Óbuda University John von Neumann Faculty of Informatics	Institute for Cyber-physical Systems

Name and code: *AI-based solutions for cyber defence (NKXMK1EMNF)* **Credits*: 5***

Computer Science Engineering MSc programme *2024/25 year II. semester*

Subject lecturers: Dr. Kail Eszter, Dr. habil. Dineva Adrienn, Dr. Leitold Ferenc

Prerequisites (with code):	

Weekly hours: 4	Lecture: 2	Seminar.: 0	Lab. hours: 2	Consultation: 0

Way of assessment:	mid-term tests, project work

Course description:

Goal: The aim of the course is to provide students with a thorough overview of selected areas of artificial intelligence, as well as to acquire practical and methodological knowledge and skills related to the application of artificial intelligence methods and algorithms. This includes the ability to evaluate performance and select appropriate techniques for a given problem area. Students should be able to assess the quality of the results of such techniques

Course description: The course introduces the fundamentals of machine learning and neural networks, and provides insights into various areas of cybersecurity where artificial intelligence-based techniques can be applied to achieve more effective solutions. The course covers the following areas of cybersecurity: threats and defensive techniques related to electronic mail, malware analysis, and intrusion detection.

Lecture schedule

Education week	*Topic*
1.	Introduction to Artificial Intelligence
2.	Machine learning basics I.
3.	Machine learning basics II.
4.	Machine learning basics III.
5.	AI based solutions in cybersecurity
6.	Reinforcement Learning Introduction
7.	Threats and vulnerabilities of machine learning models and LLMs
8.	Malware detection and analysis I.
9.	Malware detection and analysis II.
10.	Holiday
11.	Malware detection and analysis III.
12.	Summary
13.	Test, Project presentation
14.	Retake test

Midterm requirements

Education week	*Topic*
13	Test
14	Retake test

Final grade calculation methods

Achieved result	**Grade**
89%-100%	excellent (5)
76%-88<%	good (4)
63%-75<%	average (3)
51%-62<%	satisfactory (2)
0%-50<%	failed (1)

Type of exam

Written exam and project work

Type of replacement

Once in the first week of the exam period.

References

Mandatory: Lecture notes on Moodle system

Recommended:

- Witten, E. Frank und M. Hall, Data Mining: Practical Machine Learning Tools and Techniques, 3. (2011)
- Russell, Stuart Jonathan, and Peter Norvig: Artificial intelligence: A modern Approach (1995)
- Richard S. Sutton and Andrew G. Barto: reinforcement Learnig: An Introduction
- . Paul Iusztin and Maxime Labonne, LLM Engineer's Handbook: Master the art of engineering large language models from concept to production, (2024) Packt Publishing ISBN 978-1-83620-007-9