COURSE SYLLABUS

Academic year 2025 - 2026

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	Computer Network Defence			Code	FSTI.MAI.CS.M.SO.3.2020.E-7.3
2.2. Course coordinator	Professor PhD. Remus Brad				
2.3. Seminar/laboratory coordinator	Professor PhD. Remus Brad				
2.4. Year of study[2]	2	2.5. Semester[3]	1	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	36
Additional learning by using library facilities, electronic databases and on-site information	33
Preparing seminars / laboratories, homework, portfolios, and essays	33
Tutorial activities[9]	12
Exams[10]	5

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. Learning Outcomes [17]

Number of credits assigned to the discipline: 7				
Learning outcomes				Credit distribution by learning outcomes
Nr. crt.	Knowledge	Skills	Responsibility and autonomy	
LO 1	The student explains the fundamentals of CND, including cybersecurity principles, the anatomy of cyber attacks, and the cyber kill chain model.	The student applies analytical methods to identify the stages of a cyber attack.	The student demonstrates responsibility in evaluating attack scenarios and adopts a preventive approach.	1.5
LO 2	The student describes network security concepts and the components of a secure architecture.	The student designs and implements secure network architectures, including firewalls, IDS/IPS, and VPNs.	The student assumes responsibility for selecting solutions and proposes improvement measures.	1.5
LO 3	The student understands endpoint security principles.	The student configures and uses protection tools (antivirus, HIDS/HIPS, whitelisting).	The student shows autonomy in managing the security of workstations and mobile devices.	1
LO 4	The student explains incident response procedures and the basics of digital forensics.	The student applies response protocols and collects digital evidence.	The student shows responsibility in documenting incidents and complies with legal and ethical standards.	1
LO 5	The student describes threat intelligence and analysis processes.	The student conducts intelligence analyses to identify and mitigate threats.	The student demonstrates autonomy in using sources and provides informed recommendations	0.5
LO 6	The student understands the role and operation of a SOC.	The student models SOC operations and uses SIEM tools.	The student assumes responsibility for correct interpretation of alerts and adopts professional conduct.	1
LO 7	The student describes CND best practices (secure coding, vulnerability	The student applies these best practices in practical scenarios.	The student shows responsibility in consistently applying professional standards.	0.5

	management, risk assessment).			

7. Course objectives (resulted from developed competencies)

7.1. Main course objective	Acquiring and understanding the necessary notions to analyse the degree of risk of a network system, from the point of view of its degree of vulnerability and methods of ameliorating the risks.
7.2 Specific course objectives	Accumulating knowledge related to the basic rules for securing hardware and software a network, detecting mistakes in the design of information security architectures.

8. Content

8.1. Lectures[18]	**Teaching methods**[19]	**Hours**
Introduction to Computer Network Defence - CND. Fundamentals of CND, including the principles of cyber security, the anatomy of cyber attacks, and the cyber kill chain model	Lecture, use of video projector, discussions with students	4
Network security. Design and implementation of secure network architectures, including firewalls, intrusion detection and prevention systems, and virtual private networks (VPNs)	Lecture, use of video projector, discussions with students	4
Endpoint security. Protection of endpoints (computers, mobile devices) from cyber attacks, including the use of antivirus software, host-based intrusion detection and prevention systems, and application whitelisting	Lecture, use of video projector, discussions with students	4
Incident response and forensics. Procedures and protocols for responding to security incidents, including incident reporting, incident response planning, and digital forensics	Lecture, use of video projector, discussions with students	4
Threat intelligence and analysis. Gathering and analysis of threat intelligence to identify and mitigate cyber threats	Lecture, use of video projector, discussions with students	4
Security operations center (SOC) operations. Design and operation of a SOC, including the use of security information and event management (SIEM) systems	Lecture, use of video projector, discussions with students	4
CND best practices. Best practices for CND, including secure coding practices, vulnerability management, and risk assessment	Lecture, use of video projector, discussions with students	4
	Total lecture hours:	**28**

8.2. Practical activities (8.2.a. Seminar[20]/ 8.2.b. Laboratory[21]/ 8.2.c. Project[22])	**Teaching methods**	**Hours**
Design and implement secure network architectures using tools like firewalls, intrusion detection and prevention systems (IDS/IPS), and virtual private networks (VPNs). Optimal configuration of these tools to protect the network from cyber attacks	Use of video projector, discussions with students	4
Network scanning and mapping tools to identify vulnerabilities in the network	Use of video projector, discussions with students	4
How to protect endpoints (computers, mobile devices) from cyber attacks, antivirus software configurations, host-based intrusion detection	Use of video projector, discussions with students	4

and prevention systems, and how to create application whitelisting. Tools for cyber attack detection		
Incident response tools, such as SIEM and log analysis tools	Use of video projector, discussions with students	4
Threat intelligence platforms, such as Threat Connect and Recorded Future	Use of video projector, discussions with students	4
Incident management systems, and security orchestration and automation response (SOAR) tools	Use of video projector, discussions with students	4
Use of security frameworks, such as the NIST Cybersecurity Framework and the CIS Controls	Use of video projector, discussions with students	4
	Total seminar/laboratory hours:	28

9. Bibliography

9.1. Recommended Bibliography	1. J. M. Kizza, Computer Network Security and Cyber Ethics, McFarland 2019 2. R. M. Clark, S. Hakim, Cyber-Physical Security - Protecting critical infrastructure at the State and Local Level, Springer 2019 3. S. Guo, D. Zeng, Cyber-Physical Systems - Architecture, Security and Application, Springer 2019 4. S. Parkinson, A. Crampton, R. Hill, Guide to Vulnerability Analysis for Computer Networks and Systems, Springer 2021
a. Additional Bibliography	1. J. Grand, R. Russel, Hardware Hacking, Syngress 2004 2. An Introduction to Computer Security, NIST 2017 3. L. Ayala, Cybersecurity Lexicon, Apress 2016 4. The Complete Internet Security Manual, BDiTS 2019 5. K. Mitnick, The art of invisibility, IKP 2017 6. C. Hadnagy, Social Engineering: The Science of Human Hacking, Wiley 2018

4. Conjunction of the discipline's content with the expectations of the epistemic community, professional associations and significant employers of the specific study program[23]

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

5. Evaluation

Activity Type	11.1 Evaluation Criteria	11.2 Evaluation Methods		11.3 Percentage in the Final Grade	Obs.[24]
11.4a Exam / Colloquy	• Theoretical and practical knowledge acquired (quantity, correctness, accuracy)	Tests during the semester[25]:	%	50% (minimum 5)	CEF
		Homework:	%		
		Other activities[26]:	%		
		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	• Self-evaluation, project presentation • Critical evaluation of a project		40% (minimum 5)	nCPE

	justification of the chosen solutions			
11.5 Minimum performance standard[27] To pass the exam, the candidate must have a basic knowledge about computer network defence				

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: |_1_|_5_| / |_0_|_9_| / |_2_|_0_|_2_|_5_|

Department Acceptance Date: |_3_|_0_| / |_0_|_9_| / |_2_|_0_|_2_|_5_|

	Academic Rank, Title, First Name, Last Name	**Signature**
Course Teacher	Professor PhD. Remus Brad	
Study Program Coordinator	Associated Professor PhD. Nicolae Constantinescu	
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] *Chapter and paragraph titles*
[19] *Exposition, lecture, board presentation of the studied topic, use of video projector, discussions with students (for each chapter, if applicable)*
[20] *Discussions, debates, presentations and/or analyses of papers, solving exercises and problems*
[21] *Practical demonstration, exercise, experiment*
[22] *Case study, demonstration, exercise, error analysis, etc.*
[23] *The relationship with other disciplines, the usefulness of the discipline on the labour market*
[24] *CPE – Conditions Exam Participation; nCPE – Does Not Condition Exam Participation; CEF - Conditions Final Evaluation; N/A – not applicable*
[25] *The number of tests and the weeks in which they will be taken will be specified*
[26] *Scientific circles, professional competitions, etc.*
[27] *The minimum performance standard in the competence grid of the study program is customized to the specifics of the discipline, if applicable*