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		*Professional internship / Designing practice*		Subject code		**17.00**
2.2 Course responsible / lecturer		N/A				
2.3 Teachers in charge of seminars / Laboratory / project		N/A				
2.4 Year of study	II	2.5 Semester	2	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										25
(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)))	54
3.5 Total hours per semester (3.2+3.4)	250
3.6 Number of credit points	10

4. Pre-requisites (where appropriate)

4.1 Curriculum	Research Activity 1, 2 and 3
4.2 Competence	Competences of subjects mentioned at 4.1

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
	coordinate engineering teams

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
	coordinate engineering teams

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. Obtain at least a solution functional in real-life scenarios.
	2. Have detailed knowledge about the field of dissertation theme and, in that context, be able to identify and explain the advantages and limitations of the obtained solution.
	3. Identify possible future improvements of obtained solution and research directions in the field of dissertation theme.
	4. Disseminate obtained results (e.g. publish a paper).

9. Contents

9.1 Lectures	Hours	Teaching methods	Notes
N/A			

Bibliography
N/A

9.2 Applications - Seminars/Laboratory/Project	Hours	Teaching methods	Notes
Implement and assess improvements of the initial prototype.			
Integrate all obtain components in a final solution (app).			
Write the technical description of obtained solution and system (app).	14	Cooperation between dissertation supervisor and student	
Write a user manual for obtained solution (application).			
Write a technical report describing research activity performed and obtained results.			
Write a scientific paper and submit it to a conference or journal in the cybersecurity field.			

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
Implement and validate at least one solution (and its improvements) to the identified problem, write technical and user manuals for the implemented solution, write a minimum 5 page technical report.

Date of filling in 01.09.2025	Responsible	Title First name Last name	Signature
	Applications	Dissertation thesis coordinator	

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