COURSE SYLLABUS

Academic year 2024 - 2025

1. Programme Information

1.1. Higher education institution	Lucian Blaga University of Sibiu
1.2. Faculty	Faculty of Science
1.3. Department	Mathematics and Informatics
1.4. Field of study	Informatics
1.5. Level of study[1]	Master
1.6. Programme of study/qualification	Cybersecurity

2. Course Information

2.1. Name of course	CyberSecurity and Cyber Warfare			Code	FSTI.MAI.CS.M.SO .2.2020.E-7.3
2.2. Course coordinator	Prof. PhD. Acu Mugur				
2.3. Seminar/laboratory coordinator	Prof. PhD. Acu Mugur				
2.4. Year of study[2]	1	2.5. Semester[3]	2	2.6. Evaluation form[4]	E
2.7. Course type[5]	R	2.8. The formative category of the course[6]			S

3. Estimated Total Time

3.1. Course Extension within the Curriculum – Number of Hours per Week				
3.1.a. Lecture	3.1.b. Seminar	3.1.c. Laboratory	3.1.d. Project	Total
2		2		**4**
3.2. Course Extension within the Curriculum – Total Number of Hours within the Curriculum				
3.2.a. Lecture	3.2.b. Seminar	3.2.c. Laboratory	3.2.d. Project	Total[7]
28		28		**56**

Time Distribution for Individual Study[8]	**Hours**
Learning by using course materials, references and personal notes	38
Additional learning by using library facilities, electronic databases and on-site information	37
Preparing seminars / laboratories, homework, portfolios and essays	28
Tutorial activities[9]	14
Exams[10]	2
3.3. Total Individual Study Hours[11] ***(NOSI$_{sem}$)***	**119**
3.4. Total Hours in the Curriculum (*NOAD$_{sem}$*)	**56**
3.5. Total Hours per Semester[12] **(*NOAD$_{sem}$* + *NOSI$_{sem}$*)**	**175**
3.6. No. of Hours / ECTS	**25**
3.7. Number of credits[13]	**7**

4. Prerequisites (if needed)

4.1. Courses that must be successfully completed first (from the curriculum)[14]	-
4.2. Competencies	-

5. Conditions (where applicable)

5.1. For course/lectures[15]	Classroom, equipped with blackboard, computer, video projector and software
5.2. For practical activities (lab/sem/pr/app) [16]	Laboratory room equipped with computers

6. Specific competencies acquired[17]

Number of credits assigned to the discipline[18]		7	Credits distribution by competencies[19]
6.1. Professional competencies	PC1	Understanding of cybersecurity concepts, including cryptography, network security, web application security, and vulnerability management	1
	PC2	Competencies in strategic planning in order to design comprehensive and sustainable security programs	1
	PC3	Understanding risk management, identifying potential threats, developing and implementing risk mitigation strategies.	1
	PC4	Competencies in incident response in order to quickly identify the source of the incident, mitigate damage, and implement corrective actions.	1
	PC5	Competencies in ethical hacking in order to identify security gaps and developing effective risk mitigation strategies.	1
26.2. Transversal competencies	TC1	Developing a positive attitude towards work and responsibility for one's own professional training.	1
	TC2	Developing the teamwork spirit.	0.5
	TC3	Ability to interpret the results obtained	0.5

7. Course objectives (resulted from developed competencies)

7.1. Main course objective	• The primary objective of cybersecurity is to protect sensitive information and data from unauthorized access, theft, or damage. This includes financial information, personal data, and other confidential information. • Cyber Warfare aims to gather intelligence on a target's infrastructure, systems, and networks to identify vulnerabilities and potential targets.
1.1. Specific course objectives	• Specific objectives: Protecting data, maintaining system integrity, ensuring system availability, mitigating risks, disruption, destruction, psychological operations

8. Content

8.1. Lectures[20]	**Teaching methods**[21]	**Hours**
Fundamentals of Cybersecurity: an overview of cybersecurity concepts, principles, and technologies, such as cryptography, network security, malware analysis, and incident response.	Lecture, use of video projector, discussions with students	2
Cyber Threats and Attacks: various types of cyber threats and attacks, including viruses, worms, Trojans, phishing, social	Lecture, use of video projector, discussions with students	2

engineering, denial-of-service (DoS) attacks, and advanced persistent threats (APTs).		
Risk Assessment and Management: different types of cyber risks, assessing their impact and likelihood, and developing risk management strategies.	Lecture, use of video projector, discussions with students	2
Cybersecurity Policies and Regulations: national and international cybersecurity policies and regulations, such as the Cybersecurity Information Sharing Act (CISA), the General Data Protection Regulation (GDPR), and the National Institute of Standards and Technology (NIST) Cybersecurity Framework.	Lecture, use of video projector, discussions with students	4
Ethical and Legal Issues in Cybersecurity: understanding the legal and ethical implications of cybersecurity, such as privacy, data protection, cybercrime, and international cyber law.	Lecture, use of video projector, discussions with students	2
Cybersecurity Operations and Management: day-to-day management and operation of cybersecurity programs, including security incident response, security operations center (SOC) management, and security governance.	Lecture, use of video projector, discussions with students	4
Cyber Intelligence and Information Sharing: collection, analysis, and dissemination of intelligence and information about cyber threats and attacks, including threat intelligence and information sharing frameworks.	Lecture, use of video projector, discussions with students	4
Cyber Warfare: understanding the various types of cyber warfare, including offensive and defensive strategies, cyber espionage, and cyber sabotage.	Lecture, use of video projector, discussions with students	4
Emerging Technologies in Cybersecurity: emerging technologies such as artificial intelligence (AI), machine learning (ML), blockchain, and quantum computing, and their impact on cybersecurity.	Lecture, use of video projector, discussions with students	2
Hands-on Experience and Capstone Projects: practical hands-on experience in implementing cybersecurity technologies, strategies, and protocols, as well as capstone projects that demonstrate mastery of cybersecurity concepts and skills.	Lecture, use of video projector, discussions with students	2
	Total lecture hours:	**28**

8.2. Practical activities (8.2.a. Seminar[22]/ 8.2.b. Laboratory[23]/ 8.2.c. Project[24])	**Teaching methods**	**Hours**
Conduct vulnerability assessments identifying weaknesses in a system's security and testing its resilience to cyber-attacks.	Use of video projector, discussions with students	2
Penetration testing: simulating an attack on your own systems to identify vulnerabilities and weaknesses in your security protocols.	Use of video projector, discussions with students	2
Threat modeling: identifying potential threats and vulnerabilities in a system. Analyzing the security of a website or application and identifying potential attack vectors.	Use of video projector, discussions with students	2
Red teaming: simulating a cyber attack on your own organization to assess your preparedness and response capabilities.	Use of video projector, discussions with students	4
Incident response: the process of responding to a cyber-attack or security incident.	Use of video projector, discussions with students	2
Incident response planning: procedures for identifying and containing the attack, as well as strategies for mitigating the damage and restoring normal operations.	Use of video projector, discussions with students	4
Types of cyber-attacks: different types of cyber-attacks and how they work is essential to effective cybersecurity.	Use of video projector, discussions with students	4
Secure communication: how encryption and decryption work and how they can be used to protect sensitive data.	Use of video projector, discussions with students	4

Cyber warfare: understand the potential risks and threats involved in this type of warfare.	Use of video projector, discussions with students	4
Total seminar/laboratory hours:		28

9. Bibliography

9.1. Recommended Bibliography	1. Understanding Cyber-Warfare, Christopher White and Brian Mazanec, 2023
9.2. Additional Bibliography	2. Cyber War versus Cyber Realities: Cyber Conflict in the International System, Brandon Valeriano, Ryan C. Maness, Oxford University Press Colecția OUP USA, 2015

10. Conjunction of the discipline's content with the expectations of the epistemic community, professional associations and significant employers of the specific study program[25]

It is done through regular contacts with the representatives of the companies. Cybersecurity and Cyber Warfare is an actual topic and is of great interest in existing software companies on the local, national and global market.

11. Evaluation

Activity Type	11.1 Evaluation Criteria	11.2 Evaluation Methods		11.3 Percentage in the Final Grade	Obs.[26]
11.4a Exam / Colloquy	• Theoretical and practical knowledge acquired (quantity, correctness, accuracy)	Tests during the semester[27]:	%	50% (minimum 5)	CEF
		Homework:	%		
		Other activities[28]:	%		
		Final evaluation:	50%		
11.4b Seminar	• Frequency/relevance of participation or responses	Evidence of participation, portfolio of papers (reports, scientific summaries)		5% (minimum 5)	nCPE
11.4c Laboratory	• Knowledge of the equipment, how to use specific tools; evaluation of tools, processing and interpretation of results	• Written questionnaire • Oral response • Laboratory notebook, experimental works, reports, etc. • Practical demonstration		5% (minimum 5)	nCPE
11.4d Project	• The quality of the project, the correctness of the project documentation, the appropriate justification of the chosen solutions	• Self-evaluation, project presentation • Critical evaluation of a project		40% (minimum 5)	nCPE
11.5 Minimum performance standard[29] To pass the exam, the candidate must have a basic knowledge of the cyber warfare and knows how to identify possible threats					

The Course Syllabus will encompass components adapted to persons with special educational needs (SEN – people with disabilities and people with high potential), depending on their type and degree, at the level of all curricular elements (skills, objectives, contents, teaching methods, alternative assessment), in order to ensure fair opportunities in the academic training of all students, paying close attention to individual learning needs.

Filling Date: |_0_|_5_| / |_0_|_9_| / |_2_|_0_|_2_|_4_|

Department Acceptance Date: |_0_|_6_| / |_0_|_9_| / |_2_|_0_|_2_|_4_|

	Academic Rank, Title, First Name, Last Name	**Signature**
Course Teacher	Prof. PhD. Acu Mugur	
Study Program Coordinator	Lecturer PhD. Daniel Hunyadi	
Department Head	Professor PhD. Mugur Acu	

[1] *Bachelor / Master*

[2] *1-4 for bachelor, 1-2 for master*

[3] *1-8 for bachelor, 1-3 for master*

[4] *Exam, colloquium or VP A/R - from the curriculum*

[5] *Course type: R = Compulsory course; E = Elective course; O = Optional course*

[6] *Formative category: S = Specialty; F = Fundamental; C = Complementary; I = Fully assisted; P = Partially assisted; N = Unassisted*

[7] *Equal to 14 weeks x number of hours from point 3.1 (similar to 3.2.a.b.c.)*

[8] *The following lines refer to individual study; the total is completed at point 3.37.*

[9] *Between 7 and 14 hours*

[10] *Between 2 and 6 hours*

[11] *The sum of the values from the previous lines, which refer to individual study.*

[12] *The sum (3.5.) between the number of hours of direct teaching activity (NOAD) and the number of hours of individual study (NOSI) must be equal to the number of credits assigned to the discipline (point 3.7) x no. hours per credit (3.6.)*

[13] *The credit number is computed according to the following formula, being rounded to whole neighbouring values (either by subtraction or addition*

$$No.credits = \frac{NOCpSpD \times C_C + NOApSpD \times C_A}{TOCpSdP \times C_C + TOApSdP \times C_A} \times 30\ credits$$

Where:

- NOCpSpD = Number of lecture hours / week / discipline for which the credits are calculated
- NOApSpD = Number of application hours (sem./lab./pro.) / week / discipline for which the credits are calculated
- TOCpSdP = Total number of course hours / week in the Curriculum
- TOApSdP = Total number of application hours (sem./lab./pro.) / week in the Curriculum
- C_C/C_A = Course coefficients / applications calculated according to the table

Coefficients	**Course**	**Applications (S/L/P)**
Bachelor	2	1
Master	2,5	1,5
Bachelor - foreign language	2,5	1,25

[14] *The courses that should have been previously completed or equivalent will be mentioned*

[15] *Board, video projector, flipchart, specific teaching materials, online platforms, etc.*

[16] *Computing technology, software packages, experimental stands, online platforms, etc.*

[17] *Competences from the Grids related to the description of the study program, adapted to the specifics of the discipline*

[18] *From the curriculum*

[19] *The credits allocated to the course are distributed across professional and transversal competences according to the specifics of the discipline*

[20] *Chapter and paragraph titles*

[21] *Exposition, lecture, board presentation of the studied topic, use of video projector, discussions with students (for each chapter, if applicable)*

[22] *Discussions, debates, presentations and/or analyses of papers, solving exercises and problems*

[23] *Practical demonstration, exercise, experiment*

[24] *Case study, demonstration, exercise, error analysis, etc.*

[25] *The relationship with other disciplines, the usefulness of the discipline on the labour market*

[26] *CPE – Conditions Exam Participation; nCPE – Does Not Condition Exam Participation; CEF - Conditions Final Evaluation; N/A – not applicable*

[27] *The number of tests and the weeks in which they will be taken will be specified*

[28] *Scientific circles, professional competitions, etc.*

[29] *The minimum performance standard in the competence grid of the study program is customized to the specifics of the discipline, if applicable*