

Kiberfizikai Rendszerek Intézet			Mintatanterv szerinti 3. félév 2025-26-1			
Tantárgy neve:	Kódja:	Kredit:	Óraszám			
				ea	tgy	lab
MLSecOps	NKXML1HMLF	5	levelező féléves	5	5	10
Tárgyfelelős: Dr. habil. Fleiner Rita			Beosztás: egyetemi docens			
Oktató(k): Fleiner Rita, Boros Gerzson, Budaházy Gábor						
Előtanulmányi feltételek:		Korszerű operációs rendszerek				
Számonkérés módja:	évközi jegy					
A tananyag						
Oktatási cél:	A hallgatók megismertetése a DevOps, DevSecOps, MLOps és MLSecOps fogalmakkal, beleértve az agilis módszertanokat, cloud platformokat, fejlesztési és operációs eszközöket, valamint az automatizációt. A tananyag részletesen tárgyalja a DevOps és DevSecOps alapfogalmait, eszközeit, technikáit, alapelveit, kihívásait, megoldásait, beleértve a biztonsági fenyegetéseket és sebezhetőségeket. A kurzus bevezeti a hallgatókat a szabályozási keretrendszerekbe és előírásokba, mint például PCI-DSS, HIPAA és GDPR, az MLOps alapfogalmába, feladataiba, alapelveibe és szintjeibe. Foglalkozik az adat- és modellkezeléssel, verziózással, deploymenttel, az MLOps rendszer monitorozásával, data drifttel és concept drifttel. A kurzus része az automatizálás, ütemezés és skálázás MLOps-ban, az AI etika és biztonság, valamint az MLSecOps alapelvei, kihívásai, biztonsági fenyegetések és sebezhetőségek. Végül, a kurzus bemutatja a védelmi módszereket és az Adversarial Machine Learning technikákat, valamint az MLSecOps rendszer tervezését.					
Tematika:	Bevezetés a DevOps, DevSecOps, MLOps és MLSecOps fogalmakba. Agilis módszertanok, cloud platformok, fejlesztési és operációs eszközök, automatizáció. DevOps alapfogalmai, eszközei, technikái. DevSecOps alapelvei, kihívásai, megoldásai, biztonsági fenyegetések, sebezhetőség. Szabályozási keretrendszerek, előírások. MLOps alapfogalma, feladata, alapelvei és szintjei. Adat és modell kezelése, verziózása, deployment. MLOps rendszer monitorozása, data drift és concept drift. Automatizálás, ütemezés és skálázás MLOps-ban. AI etika és biztonság. MLSecOps alapelvei, kihívásai, biztonsági fenyegetések, sebezhetőség. Védelmi módszerek, Adversarial Machine Learning technikák. MLSecOps rendszer tervezés.					

Féléves ütemezés	
Oktatási hét (konzultáció)	Témakör
1.	Motiváció, DevOps és MLOps elvek Pythonban
2.	Ember, adat, modell, technológia
3.	Gépi tanulás feladatai, ML fejlesztés: adatelőkészítés
4.	Production ready kód, Pipelineok, Mlflow, Rest API
5.	MLFlow gyakorlat, DevOps
6.	DevOps, MLOps szintjei, deployment stratégiák, docker, monitorozás
7.	Ütemezés, Airflow
8.	Cloud - AWS MLOps gyakorlat: automatizálás, CICD, tesztelés
9.	DevSecOps, Adatok sérülékenysége
10.	ML Modell és MLOps rendszer sérülékenysége
11.	Security gyakorlat
12.	Keretrendszerek, AI etika és biztonság, MLSecOps rendszer tervezés

13.	Zárhelyi dolgozat
14.	Projektfeladat beadása, Zárhelyi dolgozat pótlása
Félévközi követelmények	
Évközi jegy / aláírás megszerzésének feltételei:	A hallgatók 12 foglalkozáson keresztül heti szintű feladatokat kapnak, melyek benyújtási határideje a következő konzultáció előtti nap. A kurzus sikeres teljesítéséhez a heti feladatok 70%-át sikeresen meg kell oldani 80%-os teljesítéssel. A sikeres évközi jegy feltétele, hogy mind a zárhelyi dolgozaton, mind a projektfeladaton legalább 50%-os eredményt érjen el a hallgató.
Zárhelyi dolgozatok	
Oktatási hét	Témakör
13.	Zárhelyi dolgozat (max. 50 pont szerezhető)
14.	Projektfeladat (max. 50 pont szerezhető)
Az évközi jegy kialakításának módszere (csak évközi jegyes tárgyak esetében töltendő ki)	
A végső pontszám a zárhelyi dolgozat és a projektfeladat eredményén elért pontszámok összege	
Pótlás módja	
A ZH / évközi jegy / aláírás pótlásának módja:	14. héten a zárhelyi dolgozat pótolható. A projektfeladat leadási határideje 12.09., pótleadás határideje 12.12. Pótleadás esetén 10 pont levonásra kerül, így legfeljebb 40 pont érhető el.
Vizsga módja (csak vizsgás tantárgy esetében töltendő ki)	
-	
Vizsgajegy kialakítása (csak vizsgás tantárgy esetében töltendő ki)	
-	
Az egyes érdemjegyek ponthatárai:	
88 – 100 pont: jeles (5) 76 – 87 pont: jó (4) 64 – 75 pont: közepes (3) 52 – 63 pont: elégséges (2) 0 – 51 pont: elégtelen (1)	
Irodalom	
Kötelező:	- 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 - Órai előadásokhoz kapcsolódó prezentációk anyagai, jegyzetek
Ajánlott:	- 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
Egyéb segédletek:	https://elearning.uni-obuda.hu/