UNIVERSITATEA TEHNICĂ DIN CLUJ-NAPOCA
Facultatea de Electronică, Telecomunicații și Tehnologia Informației

www.etti.utcluj.ro

SYLLABUS

1. Data about the program of study

1.1 Institution	Technical University of Cluj-Napoca
1.2 Faculty	Faculty of Electronics, Telecommunications and Information Technology
1.3 Department	Communications
1.4 Field of study	Electronic Engineering, Telecommunications and Information Technologies
1.5 Cycle of study	Master of Science
1.6 Program of study / Qualification	Telecommunications / Master Multimedia Technologies / Master Artificial Intelligence and Signal Processing in Electronics and Telecommunications / Master
1.7 Form of education	Full time
1.8 Subject code	TC-E17.40

2. Data about the subject

2.1 Subject name	AI-Based Cybersecurity
2.2 Subject area	Theoretical area Methodological area Analytic area
2.3 Course responsible	Associate Professor Daniel ZINCA, Ph.D. Daniel.Zinca@com.utcluj.ro
2.4 Teacher in charge with seminar / laboratory / project	Associate Professor Daniel ZINCA, Ph.D. Daniel.Zinca@com.utcluj.ro

2.5 Year of study	2	2.6 Semester	1	2.7 Assessment	E	2.8 Subject category	DA/DO

3. Estimated total time

3.1 Number of hours per week	3	of which: 3.2 course	1	3.3 laboratory	2
3.4 To Total hours in the curriculum	42	of which: 3.5 course	14	3.6 laboratory	28

Distribution of time	hours
Manual, lecture material and notes, bibliography	20
Supplementary study in the library, online specialized platforms and in the field	12
Preparation for seminars / laboratories, homework, reports, portfolios and essays	20
Tutoring	3
Exams and tests	3
Other activities:	

3.7 Total hours of individual study	58
3.8 Total hours per semester	100
3.9 Number of credit points	4

4. Pre-requisites (where appropriate)

4.1 curriculum	N. A.
4.2 competence	N. A.

5. Requirements (where appropriate)

5.1. for the course	Amphitheatre, Cluj-Napoca
5.2. for the seminars / laboratories / projects	Laboratory, Cluj-Napoca

6. Specific competences

Professional competences	C1. Use of the fundamental elements related to devices, circuits, systems, instrumentation and electronic technology C2. Applying the basic methods for the acquisition and processing of signals C3. Application of the basic knowledge, concepts and methods regarding the architecture of computer systems, microprocessors, microcontrollers, languages and programming techniques C4. Design, implementation and operation of data, voice, video and multimedia services. This is based on the understanding and the application of fundamental concepts in telecommunications and transmission of information C5. Selecting, installing, configuring and operating fixed or mobile telecommunications equipment. Equipping a site with usual telecommunications networks C6. Solving specific problems of the broadband communications networks: propagation in different environments, circuits and equipment for high frequencies (microwaves and optical). C7. Design, implementation and testing of systems and of various types of applications (signal processing, classification, regression, detection, natural language processing, shape recognition) based on machine learning or deep learning techniques
Cross competences	N.A.

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

7.1 General objective	Development of professional skills in the field of Artificial Intelligence applied to cybersecurity
7.2 Specific objectives	1. Assimilation of the theoretical knowledge regarding the operation of cybersecurity systems 2. Development of skills and abilities needed to design and implement of cybersecurity detection systems

8. Contents

8.1 Lecture (syllabus)	Teaching methods	Notes
1. Introduction to Cybersecurity.	The discipline content and the acquired skills are in agreement with the expectations of the professional	N/A
2. Artificial Intelligence Applications to Cybersecurity.		
3. Artificial Intelligence algorithms for spam email and phishing		
4. Artificial Intelligence-based Intrusion Detection Systems		
5. Generative Adversarial Networks and Cybersecurity applications		
6. Feature extraction in Intrusion Detection Systems		
7. DNS Exfiltration and DNS tunneling detection using Machine Learning ALgorithms		
Bibliography: 1. E. Tsukerman, “Machine Learning for Cybersecurity Cookbook”, Packtpub, 2019. 2. A. Parisi. “Hands-on Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber-attacks and detecting threats and network anomalies”, Packtpub, 2019 3. A-G. Mari, D. Zinca, V. Dobrota. Development of a Machine-Learning Intrusion Detection System and Testing of Its Performance Using a Generative Adversarial Network, Sensors, Vol. 23, issue 3, 2023		
8.2 Laboratory	Teaching methods	Notes
1. Google Colab platform and libraries used	Practical experiments on physical, virtual, cloud and emulator equipment.	N/A
2. Spam email detection using Machine Learning algorithms.		
3. Phising email detection using Artificial Intelligence		
4. Implementation of Snort rules for the implementation of Intrusion Detection Systems		
5. The NSL-KDD dataset for Machine Learning Applications		
6. Implementation of Intrusion Detection Systems using Machine Learning algorithms		
7. Generative Adversarial Networks GAN in Intrusion Detection Systems		
8. DDoS detection using Machine Learning algorithms and the CICDDoS2019 dataset		
9. Feature extraction for Machine Learning-based Intrusion Detection using Wireshark and Python		
10. VPN traffic detection using Machine Learning and the ISCXVPN2016 dataset		
11. DNS Exfiltration using Machine Learning and the CIC-Bell-DNS-EXF-2021 dataset		
12. Machine learning algorithms for cybersecurity in Azure/AWS		
13. Machine Learning application for detecting anomalies in Microsoft Windows Event Log.		
14. Machine Learning Pipeline for Cybersecurity applications		
Bibliography 1. E. Tsukerman, “Machine Learning for Cybersecurity Cookbook”, Packtpub, 2019. 2. A. Parisi. “Hands-on Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber-attacks and detecting threats and network anomalies”, Packtpub, 2019		

3. A-G. Mari, D. Zinca, V. Dobrota. Development of a Machine-Learning Intrusion Detection System and Testing of Its Performance Using a Generative Adversarial Network, Sensors, Volume 23, issue 3, 2023

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

The discipline content and the acquired skills are in agreement with the expectations of the professional Competences acquired will be used in the following COR occupations (Electronics Engineer; Telecommunications Engineer; Electronics Design Engineer; System and Computer Design Engineer; Communications Design Engineer) or in the new occupations proposed to be included in COR (Sale Support Engineer; Multimedia Applications Developer; Network Engineer; Communications Systems Test Engineer; Project Manager; Traffic Engineer; Communications Systems Consultant).

10. Evaluation

Activity type	10.1 Assessment criteria	10.2 Assessment methods	10.3 Weight in the final grade
10.4 Course	The level of acquired theoretical knowledge and practical skills	Written exam including theory and problems (25 questions)	75%
10.5 Seminar/ Laboratory	The level of acquired knowledge and abilities	Multiple choice tests at the end of each lab	25%
10.6 Minimum standard of performance			

Qualitative point of view

Minimal theoretical and practical knowledge:

- ✓ Understanding of the architecture, functionality, stack of a cybersecurity detection
- ✓ Ability to perform cybersecurity detection using AI algorithms

Minimal acquired competences:

- ✓ Ability to develop Artificial Intelligence Algorithms to detect a specific cybersecurity attack
- ✓ Ability to analyze and improve performance of Artificial Intelligence-based Cybersecurity applications

Quantitative point of view

- ✓ Minimal mean at the exam 5
- ✓ Final mark = 0.75 x Exam + 0.25 x Mean of the marks at the lab tests

Date of filling in:	**Responsible**	**Title First name SURNAME**	**Signature**
19.06.2024	Course	Associate Professor Daniel ZINCA, Ph.D.	
	Applications	Associate Professor Daniel ZINCA, Ph.D.	

Date of approval in the Council of the Communications Department 10.07.2024	Head of Communications Department Prof. Virgil DOBROTA, Ph.D.
Date of approval in the Council of the Faculty of Electronics, Telecommunications and Information Technology 11.07.2024	Dean Prof. Ovidiu POP, Ph.D.