Cyber-physical Systems Institute			Semester 3. of the curriculum 2026-27-1			
Name of the subject:	Code of the subject:	Credits:	Weekly hours:			
				lec	sem	lab
AI based solutions for cyber defense	NKXMK1EMNF	5	full-time	2	0	2
Responsible person for the subject: Balázsné Dr. Kail Eszter			Classification: senior lecturer			
Subject lecturer(s): Balázsné Dr. Kail Eszter, Dr. Leitold Ferenc, Dobrovodsky Patrik						
Prerequisites:	NSXPPDEMNF	Programming paradigms and data structures				
Way of the assessment:	exam					

Course description	
Goal:	The aim of the course is to provide students with a comprehensive understanding of the fundamental methods of artificial intelligence and machine learning, as well as their applications in the field of cybersecurity. Students will gain insight into modern AI-based cybersecurity solutions, with particular emphasis on anomaly detection, malware analysis, support for red teaming activities, and the security aspects of generative artificial intelligence and Large Language Models (LLMs). Furthermore, the course aims to develop practical skills in the application, evaluation, and security-oriented analysis of artificial intelligence methods and techniques.
Course description:	The course provides an overview of the fundamental concepts of artificial intelligence, machine learning, and neural networks, and introduces their applications in various areas of cybersecurity. Students will become familiar with classical machine learning algorithms and their use in tasks such as anomaly detection and malware detection. The course places particular emphasis on cybersecurity applications of reinforcement learning, AI-based red teaming solutions, the operation of generative artificial intelligence and Large Language Models (LLMs), as well as attacks against and defenses for these technologies. Furthermore, the course examines the role of Explainable Artificial Intelligence (XAI) in security decision support and in improving the transparency, trustworthiness, and reliability of AI systems. The course also includes project-based practical components, during which students apply the acquired methods and techniques to real-world cybersecurity problems.

Lecture schedule	
Education week	Topic
1.	Introduction to Artificial Intelligence
2.	Machine Learning Fundamentals I – Basic Concepts
3.	Machine Learning Fundamentals II – Classical Algorithms
4.	Machine Learning Fundamentals III – Classical Algorithms
5.	Anomaly detection
6.	Reinforcement Learning-Based Cybersecurity Solutions and Red Teaming
7.	Malware Detection and Analysis
8.	Generative AI and Large Language Models (LLMs)
9.	Attacks and Defenses Against Machine Learning and LLM-Based System
10.	Explainable Artificial Intelligence (XAI) in Cybersecurity
11.	AI-Based Solutions for Cyber Defense
12.	Holiday

13.	Project presentation
14.	Project presentation

Mid-term requirements	
Conditions for obtaining a mid-term grade/signature	**Participation at the lessons is mandatory. Students who missed more than 30% of lessons must take the signature retake exam. A successful completion of the project is mandatory to acquire signature.**

Assessment schedule	
Education week	Topic
13.	Project presentation
14.	Project presentation

Method used to calculate the *mid-term grade* (to be filled out only for subjects with mid-term grades)

Type of the replacement	
Type of the replacement of written test/mid-term grade/signature	

Type of the exam (to be filled out only for subjects with exams)

Written exam

Calculation of the exam mark (to be filled only for subjects with exams)

The final grade is calculated as the average of the project work and the written examination results; however, obtaining at least a passing grade in both components is a mandatory requirement.

Final grade calculation methods:

The final grade will be calculated using the following scale:

Achieved result	Grade
87% - 100%	excellent (5)
75%- 86%	good (4)
64% -74%	satisfactory (3)
51% - 63%	pass (2)
0 - 50 %	failed (1)

References

Obligatory:	
Recommended:	
Other references:	