SYLLABUS

1. Data about the program of study

1.1	Institution	Technical University of Cluj-Napoca
1.2	Faculty	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 of Science
1.6	Program of study / Qualification	Cybersecurity Engineering / Master
1.7	Form of education	Full time
1.8	Subject code	5.

2. Data about the subject

2.1	Subject name			***Research Activity 1***		
2.2	Course responsible/lecturer			N/A		
2.3	Teachers in charge of applications			Conf. dr. ing. Adrian COLEȘA - 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	3.2 Course	0	3.3 Seminar	0	3.3 Laboratory	0	3.3 Project	14
3.4 Total hours in the curriculum	196	of which	3.5 Course	0	3.6 Seminar	0	3.6 Laboratory	0	3.6 Project	196

3.7 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

3.8 Total hours of individual study (sum (3.7(a)...3.7(f)))	29
3.9 Total hours per semester (3.4+3.8)	225
3.10 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 competences

Professional competences	**C1. Identify and understand the security issues specific to the different contexts of computing system usage. Appropriately apply the basic elements of security management and methods of evaluation and management of information security risks.** • **C1.1.** Knowledge of advanced theoretical and practical terminology, concepts, and principles specific to cybersecurity field. Knowledge of concepts about cybersecurity risk evaluation, and management. • **C1.2.** Understanding cybersecurity risks specific to new situations and their relationship with previously experienced situations and risks. Be able to predict possible threat scenarios when using cybersecurity solutions in new fields or situations. • **C4.3.** Capability to develop complex secure software, complying with recommended good practices of built-in security and secure coding. Capability to develop software tools used for cybersecurity pentesting and assessment. • **C4.4.** Capability to assess complex software projects and identify their cybersecurity vulnerabilities and flaws, regarding their design, implementation, or testing, and propose improved development methods from the cybersecurity perspective. **C5. Develop rigorous and efficient security solutions to complex real-life problems and situations. Be able to use security mathematical tools and models, engineering approaches and technologies specific and appropriate for the information and computing system security field.** • **C5.1.** Knowledge of complex relationship between cybersecurity and real-life aspects. Knowledge of mathematical theory some cybersecurity mechanisms and solutions are based on. • **C5.2.** Be able to analyze and understand new complex real-life scenarios from the cybersecurity perspective. Be able to identify needed cybersecurity solutions and derive new ones for new particular cases. • **C5.3.** Capability to apply mathematical and computer engineering theoretical models to analyze, assess and address real-life cybersecurity and privacy issues and challenges. • **C5.4.** Capability to identify and assess limitations of existing cybersecurity solutions and tools used in real-life situations, their residual cybersecurity risks, and their criticality. Capability to identify and research new cybersecurity fields and methods that could be used to reduce the limitations of existing cybersecurity solutions. • **C5.5.** Capability to run research activities and projects aimed to derive applicable cybersecurity solutions, implement their hardware and/or software prototype.
Cross competences	**CT1.** Understand the economical, ethical, legal, and social aspects of the own business context and environment, such that to be able to correctly identify the challenges and to schedule the appropriate activities and decisions to deal with those challenges. Be able to evaluate the social, ethical, and legal impact of your own business decisions

7. Discipline objectives (as results from the *key competences gained*)

7.1	General objective	Gain the ability and skills to do research, design, development, and assessment work in the cybersecurity field.
7.2	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.

8. Contents

8.1. Lecture (syllabus)	Number of hours	Teaching methods	Notes
N/A	N/A	N/A	N/A

Bibliography N/A			
8.2. Seminar / Laboratory / Project	Number of 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 presentation Technical report's quality	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		**Title Surname Name**	**Signature**
	Teachers in charge of application	Conf. dr. ing. Adrian COLEȘA	

Date of approval in the Computer Science Department 20.02.2024	Head of department Prof.dr.ing. Rodica Potolea
Date of approval in the faculty of Automation and Computer Science 22.02.2024	Dean Prof.dr.ing. Mihaela Dinsoreanu