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	2.

2. Data about the subject

2.1 Subject name			***Information Security***		
2.2 Course responsible/lecturer			Lect. Dr. eng. Marius Joldoş – Marius.Joldos@cs.utcluj.ro		
2.3 Teachers in charge of seminars/ laboratory/ project			Lect. Dr. eng. Marius Joldoș – Marius.Joldos@cs.utcluj.ro		
2.4 Year of study	I	2.5 Semester	1	2.6 Type of assessment (E - exam, C - colloquium, V - verification)	E
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	3	of which:	Course	2	Seminars	1	Laboratory	0	Project	0
3.2 Number of hours per semester	42	of which:	Course	28	Seminars	14	Laboratory	0	Project	0
3.3 Individual study:										
(a) Manual, lecture material and notes, bibliography										50
(b) Supplementary study in the library, online and in the field										20
(c) Preparation for seminars/laboratory works, homework, reports, portfolios, essays										11
(d) Tutoring										0
(e) Exams and tests										2
(f) Other activities:										0

3.4 Total hours of individual study (suma (3.3(a)…3.3(f)))	83
3.5 Total hours per semester (3.2+3.4)	125
3.6 Number of credit points	5

4. Pre-requisites (where appropriate)

4.1	Curriculum	N/A
4.2	Competence	Operating systems architecture, computer architecture, basic computer networks knowledge

5. Requirements (where appropriate)

5.1	For the course	blackboard, beamer, computers
5.2	For the applications	blackboard, beamer, computers

6. Specific competence

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. • **C1.3.** Capability to identify and model new types of cybersecurity risks affecting end users, computing systems, and software applications, and identify and evaluate possible solutions against such risks. • **C1.4.** Capability to identify and assess the limitations of existing cybersecurity solutions and their security risks, relative to well-known classifications. • **C1.5.** Capability to develop new theoretical models and methods to analyze and assess the cybersecurity properties and effectiveness of existing solutions. **C4. Design and develop highly secure software, security solutions and tools.** • **C4.2**. Be able to identify new situations and scenarios when it is needed to develop a new cybersecurity solution or use an existing one. Be able to analyze proposed cybersecurity solutions and compare them with existing ones. • **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. • **C4.5.** Capability to develop software modules and tools that could provide a high degree of cybersecurity. Capability to propose new methods to assess the cybersecurity of computing systems and devices and ways to improve it. **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. • **C5.4.** 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.
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 objective (as results from the *key competences gained*)

7.1	General objective	Acquiring a global, comprehensive view on the many areas and aspects which are part or are directly connected with computer systems, networks, and information security. Understanding the applicability of notions and information security specific elements to the real world (and, particularly to software and computer systems) and acquiring an ability to observe, analyze and evaluate the connections of information security with the real world.
7.2	Specific objectives	1. Familiarization with information security specific terminology and correct use of that terminology. 2. Understanding the various aspects and ways that connect cybercrime and information security to day-to-day activities.

		3. Acquiring an ability to analyze an information system from the point of view of information security (for example, a critical viewpoint). 4. Acquiring an overall view and the ability to connect the various engineering areas, various software project types, the field, and the elements specific to information security and the applicable standards and procedures. 5. Familiarization with the 8 fundamental domains (as stated in CISSP) of information security.

8. Contents

8.1 Lectures	Hours	Teaching methods	Notes
Cybersecurity Governance (I)	2	Blackboard illustrations and explanations, beamer presentations, discussions, short challenges	Uses a video-projector
Cybersecurity Governance (II)	2		
Risk management (I)	2		
Risk management (II)	2		
Compliance	2		
Frameworks	2		
System architectures	2		
Security architectures	2		
Site and Facility Security	2		
Identity and Access Management	2		
Security Operations (I)	2		
Security Operations (II)	2		
Software Development Security (I)	2		
Software Development Security (II)	2		
Bibliography 1. CISSP Exam Guide – Maymi, F. and Harris, S. – McGraw-Hill, 2022, 9th edition 2. Computer and Information Security Handbook – Vacca, J. – Morgan Kaufmann, 2017, 3nd edition 3. Geekonomics. The Real Cost of Insecure Software – Rice, D. – Addison-Wesley, 2008 4. Various articles and technical reports from the specialists of the field – in electronic format.			
8.2 Applications – Seminars/Laboratory/Project	Hours	Teaching methods	Notes
Economic and social impact of cybercrime	2	Tutoring, discussions, case studies	
Social engineering and Trust	2		
Analysis of recent technical reports and articles (1)	2		
Analysis of recent technical reports and articles (2)	2		
Analysis of recent technical reports and articles (3)	2		
Analysis of recent technical reports and articles (4)	2		
Analysis of recent technical reports and articles (5)	2		
Bibliography 1. Moodle course Web Site available at https://moodle.cs.utcluj.ro/			

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

The fundaments of this course rely on the CISSP® (Certified Information Systems Security Professional), one of the most important certifications in information security, internationally appreciated and recognized (https://www.isc2.org/cissp/default.aspx).
There are periodical discussions with the representatives of significant employers, especially the ones that develop projects in information security.
The materials supporting the lectures and the seminars are found on https://moodle.cs.utcluj.ro/

10. Evaluation

Activity type	Assessment criteria	Assessment methods	Weight in the final grade
Course	Ability to solve domain-specific problems. Activity, interaction during the lectures	Written exam, including online quiz tests (e.g. on Moodle platform) and presentation(s) of	80%

		different subjects / paper in the course's field during semester time. In exceptional cases, which imposes remote classes, the exam could be given online remotely, using Moodle and Teams platforms.	
Seminar	Ability to solve domain-specific problems. Activity, interaction during the lectures	Presentation of a research result and/or presentation of a solution similar to the one discussed at the seminar. In exceptional cases, which imposes remote classes, the exam could be given online remotely, using Moodle and Teams platforms.	20%

Minimum standard of performance

Attending **minimum 50%** of lecture classes, to be allowed to take the final examination. Attending **all lab classes** (one lab could be recovered during the semester, and one more during re-examination sessions).
Evaluation grade ≥ 5 (out of 10).
Demonstration of understanding of the concepts and notions of information security, and their correct use and application. The ability to critically analyze of a case study and the ability to define and explain the specific terms used.

Date of filling in:	**Holders**	**Title Firstname LASTNAME**	**Signature**
	Course	Lect.dr.eng. Marius Joldos	
	Applications	Lect.dr.eng. Marius Joldos	

Date of approval in the department **20.02.2024**	Head of department Prof.dr.ing. Rodica Potolea
Date of approval in the Faculty Council **22.02.2024**	Dean Prof.dr.ing. Mihaela Dinsoreanu