SYLLABUS
Academic year 2025-2026

Dean,
Prof. dr. eng. Vasile-Ion Manta

1. Program data

1.1 Higher education institution	"Gheorghe Asachi" Technical University of Iași
1.2 Faculty	Automatic Control and Computer Engineering
1.3 Department	Computers
1.4 Field of studies	Computers and Information Technology
1.5 The cycle of studies[1]	Master
1.6 Study program	Artificial Intelligence

2. Subject data

2.1 Name of the subject / Code				**Intelligent Cyber-Security** (*Securitate cibernetică inteligentă*) / **AI.210**			
2.2 Course coordinator				Assoc. Prof. dr. eng. Elena ȘERBAN			
2.3 Application instructor				Lect. dr. eng. Alexandru ARCHIP			
2.4 Year of study[2]	2	2.5 Semester[3]	3	2.6 Type of assessment[4]	colloquium	2.7 Type of subject[5]	DA

3. Estimated total time of daily activities (hours per semester)

3.1 Number of hours per week	2	3.2 lectures	1	3.3a sem.		3.3b laboratory		3.3c project	1
3.4 Total hours in curriculum[6]	28	3.5 lectures	14	3.6a sem.		3.6b laboratory		3.6c project	14

Distribution of the time fund[7]	No. hours
Study by textbook, course support, bibliography and notes	25
Additional documentation in the library, on specialist electronic platforms and in the field	25
Preparation of seminars/labs/projects, assignments, reports and portfolios	20
Tutorial[8]	
Examinations[9]	2
Other activities:	

3.7 Total hours of individual study[10]	72
3.8 Total hours per semester[11]	100
3.9 Number of credits	4

4. Prerequisites (where applicable)

4.1 curriculum[12]	AI.101 - Fundamentals of Machine Learning AI.106 - Deep Learning
4.2 competences	- ability to work with ML techniques (clustering, classification, association analysis) - knowledge of how computers operate, how software systems/applications are built - knowledge of computer networks, distributed systems/applications and Web

5. Conditions (where applicable)

5.1 conducting the lectures[13]	• Blackboard, video projector
5.2 conducting the seminar / laboratory / project[14]	• Laboratory room with computers and Internet access

[1] *Bachelor / Master*
[2] *1-4 for Bachelor's, 1-2 for Master's*
[3] *1-8 for Bachelors, 1-3 for Masters*
[4] *Exam, colloquium or VP A/R – from the curriculum*
[5] *DF - fundamental subject, DID - subject in the field, DS - specialized subject or DC - complementary subject - from the education plan*
[6] *It is equal to 14 weeksx number of hours from point 3.1 (similar for 3.5, 3.6abc)*
[7] *The lines below refer to the individual study; the total is completed at point 3.7.*
[8] *Between 7 and 14 hours*
[9] *Between 2 and 6 hours*
[10] *The sum of the values on the previous lines, which refer to the individual study.*
[11] *The sum of the number of hours of direct teaching activity (3.4) and the number of hours of individual study (3.7); must be equal to the number of credits allocated to the subject (point 3.9)x 24 hours per credit.*
[12] *Mention the subjects that must be passed previously or equivalent*
[13] *Blackboard, video projector, flipchart, specific teaching materials, etc.*
[14] *Computing technique, software packages, experimental stands, etc.*

	• IntelliJ/ PyCharm or similar IDE (academic license) for Java/Python programming languages

6. Specific competences accumulated[15]

		Number of credits assigned to the subject[16]:	**4**	Distribution of credits per competences[17]
Professional competences	CP1	Knowledge of advanced concepts of computer science and information technology and the ability to work with these concepts.		0.5
	CP2	Scientific and practical research in the field of artificial intelligence.		0,5
	CP3	Problem solving using artificial intelligence methods and techniques.		1
	CP4	Design and development of artificial intelligence systems.		0.5
	CP5	Utilization of artificial intelligence tools and technologies.		0.5
	CP6			
	CPS1			
	CPS2			
Transversal competences	CT1	Legislation compliant application of the intellectual property rights and of the principles, norms and values of the professional ethics code within their own strategies for rigorous, effective and responsible work.		0.2
	CT2	Application of communication techniques and effective group work; developing empathic interpersonal communication skills and assuming leadership roles/functions in a multi-specialized team.		0.4
	CT3	Creating opportunities for continuous training and the effective utilization of learning resources and techniques for personal development.		0.4
	CTS			

7. Objectives of the subject (resulting from the grid of specific competences accumulated)

7.1 General objective of the subject	Understand both the benefits and drawbacks of using Artificial Intelligence/Machine Learning (AI/ML) in Cyber-Security. Gain theoretical and practical knowledge in building robust AI/ML models for Cyber-Security and in using these models in various practical scenarios.
7.2 Specific objectives	The goal of this course is to establish a bridge between AI/ML and Cyber-Security. Different defensive and offensive techniques are discussed in relation to AI/ML, emphasizing both the theoretical models and the practical implications of using these models alongside common security tools such as firewalls and antivirus programs.

8. Contents

8.1 Course[18]	Teaching methods[19]	Remarks
1. Introduction to Cybersecurity (2h) Computer security and human factors. Threat and defense models: Cyber Kill Chain & Advanced Persistent Threat. ***2. HIDS/NIDS and preventive approaches (2h)*** Attack patterns on host/network. Detection vs. prevention. Signature vs. anomaly based attack detection. Data sources (threat intelligence) and data models for AI/ML applications. ***3. Case studies - host attack patterns (2h)*** Command injection techniques. Data sources and AI/ML models for detection and prevention. ***4. Case studies - network attack patterns (2h)*** Denial-of-Service attacks and network intrusion techniques. Data sources and	Lectures with PDF presentations, explanations and answers to questions.	Lectures will take place during the first 7 weeks of the semester.

[15] *Competencies from the G1 and G1bis Grids of the study program, adapted to the specifics of the subject, for which credits are allocated (www.rncis.ro or the faculty website)*

[16] *From the education plan*

[17] *The credits allocated to the subject are distributed on professional and transversal competences according to the specifics of the subject*

[18] *Chapter and paragraph headings*

[19] *Exposition, lecture, blackboard presentation of the studied issue, use of video projector, discussions with students (for each chapter, if applicable)*

AI/ML models for detection and prevention. ***5. Case studies - social attacks (2h)*** Phishing attacks - impact and challenges. Data sources and AI/ML models for detection and prevention. ***6. Autonomous defense systems (2h)*** Concepts and vision. Security Orchestration, Automation and Response (SOAR) principles. ***7. Adversarial ML (2h)*** Advanced attack patterns and AI/ML models used in cyber attacks. Impact on AI/ML based defensive tools.		

Course references:

[1] Giovanni Apruzzese, Pavel Laskov, Edgardo Montes de Oca, Wissam Mallouli, Luis Brdalo Rapa, Athanasios Vasileios Grammatopoulos, and Fabio Di Franco. ***The Role of Machine Learning in Cybersecurity***. Digital Threats 4, 1, Article 8 (March 2023), 38 pages. 2023. https://doi.org/10.1145/3545574
[2] Dasgupta D, Akhtar Z, Sen S. Machine learning in cybersecurity: a comprehensive survey. The Journal of Defense Modeling and Simulation. 2022;19(1):57-106. doi:10.1177/1548512920951275
[3] M. Hemmati and M. A. Hadavi, ***Using Deep Reinforcement Learning to Evade Web Application Firewalls***, 2021 18th International ISC Conference on Information Security and Cryptology (ISCISC), Isfahan, Iran, Islamic Republic of, 2021, pp. 35-41, doi: 10.1109/ISCISC53448.2021.9720473.
[4] Vaclav Bartos, Martin Zadnik, Sheikh Mahbub Habib, Emmanouil Vasilomanolakis, ***Network entity characterization and attack prediction***, Future Generation Computer Systems, Volume 97, 2019, Pages 674-686, ISSN 0167-739X, https://doi.org/10.1016/j.future.2019.03.016
[5] Kaur, J., Garg, U. & Bathla, G. ***Detection of cross-site scripting (XSS) attacks using machine learning techniques: a review***. Artif Intell Rev 56, 12725–12769 (2023). https://doi.org/10.1007/s10462-023-10433-3
[6] Wei Zhang, Yueqin Li, Xiaofeng Li, Minggang Shao, Yajie Mi, Hongli Zhang, Guoqing Zhi, ***Deep Neural Network-Based SQL Injection Detection Method***, Security and Communication Networks, vol. 2022, Article ID 4836289, 9 pages, 2022. https://doi.org/10.1155/2022/4836289
[7] Manuel Sánchez-Paniagua, Eduardo Fidalgo, Enrique Alegre, Rocío Alaiz-Rodríguez, ***Phishing websites detection using a novel multipurpose dataset and web technologies features***, Expert Systems with Applications, Volume 207, 2022, 118010, ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2022.118010
[8] Mironeanu, Cătălin, Alexandru Archip, Cristian-Mihai Amarandei, and Mitică Craus. ***Experimental Cyber Attack Detection Framework***, Electronics 10, no. 14: 1682. 2021. https://doi.org/10.3390/electronics10141682
[9] https://attack.mitre.org/
[10] Wagner, C. and Dulaunoy, Al. and Wagener, G. and Iklody, A., ***MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform***, Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, pages 49-56, 2016, ACM - https://www.misp-project.org/

8.2a Seminar	Teaching methods[20]	Remarks
8.2b Laboratory	Teaching methods[21]	Remarks
8.2c Project	Teaching methods[22]	Remarks
Individual project to design and implement a multiagent system. Stages: ***1. Clarification of the project topic (2h)*** Establish target attack types and AI/ML models/algorithms to be studied and implemented ***2. Solution design (4h)*** Simulate the attack to understand the underlying pattern. Establish and acquire target data/data source. Build the data model and design the prevention solution. ***4. Implementation of the solution based on the design made in the previous stages (6h)*** Implement the demo application based on the previously selected AI/ML models/algorithms. Determine the final data format for the results. Integrate the result model with existing, classic detection & prevention tools or develop a	General and individual explanations, individual project work	Project activity will be performed during the last 7 weeks of the semester.

[20] *Discussions, debates, presentation and/or analysis of papers, solving exercises and problems*
[21] *Practical demonstration, exercise, experiment*
[22] *Case study, demonstration, exercise, error analysis, etc.*

stand-alone demo detection & prevention application based on this result model. ***5. Elaboration of the documentation, verification of its correctness (2h)***		
Applications (laboratory / project) references: See "Course references"		

9. Corroboration of the contents of the subject with the expectations of representatives of the epistemic community, professional associations and representative employers in the field related to the program[23]

While technological evolution has been beneficial to more robust and secure applications, it has also allowed a greater variety of cyber-attacks. Classic security tools tend to become obsolete, while a huge amount of both benign and malicious data is seemingly unused. Nowadays, AI/ML techniques seem to be the de facto standard in processing such data and cyber-security seems to be yet another field they could be beneficial for. Several high-ranking security companies are already employing such techniques to further their security products. This course could enrich professionals with the knowledge required to build better, more robust security tools.

Furthermore, similar lectures and research interests can be found at different universities such as Oxford, Harvard or Berkeley.

10. Evaluation

Type of activity	10.1 Evaluation criteria	10.2 Evaluation methods		10.3 Weight in the final grade
10.4a Colloquium	Acquired theoretical and practical knowledge (quantity, correctness, accuracy)	Periodic tests[24]:		50% (minimum 5)
		Homework:		
		Other activities[25]:		
		Final evaluation:	100%	
10.4b Seminar				
10.4c Laboratory				50% (minimum 5)
10.4d Project	The quality of the completed project, the correctness of the project documentation, the reasoning of the chosen solutions	• Self-assessment, presentation and/or defense of the project • Critical evaluation of a project		
10.5 Minimum performance standard[26]: grade 5 in the exam and applications (the average between laboratory and project)				

Date of completion,
5 January 2023

Signature of course coordinator,
Assoc. Prof. dr. eng. Elena ȘERBAN

Signature of application instructor,
Lect. dr. eng. Alexandru ARCHIP

Date of approval in the department,
21 September 2023

Director of department,
Assoc. prof. dr. eng. Andrei Stan

[23] *The connection with other subjects, the usefulness of the subject on the labor market*

[24] *The number of tests and the weeks in which they will be held will be specified.*

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

[26] *The minimum performance standard from the competences grid of the study program is customized to the specifics of the subject, if applicable.*