessment, cyber vulnerability detection, cyber threat mitigation techniques implementation, and cyber resilience skills development for enterprise purposes.

Key competences developed throughout the course: digital and civic.

II. THEMATIC CONTENT

№	TITLE OF UNIT AND SUBTOPICS	NUMBER OF HOURS		
		L	S	L.E.
Theme 1. Cybersecurity fundamentals		**2**	**2**	
1.1.	Origins			
1.2.	Network security			
1.3.	Cybersecurity risks			
Theme 2. Computer security concepts		**2**	**2**	
2.1.	A Definition of Computer Security			
2.2.	The Challenges of Computer Security			
3.3.	Examples			
Theme 3. Cryptography as a cybersecurity fundamental		**2**	**2**	
3.1.	Cryptography as an Equation			
3.2.	Integrity and Hashing			
3.3	Cryptography and Nonrepudiation			
Theme 4. Cyber security and risk management		**2**	**2**	
4.1.	Threat identification			
4.2.	Steps to reduce cyber risks			
Theme 5. Cybersecurity applications		**2**	**2**	
5.1.	Username and password			
5.2.	VPNs			
5.3.	Blockchain technology			
Theme 6. Maritime cybersecurity		**2**	**2**	
6.1.	Characteristics			
6.2.	Roles, responsibilities, and tasks			
Theme 7. Port cybersecurity		**2**	**2**	
7.1.	The port authority			
7.2.	Cyber security issues for port communities			
Theme 8. Social Engineering		**2**	**2**	
8.1.	The essence			
8.2.	Social engineering and cybersecurity			
8.3.	Protection against social engineering			
Theme 9. Fundamental Concepts of Cyber Resilience		**2**	**2**	
9.1.	The need of cyber resilience			
9.2.	Resilience and Systems			
9.3.	Assessment			
Theme 10. Cyber Dependencies		**2**	**2**	

10.1.	Formal Definitions			
10.2.	Identifying Cyber Dependencies			
10.3.	Managing the Risk of Cyber Dependencies			
Theme 11. Modelling the Impact of Cyber Attacks		**2**	**2**	
11.1.	Techniques			
11.2.	Architecture and implementation			
11.3.	Case study			
Theme 12. Enhancing Cyber Resilience		**2**	**2**	
12.1.	Active Defence Techniques			
12.2.	Managing Human Factors			
12.3.	Insider Threat Mitigation			
Theme 13. Internet of Things		**2**	**2**	
13.1.	Next-Generation Cyber-Physical Systems			
13.2.	Resilience in Smart Cities Context			
Theme 14. Supply Chains		**2**	**2**	
14.1.	Overview of the Electronics Supply Chain			
14.2.	From Risk to Resilience in Global Supply Chains			
14.3.	Examples			
Theme 15. Economic Effectiveness		**2**	**2**	
15.1.	Basic Principles			
15.2.	Costs of Cyber Disruptions			
15.3.	Cyber Disruption Mitigation			
	Total:	**30**	**30**	

III. FORMS OF CONTROL:

№	TYPE AND FORM OF CONTROL	Number	extracurricular, hours
1.	**Midterm control**		
1.1.	Project	**1**	**30**
1.2.	Test	**2**	**50**
	Total midterm control:	**3**	**80**
2.	**Final term control**		

2.1.	Examination	**1**	**100**
	Total final term control:	**1**	**100**
	Total for all types of control:	**4**	**180**

IV. LITERATURE

REQUIRED (BASIC) LITERATURE:

1. Wilson, D. *Cybersecurity*. The Massachusetts Institute of Technology Press, 2021.
2. Kott, A. and Linkov, I. *Cyber Resilience of Systems and Networks*, Springer International Publishing AG, 2019. https://doi.org/10.1007/978-3-319-77492-3

RECOMMENDED (ADDITIONAL) LITERATURE:

1. Conti, M. Somani, G. and Poovendran, R. *Versatile Cybersecurity*, Springer Nature Switzerland AG, 2018. https://doi.org/10.1007/978-3-319-97643-3
2. Eric C. *Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents*, Thompson Lisle, Illinois, USA, 2018.
3. *The Cyber Resilience Index: Advancing Organizational Cyber Resilience*, World Economic Forum, 2022.
4. *The Guidelines on Cyber Security Onboard Ships*, issued by ICS, IUMI, BIMCO, OCIMF, INTERTANKO, INTERCARGO, InterManager, WSC and SYBAss