SYLLABUS

1. Data about the program of study

1.1 Institution	The Technical University of Cluj-Napoca
1.2 Faculty	Faculty of Automation and Computer Science
1.3 Department	Computer Science
1.4 Field of study	Computer Science and Information Technology
1.5 Cycle of study	Master
1.6 Program of study / Qualification	Cybersecurity Engineering / Master
1.7 Form of education	Full time

2. Data about the subject

2.1 Subject name	*Research Activity 1*			Subject code		**5.00**
2.2 Course responsible / lecturer	N/A					
2.3 Teachers in charge of seminars / Laboratory / project	Assoc.prof.dr.eng. Adrian COLEŞA - adrian.colesa@cs.utcluj.ro					
2.4 Year of study	I	2.5 Semester	1	2.6 Type of assessment (E - exam, C - colloquium, V – verification)		V
2.7 Subject category	Formative category: DA – advanced, DS – speciality, DC – complementary					DS
	Optionality: DI – imposed, DO – optional (alternative), DF – optional (free choice)					DI

3. Estimated total time

3.1 Number of hours per week	14	of which:	Course	0	Seminars	0	Laboratory	0	Project	14
3.2 Number of hours per semester	196	of which:	Course	0	Seminars	0	Laboratory	0	Project	196
3.3 Individual study:										
(a) Manual, lecture material and notes, bibliography										0
(b) Supplementary study in the library, online and in the field										25
(c) Preparation for seminars/laboratory works, homework, reports, portfolios, essays										0
(d) Tutoring										0
(e) Exams and tests										4
(f) Other activities:										0

3.4 Total hours of individual study (suma (3.3(a)…3.3(f)))	29
3.5 Total hours per semester (3.2+3.4)	225
3.6 Number of credit points	9

4. Pre-requisites (where appropriate)

4.1 Curriculum	N/A
4.2 Competence	N/A

5. Requirements (where appropriate)

5.1. For the course	N/A
5.2. For the applications	Hardware and software specific to dissertation theme

6. Specific competence

6.1 Professional competences	perform ICT security testing perform data analysis identify ICT security risks perform risk analysis ensure information privacy monitor developments in field of expertise keep up with the latest information systems solutions execute ICT audits
6.2 Cross competences	develop an analytical approach taking a proactive approach developing strategies to solve problems being open minded

7. Expected Learning Outcomes

Knowledge	ICT security standards security engineering cyber security cyber attack counter-measures information confidentiality information security strategy computer forensics ethical hacking principles risk management assessment of risks and threats attack vectors security threats ICT infrastructure ICT performance analysis methods
Skills	analyse ICT systems define technical requirements identify ICT security risks and weaknesses perform ICT security testing perform risk analysis collect cyber defence data perform scientific research report test findings and give live presentations solve ICT system problems address problems critically assess ICT knowledge execute ICT audits implement ICT security policies interpret technical texts
Responsibilities and autonomy	develop an analytical approach take a proactive approach develop strategies to solve problems be open-minded

8. Discipline objective (as results from the *key competences gained*)

8.1 General objective	Gain the ability and skills to do research, design, development, and assessment work in the cybersecurity field.
8.2 Specific objectives	1. Ability to identify cybersecurity weaknesses / vulnerabilities in a software application, computing system, communication protocol etc. 2. Ability to describe the cybersecurity requirements aimed to solve identified

	cybersecurity vulnerabilities.
	3. Capability to derive a strategy to research identified cybersecurity vulnerabilities and establish a plan to fix them.
	4. Know the state-of-the-art regarding the investigated application or computing system.

9. Contents

9.1 Lectures	Hours	Teaching methods	Notes
N/A	N/A	N/A	N/A

Bibliography

N/A

9.2 Applications - Seminars/Laboratory/Project	Hours	Teaching methods	Notes
Establish dissertation (research) theme and specifications	14	Cooperation between dissertation supervisor and student	
Establish main research direction and basic working plan			
Read papers to find out the state-of-the-art regarding research theme			
Write a document to list and describe important found references			
Write a technical report describing state-of-the art and identified open problems of interest			

Bibliography

Established by each supervisor for students she/he coordinates, specific to chosen dissertation themes.

9. Bridging course contents with the expectations of the representatives of the community, professional associations and employers in the field

It is performed by periodic talks with important cybersecurity industry representatives.

10. Evaluation

Activity type	Assessment criteria	Assessment methods	Weight in the final grade
Project	Based on the contents and relevance of the written technical report	Oral presentations *(continuous assessment)* Technical report's quality *(summative assessment)*	60% 40%

Minimum standard of performance

Establish dissertation subject, identify and cover basic papers describing state-of-the-art, write a minimum 5 page technical report.

Date of filling in 01.09.2025	Responsible	Title First name Last name	Signature
	Applications	Assoc.prof.dr.eng. Adrian COLEȘA	

Date of approval in the department 17.09.2025	Head of department, Prof.dr.eng. Rodica Potolea
Date of approval in the Faculty Council 19.09.2025	Dean, Prof.dr.eng. Vlad Mureşan

4/4