COURSE SYLLABUS

Academic year 2024 - 2025

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	Intelligent Systems in Risk Analysis			Code	FSTI.MAI.CS.M.SO .2.1020.E-6.2
2.2. Course coordinator	Professor PhD. Acu Ana Maria				
2.3. Seminar/laboratory coordinator	Professor PhD. Acu Ana Maria				
2.4. Year of study[2]	1	2.5. Semester[3]	2	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		2		**3**

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		28		**42**

Time Distribution for Individual Study[8]	**Hours**
Learning by using course materials, references and personal notes	33
Additional learning by using library facilities, electronic databases and on-site information	30
Preparing seminars / laboratories, homework, portfolios, and essays	29
Tutorial activities[9]	11
Exams[10]	5
3.3. Total Individual Study Hours[11] *(NOSI$_{sem}$)*	**108**
3.4. Total Hours in the Curriculum (*NOAD$_{sem}$)*	**42**
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]	Cybersecurity introduction; 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. Specific competencies acquired[17]

Number of credits assigned to the discipline[18]			6	Credits distribution by competencies[19]
6.1. Professional competencies	PC1	Manages semantic integration in ICT		1
	PC2	Presents test results reports		2
	PC3	Perform data analysis		2
26.2. Transversal competencies	TC1	Monitor system performance		0.5
	TC2	Performs preservation of digital devices for forensic purposes		0.5

7. Course objectives (resulted from developed competencies)

7.1. Main course objective	Acquiring and understanding the necessary notions to automatize the analyse of the degree of risk of a system, from the point of view of data and integration vulnerability.
1.1. Specific course objectives	Accumulating knowledge related to the basic rules to use tools for automatic analyse of systems and data.

8. Content

8.1. Lectures[20]	**Teaching methods**[21]	**Hours**
Introduction to Risk Analysis: The basic concepts and principles of risk analysis, including risk assessment, risk management, and risk communication and application based on intelligent systems.	Lecture, use of video projector, discussions with students	2
Probability Theory: An overview of probability theory and its application in risk analysis.	Lecture, use of video projector, discussions with students	2
Statistical Analysis: The use of statistical analysis in risk assessment, including descriptive statistics, inferential statistics, and regression analysis.	Lecture, use of video projector, discussions with students	2
Data Mining: The use of intelligent data mining techniques in risk analysis, including association rules, clustering, and classification.	Lecture, use of video projector, discussions with students	2
Machine Learning: The use of machine learning algorithms in risk analysis, including decision trees, random forests, and support vector machines.	Lecture, use of video projector, discussions with students	2

Artificial Intelligence: The use of artificial intelligence techniques in risk analysis, including neural networks, genetic algorithms, and fuzzy logic.	Lecture, use of video projector, discussions with students	2
Case Studies: Case studies of the application of intelligent systems in risk analysis, including environmental risk assessment, financial risk analysis, and cybersecurity risk analysis.	Lecture, use of video projector, discussions with students	2
	Total lecture hours:	**14**

8.2. Practical activities (8.2.a. Seminar[22]/ 8.2.b. Laboratory[23]/ 8.2.c. Project[24])	**Teaching methods**	**Hours**
Probability and Statistical Analysis: How to use statistical software to analyze data and calculate probabilities related to different risk scenarios. How to use descriptive and inferential statistics to assess and communicate risk.	Use of video projector, discussions with students	4
Data Mining and Machine Learning: How to use data mining and machine learning techniques to analyze and classify data related to different risk scenarios. How to use association rules, clustering, and decision trees to identify patterns and make predictions.	Use of video projector, discussions with students	4
Artificial Intelligence and Risk Analysis: How to use artificial intelligence techniques, such as neural networks and genetic algorithms, to model and analyze risk scenarios. How to develop and train models that can make predictions and provide recommendations for risk management.	Use of video projector, discussions with students	4
Natural Language Processing and Risk Communication: How to use natural language processing techniques to analyze and summarize risk-related texts, such as news articles and social media posts. How to use sentiment analysis, opinion mining, and text summarization to communicate risk information to different audiences.	Use of video projector, discussions with students	8
Case Studies: Real-world case studies related to different areas of risk analysis, such as environmental risk assessment, financial risk analysis, and cybersecurity risk analysis. How to apply the concepts and techniques to solve practical problems and make recommendations for risk management.	Use of video projector, discussions with students	8
	Total seminar/laboratory hours:	28

9. Bibliography

9.1. Recommended Bibliography	1. W.Q. Yan, Introduction for Intelligent Surveillance, Springer 2019 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

7. Conjunction of the discipline's content with the expectations of the epistemic community, professional associations and significant employers of the specific study program[25]

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.

8. Evaluation

Activity Type	11.1 Evaluation Criteria	11.2 Evaluation Methods		11.3 Percentage in the Final Grade	Obs.[26]
11.4a Exam / Colloquy	• Theoretical and practical knowledge acquired (quantity, correctness, accuracy)	Tests during the semester[27]:	%	50% (minimum 5)	CEF
		Homework:	%		
		Other activities[28]:	%		
		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 of tools, processing and interpretation of results	• Written questionnaire • Oral response • Laboratory notebook, experimental works, reports, etc. • Practical demonstration		5% (minimum 5)	nCPE
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[29] To pass the exam, the candidate must have a basic knowledge of the risk analysis.					

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: |_0_|_5_| / |_0_|_9_| / |_2_|_0_|_2_|_4_|

Department Acceptance Date: |_0_|_6_| / |_0_|_9_| / |_2_|_0_|_2_|_4_|

	Academic Rank, Title, First Name, Last Name	**Signature**
Course Teacher	Professor PhD. Acu Ana Maria	
Study Program Coordinator	Lecturer PhD. Daniel Hunyadi	
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] *From the curriculum*

[19] *The credits allocated to the course are distributed across professional and transversal competences according to the specifics of the discipline*

[20] *Chapter and paragraph titles*

[21] *Exposition, lecture, board presentation of the studied topic, use of video projector, discussions with students (for each chapter, if applicable)*

[22] *Discussions, debates, presentations and/or analyses of papers, solving exercises and problems*

[23] *Practical demonstration, exercise, experiment*

[24] *Case study, demonstration, exercise, error analysis, etc.*

[25] *The relationship with other disciplines, the usefulness of the discipline on the labour market*

[26] *CPE – Conditions Exam Participation; nCPE – Does Not Condition Exam Participation; CEF - Conditions Final Evaluation; N/A – not applicable*

[27] *The number of tests and the weeks in which they will be taken will be specified*

[28] *Scientific circles, professional competitions, etc.*

[29] *The minimum performance standard in the competence grid of the study program is customized to the specifics of the discipline, if applicable*