Institute of Cyberphysical Systems			Semester 3. of the curriculum 2026-27-1			
Name of the subject	Code of the subject	Credits	Weekly hours			
				lec	sem	lab
MLSecOps	NKXML1EMNF	5	full-time	1	1	2
Responsible person for the subject: Dr. habil. Rita Fleiner			Classification: Associate professor			
Subject lecturer(s): Dr. Zoltán Fried						
Prerequisites:	NKXMO1EMNF	Modern operating systems				
Way of the assessment:	mid-term grade					

Course description	
Goal:	To introduce students to the concepts of DevOps, DevSecOps, MLOps, and MLSecOps, including agile methodologies, cloud platforms, development and operations tools, and automation. The curriculum covers in detail the basic concepts, tools, techniques, principles, challenges, and solutions of DevOps and DevSecOps, including security threats and vulnerabilities. The course introduces students to regulatory frameworks and regulations such as PCI-DSS, HIPAA, and GDPR, the basic concepts, tasks, principles, and levels of MLOps. It covers data and model management, versioning, deployment, MLOps system monitoring, data drift, and concept drift. The course covers automation, scheduling, and scaling in MLOps, AI ethics and security, and MLSecOps principles, challenges, security threats, and vulnerabilities. Finally, the course introduces defense methods and Adversarial Machine Learning techniques, as well as the design of the MLSecOps system.
Course description:	Introduction to DevOps, DevSecOps, MLOps and MLSecOps concepts. Agile methodologies, cloud platforms, development and operational tools, automation. Basic concepts, tools, techniques of DevOps. DevSecOps principles, challenges, solutions, security threats, vulnerabilities. Regulatory frameworks, regulations. Basic concept, task, principles and levels of MLOps. Data and model management, versioning, deployment. MLOps system monitoring, data drift and concept drift. Automation, scheduling and scaling in MLOps. AI ethics and security. MLSecOps principles, challenges, security threats, vulnerabilities. Protection methods, Adversarial Machine Learning techniques. MLSecOps system design.

Lecture schedule	
Education week	Topic
1.	Motivation, DevOps and MLOps principles in Python
2.	People, data, model, technology
3.	Machine learning tasks, ML development: data preparation
4.	Production ready code, Pipelines, MLflow, Rest API
5.	MLFlow practice, DevOps
6.	DevOps, MLOps levels, deployment strategies, docker, monitoring
7.	Scheduling, Airflow
8.	Cloud: automation, CICD, testing
9.	DevSecOps, Data vulnerabilities
10.	ML Model and MLOps system vulnerabilities
11.	Security practice
12.	Frameworks, AI ethics and security, MLSecOps system design
13.	Mid-term exam, Homework project submission/presentation
14.	Reatke mid-term exam, Homework project presentation

Mid-term requirements	
Conditions for obtaining a mid-term grade/signature:	Students must reach 50% of result of mid-term exam and 60% of result of homework project to pass.

Assessment schedule	
Education week	Topic
13.	Mid-term exam: Lecture topics
14.	Retake mid-term exam: Lecture topics

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

It will be calculated by mean of result of mid-term exam and homework project.

88% –: excellent (5)
77% –: good (4)
66% –: satisfactory (3)
55% –: pass (2)
0% –: failed (1)

Late summit for homework project indicates 10%/day minus from result of the homework project.

Type of the replacement	
Type of the replacement of written test/mid-term grade/signature:	The student may retake the mid-term exam in week 14th or during the first week of the exam period.

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

-

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

-

References

Obligatory:	– Bell, L., Brunton-Spall, M., Smith, R., & Bird, J. (2017). Agile application security: enabling security in a continuous delivery pipeline. " O'Reilly Media, Inc.". ISBN-13: 978-1491938843 – Moodle materials
Recommended:	– WILSON, Glenn. DevSecOps: A Leader's Guide to Producing Secure Software Without Compromising Flow, Feedback and Continuous Improvement. Rethink Press, 2020. ISBN-13: 978-1781335024 – TREVEIL, Mark, et al. Introducing MLOps. O'Reilly Media, 2020. ISBN-13: 978-1492083290 – Gift, Noah., Deza, Alfredo. Practical MLOps. N.p.: O'Reilly Media, 2021. ISBN-13. 978-1098103019
Other references:	-