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	Prevention in cybersecurity models			Code	FSTI.MAI.CS.M.SO .3.1010.E-6.5
2.2. Course coordinator	Professor PhD. Acu Mugur				
2.3. Seminar/laboratory coordinator	Professor PhD. Acu Mugur				
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
1		1		**2**
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]
14		14		**28**

Time Distribution for Individual Study[8]	**Hours**
Learning by using course materials, references and personal notes	39
Additional learning by using library facilities, electronic databases and on-site information	33
Preparing seminars / laboratories, homework, portfolios, and essays	33
Tutorial activities[9]	6
Exams[10]	5
3.3. Total Individual Study Hours[11] $(NOSI_{sem})$	**122**
3.4. Total Hours in the Curriculum $(NOAD_{sem})$	**28**
3.5. Total Hours per Semester[12] $(NOAD_{sem} + NOSI_{sem})$	**150**
3.6. No. of Hours / ECTS	**25**
3.7. Number of credits[13]	**6**

4. Prerequisites (if needed)

4.1. Courses that must be successfully completed first (from the curriculum)[14]	Security of Information Systems
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: 6				
Learning outcomes				Credit distribution by learning outcomes
Nr. crt.	Knowledge	Skills	Responsibility and autonomy	
LO 1	The student explains the fundamental concepts of threat modeling and risk assessment.	The student applies methods to identify threats and evaluate risks for information systems.	The student demonstrates responsibility in documenting results and adopts a critical approach in interpreting risks.	1.5
LO 2	The student describes access control mechanisms and the principles of encryption.	The student implements access control policies and applies data encryption techniques.	The student shows autonomy in selecting and using mechanisms and complies with legal and ethical standards.	1.5
LO 3	The student understands the principles of network and application security.	The student configures and uses security measures for networks and applications (firewalls, IDS, authentication, input validation).	The student shows responsibility in protecting resources and adopts professional best practices.	1.5
LO 4	The student explains the role of security policies, procedures, and incident response.	The student develops security policies and applies incident response procedures.	The student assumes responsibility for the accuracy of interventions and proposes preventive measures.	1.5

7. Course objectives (resulted from developed competencies)

7.1. Main course objective	Acquiring and understanding the necessary notions to project and analyse a system and give the necessary information to prevent penetrations, 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 systems to be resistant to cyber attacks, detecting mistakes in the design of information security architectures.

8. Content

8.1. Lectures[18]	Teaching methods[19]	Hours

Threat modeling: The process of identifying potential threats and vulnerabilities in a system, and assessing their likelihood and potential impact.	Lecture, use of video projector, discussions with students	2
Risk assessment: The process of identifying, analyzing, and evaluating potential risks to a system, and determining the likelihood and potential impact of each risk.	Lecture, use of video projector, discussions with students	2
Access controls: The mechanisms used to restrict access to sensitive data or systems, and to enforce security policies.	Lecture, use of video projector, discussions with students	2
Encryption: The process of encoding data in a way that only authorized users can access it, even if it is intercepted by unauthorized parties.	Lecture, use of video projector, discussions with students	2
Network security: The measures used to secure networks, including firewalls, intrusion detection systems, and other security devices.Application security: The measures used to secure applications, including authentication, authorization, and input validation.	Lecture, use of video projector, discussions with students	2
Security policies and procedures: The guidelines and protocols that organizations use to enforce security policies and procedures, and to respond to security incidents.	Lecture, use of video projector, discussions with students	2
Incident response: The process of detecting, analyzing, and responding to security incidents, including the steps needed to mitigate the impact of an incident and prevent it from happening again.	Lecture, use of video projector, discussions with students	2
	Total lecture hours:	**14**

8.2. Practical activities (8.2.a. Seminar[20]/ 8.2.b. Laboratory[21]/ 8.2.c. Project[22])	**Teaching methods**	**Hours**
Threat modeling exercise: Identify potential threats and vulnerabilities in a system, and assess their likelihood and potential impact. Develop a plan to mitigate each threat and present threat that are found.	Use of video projector, discussions with students	2
Access control implementation: Set up access controls for a system or application, using tools such as role-based access control (RBAC) and access control lists (ACLs).Test the access controls to ensure that they are working correctly.	Use of video projector, discussions with students	2
Encryption implementation: How to encrypt data using tools such as GPG or OpenSSL. Apply encryption to a sample data set and test the decryption process to ensure that it is working correctly.	Use of video projector, discussions with students	2
Network security implementation: Set up a network security system, using tools such as firewalls, intrusion detection systems	Use of video projector, discussions with students	2

(IDS), and virtual private networks (VPN). Test the system to ensure that it is effective at detecting and preventing attacks.		
Application security implementation: Application to implement security features such as authentication, authorization, and input validation. Test the application to ensure that it is secure against common attacks such as cross-site scripting (XSS) and SQL injection.	Use of video projector, discussions with students	2
Incident response simulation: Simulate a security incident and work through the steps needed to respond to it. This may include identifying the source of the attack, mitigating its impact, and developing a plan to prevent similar attacks from happening in the future.	Use of video projector, discussions with students	4
	Total seminar/laboratory hours:	14

9. Bibliography

9.1. Recommended Bibliography	1. G. Weidman, Penetration Testing, Starch Press 2014 2. N. Adams, N. Heard, Data Analysis for Network Cyber Security, Imperial College Press, 2019 3. R. M. Clark, S. Hakim, Cyber-Physical Security - Protecting critical infrastructure at the State and Local Level, Springer 2019 4. S. Guo, D. Zeng, Cyber-Physical Systems - Architecture, Security and Application, Springer 2019 5. 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

10. 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.

11. 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	• Written questionnaire • Oral response • Laboratory notebook, experimental works, reports, etc.		5% (minimum 5)	nCPE

	of tools, processing and interpretation of results	• Practical demonstration		
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[27] To pass the exam, the candidate must have a basic knowledge of the cybersecurity models.				

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. Mugur Acu	
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*