Universitatea Naţională de Ştiinţă şi Tehnologie Politehnica Bucureşti
Facultatea de Electronică, Telecomunicaţii şi
Tehnologia Informaţiei

COURSE DESCRIPTION

1. Program identification information

1.1 Higher education institution	**National University of Science and Technology Politehnica Bucharest**
1.2 Faculty	**Electronics, Telecommunications and Information Technology**
1.3 Department	**Telecommunications**
1.4 Domain of studies	Electronic Engineering, Telecommunications and Information Technology
1.5 Cycle of studies	Bachelor/Undergraduate
1.6 Programme of studies	Networks and Telecommunications Software

2. Date despre disciplină

2.1 Course name (ro) (en)				Detecţia şi prevenţia atacurilor cibernetice Detection and Prevention of Cyberattacks			
2.2 Course Lecturer				Dr. ing. Amelia SARU, Conf. dr. ing. Şerban Georgică OBREJA			
2.3 Instructor for practical activities				As. drd. ing. Dan CURĂVALE			
2.4 Year of studies	4	2.5 Semester	2	2.6. Evaluation type	V	2.7 Course regime	Ob
2.8 Course type		S	2.9 Course code	04.S.08.O.312		2.10 Tipul de notare	Nota

3. Total estimated time (hours per semester for academic activities)

3.1 Number of hours per week	3	Out of which: 3.2 course	2	3.3 seminary/laboratory	1
3.4 Total hours in the curricula	42	Out of which: 3.5 course	28	3.6 seminary/laboratory	14
Distribution of time:					hours
Study according to the manual, course support, bibliography and hand notes Supplemental documentation (library, electronic access resources, in the field, etc) Preparation for practical activities, homework, essays, portfolios, etc.					50
Tutoring					4
Examinations					4
Other activities (if any):					0

3.7 Total hours of individual study	58.00
3.8 Total hours per semester	100
3.9 Number of ECTS credit points	4

4. Prerequisites (if applicable) (where applicable)

4.1 Curriculum	- Basic knowledge of computer networks and protocols - Fundamentals of operating systems - Introduction to cybersecurity principles - Basic programming skills (e.g., Python or similar)

4.2 Results of learning	- Understand the nature and types of cyberattacks - Learn techniques for detecting cyber threats and intrusions - Develop skills to implement preventive measures and security controls - Analyze real-world cyberattack cases and responses - Gain hands-on experience in identifying vulnerabilities and deploying security tools

5. Necessary conditions for the optimal development of teaching activities (where applicable)

5.1 Course	According to the university studies regulations at UNSTPB. The presentations are delivered using modern display technologies, such as a video projector or an LCD screen.
5.2 Seminary/ Laboratory/Project	The laboratory takes place on a dedicated infrastructure that includes computers or laptops with Internet access, running a Kali Linux operating system. A variety of software tools are installed and used, including: - Splunk, Elastic Stack - Nessus or OpenVAS

6. General objective *(Reffering to the teachers' intentions for students and to what the students will be thought during the course. It offers an idea on the position of course in the scientific domain, as well as the role it has for the study programme. The course topics, the justification of including the course in the currcula of the study programme, etc. will be described in a general manner)*

In the context of the digital society, the field of cybersecurity has gained major importance. The ability to prevent cyber attacks is a key component for maintaining the security of todayţs society. The general objective of this course is to provide the students with knowledge and skills to understand and detect cyber attacks, to implement preventive measures and security controls, and to identify vulnerabilities and deploy security tools.

7. Competences *(Proven capacity to use knowledge, aptitudes and personal, social and/or methodological abilities in work or study situations and for personal and proffesional growth. They refflect the empolyers requirements.)*

Specific Competences	- Ability to identify different types of cyberattacks. - Proficiency in using detection tools and intrusion detection systems (IDS). - Skills to configure and deploy security measures. - Capacity to analyze security logs and respond to incidents. - Competence to develop and implement preventive security policies. - Correlates and integrates the acquired knowledge to achieve a deeper understanding of the field. - Applies theoretical knowledge in real-world contexts, demonstrating operational skills. - Uses standardized methods and tools specific to the field to carry out the processes of assessment and diagnosis of a given situation, based on the identified/reported problems, and identifies appropriate solutions. - Argues and analyzes coherently and correctly the context of applying the fundamental knowledge of the field, using the key concepts of the discipline and the specific methodology.
Transversal (General) Competences	- Critical thinking and analytical skills - Problem-solving and decision-making abilities - Teamwork and collaboration in the laboratory sessions - Communication skills in articulating security issues and solutions - Ethical awareness regarding cybersecurity practices

8. Learning outcomes *(Synthetic descriptions for what a student will be capable of doing or showing at the completion of a course. The learning outcomes reflect the student's acomplishments and to a lesser extent the teachers' intentions. The learning outcomes inform the students of what is expected from them with respect to performance and to obtain the desired grades and ECTS points. They are defined in concise terms, using verbs similar to the examples below and indicate what will be required for evaluation. The*

learning outcomes will be formulated so that the correlation with the competences defined in section 7 is highlighted.)

Knowledge	*The result of knowledge aquisition through learning. The knowledge represents the totality of facts, priciples, theories and practices for a given work or study field. They can be theoretical and/or factual.* - Types and mechanisms of cyberattacks (e.g., malware, phishing, DDoS) - Detection technologies (IDS, IPS, SIEM systems) - Vulnerability assessment
Skills	*The capacity to apply the knowledge and use the know-how for completing tasks and solving problems. The skills are described as being cognitive (requiring the use of logical, intuitive and creative thinking) or practical (implying manual dexterity and the use of methods, materials, tools and intrumentation).* Threat Identification and Analysis - Recognize and categorize various types of cyberattacks - Analyze network traffic and logs to detect malicious activities Use of Security Tools and Technologies - Deploy and configure Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and SIEM solutions - Conduct vulnerability scans and interpret results 3. Incident Response and Forensic Skills - Investigate security incidents and collect relevant evidence - Develop and implement effective incident response strategies Cybersecurity Policy Implementation - Design and enforce security policies to prevent attacks - Educate users and organizations about best practices in cybersecurity Application of Artificial Intelligence in Security - Use machine learning models to detect anomalies and predict threats - Implement AI-based solutions for proactive cybersecurity defense Hands-on Technical Proficiency - Perform penetration testing and vulnerability assessments - Simulate cyberattack scenarios and respond effectively Critical Thinking and Problem Solving - Analyze complex security problems and identify optimal solutions - Adapt to evolving cyber threat landscapes with innovative approaches

Responsability and autonomy	*The student's capacity to autonomously and responsably apply their knowledge and skills.* Selects suitable bibliographic sources and analyses them. Adheres to academic ethics principles by correctly citing all utilised bibliographic references. Demonstrates openness and adaptability to new learning contexts. Engages in collaboration with peers and academic staff during educational activities. Demonstrates autonomy in organising their own learning context or in addressing a problem situation. Displays social responsibility through active involvement in student life and academic community events. Promotes and contributes new solutions in their area of expertise to enhance the quality of social life. Recognises the value of their engineering contributions in identifying viable and sustainable solutions to social and economic problems (social responsibility). Applies ethical and professional principles in analysing the technological impact of proposed solutions within their field of expertise. Analyses and capitalizes on business and entrepreneurial development opportunities in their area of specialisation. Demonstrates management skills for real-world situations (time management, collaboration versus conflict).

9. Teaching techniques *(Student centric techniques will be considered. The means for students to participate in defining their own study path, the identification of eventual fallbacks and the remedial measures that will be adopted in those cases will be described.)*

Based on the analysis of students' learning characteristics and their specific needs, the teaching process will explore both expository methods (lecture, presentation) and conversational-interactive methods, grounded in discovery-based learning models that facilitate both direct and indirect exploration of reality (experiment, demonstration, modeling), as well as action-based approaches such as exercises, practical activities, and problem-solving. Lectures will be supported by PowerPoint presentations or various videos made available to students. Each class will begin with a review of previously covered chapters, emphasising concepts studied in the last session. Presentations will incorporate images and diagrams to ensure that information is easily understood and assimilated. The course covers both theoretical content and practical activities designed to support students in their learning efforts and to foster optimal collaboration and communicative relationships within a learning environment conducive to discovery. Particular emphasis will be placed on practicing active listening and assertive communication skills, as well as on feedback construction mechanisms, as means of behavioural regulation in various situations and as ways to adapt pedagogical approaches to the students' learning needs.

10. Contents

COURSE		
Chapter	**Content**	**No. hours**
1	Introduction to Cybersecurity and Cyberattacks - Overview of cybersecurity principles - Common types of cyberattacks (malware, phishing, DDoS, zero-day exploits) - The cyberattack lifecycle and threat landscape	5

2	Understanding Network Security - Network protocols and vulnerabilities - Firewalls, VPNs, and basic security controls - Common network-based attacks and their detection	4
3	Detection Technologies and Tools - Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) - Security Information and Event Management (SIEM) systems - Log analysis and anomaly detection	3
4	Incident Response and Forensics - Detecting and analyzing security incidents - Evidence collection and preservation - Incident response strategies	3
5	Vulnerability Assessment and Penetration Testing - Scanning and assessing vulnerabilities - Penetration testing methodologies	3
6	Artificial Intelligence in Cybersecurity - Machine Learning (ML) and AI fundamentals - Using AI for anomaly detection and threat prediction - Case studies of AI-based cyberattack detection	7
7	Preventive Measures and Security Policies - Configuring security controls	3
	Total:	28

Bibliography:

Artificial Intelligence for Cybersecurity; Mark Stamp, Corrado Aaron Visaggio, Francesco Mercaldo, Fabio Di Troia; Springer Nature Switzerland AG, iulie 2022
Computer Security Principles and Practice, Second Edition; William Stallings, Lawrie Brown; Pearson Education, 2012.
The Practice of Network Security Monitoring: Understanding Incident Detection and Response 1st Edition; by Richard Bejtlich; No Starch Press, 2013

LABORATORY

Crt. no.	Content	No. hours
1	Network Traffic Monitoring and Log Analysis - Objective: Learn to capture and analyze network traffic - Activities: Use tools like Wireshark to observe normal network behavior and identify suspicious patterns	2
2	Implementing and Configuring IDS/IPS - Objective: Deploy and configure Intrusion Detection and Prevention Systems (Snort) - Activities: Create rules for detecting common attack signatures, simulate attacks, and review alerts - Outcome: Skills in real-time attack detection and response	2

3	SIEM Deployment and Log Correlation Analysis - Objective: Collect and analyze security logs using SIEM (e.g., Elastic Stack) - Activities: Set up log collection, create search queries to detect attacks, and generate incident reports - Outcome: Improved ability to correlate logs and identify security breaches	2
4	Vulnerability Scanning and Penetration Testing - Objective: Conduct vulnerability assessments using tools like OpenVAS - Activities: Identify vulnerabilities, attempt controlled exploitation, and suggest mitigation measures - Outcome: Understanding of common vulnerabilities and defensive strategies	4
5	AI-based Anomaly Detection	4
	Total:	14

Bibliography:

https://www.kali.org/
https://www.snort.org/
https://github.com/elastic/elasticsearch-py/
https://www.openvas.org/

11. Evaluation

Activity type	11.1 Evaluation criteria	11.2 Evaluation methods	11.3 Percentage of final grade
11.4 Course	Final evaluation: - knowledge of fundamental theoretical concepts; - knowledge of how to apply theory to specific problems in the field of detection and prevention of cyber attacks; - comparison and evaluation of various techniques and methods used in practice.	Written exame	20
11.5 Seminary/laboratory/project	Practical application	Development of a practical application based on the concepts acquired during the course and laboratory sessions.	50
	Solving the lab requirements.	Solve the lab requirements	30
11.6 Passing conditions			
Obtaining 50% of the total score.			

12. Corroborate the content of the course with the expectations of representatives of employers and representative professional associations in the field of the program, as well as with the current state of knowledge in the scientific field approached and practices in higher education institutions in the European Higher Education Area (EHEA)

The course emphasizes practical skills such as using detection tools, configuring security systems, and applying AI techniques, aligning with employers' demand for graduates who can immediately contribute to cybersecurity teams.

Laboratory activities simulate real attack scenarios, incident response, and AI-based detection, ensuring students acquire applicable experience.

Date	Course lecturer	Instructor(s) for practical activities
25.09.2025	Dr. ing. Amelia SARU	Conf. dr. ing. Șerban Georgică OBREJA

Date of department approval	Head of department
26.09.2025	Conf. Dr. Serban Georgica Obreja

Date of approval in the Faculty Council	Dean
26.09.2025	Prof. Dr. Mihnea Udrea