

Kiberfizikai Rendszerek Intézet			Mintatanterv szerinti 3 félév 2025-26-1			
Tantárgy neve:	Kódja:	Kredit:	Óraszám			
				ea	tg	lab
MI-alapú megoldások a kibervédelemben	NKXMK1HMLF	5	levelező féléves	10	0	10
Tárgyfelelős: Balázsne Dr. Kail Eszter			Beosztás: egyetemi adjunktus			
Oktató(k): Balázsne Dr. Kail Eszter, Dr. Leitold Ferenc, Dr. habil Dineva Adrienn, Dobrovodsky Patrik						
Előtanulmányi feltételek:	NSXPP1HMLF	Programozási paradigmák és adatszerkezetek				
Számonkérés módja:	vizsga					
A tananyag						
Oktatási cél:	A kurzus célja, A hallgatók alapos áttekintést kapjanak a mesterséges intelligencia kiválasztott területeiről, valamint gyakorlati és módszertani ismereteket és készségeket szerezzenek a mesterséges intelligencia módszereinek és algoritmusainak alkalmazásával kapcsolatban.					
Tematika:	A kurzus bemutatja a gépi tanulás és a neurális hálózatok alapjait, valamint betekintést nyújt a kibervédelem különböző területeibe, ahol a mesterséges intelligencia alapú technikák alkalmazhatóak a hatékonyabb megoldások elérése érdekében. Kiemelt figyelmet kapnak a korszerű megközelítések, mint a megerősítéses tanulás, a nagyméretű nyelvi modellek (LLM) elleni támadások és védekezések, valamint a magyarázható mesterséges intelligencia (XAI).					

Féléves ütemezés	
Oktatási hét (konzultáció)	Témakör
1.	Általános bevezető a mesterséges intelligenciába
2.	Gépi tanulás alapjai I.
3.	Gépi tanulás alapjai II.
4.	Gépi tanulás alapjai III.
5.	Mesterséges intelligencia megoldások a kibervédelem területén
6.	Megerősítéses tanulás alapú kibervédelmi megoldások
7.	Malware detektálás és elemzés I.
8.	Malware detektálás és elemzés II.
9.	LLM elleni támadások és védekezések
10.	Értelmezhető AI (XAI) a kiberbiztonságban
11.	Rektori szünet
12.	Generatív AI és szintetikus adat a kiberbiztonságban
13.	Elméleti Zh, projektmunka beszámoló
14.	Elméleti pót ZH, projektbemutató
Félévközi követelmények	
Évközi jegy / aláírás megszerzésének feltételei:	Az aláírás feltétele a projektmunka sikeres bemutatása.
Zárthelyi dolgozatok	
Oktatási hét	Témakör

Az évközi jegy kialakításának módszere (csak évközi jegyes tárgyak esetében töltendő ki)			
-			
Pótlás módja			
A ZH / évközi jegy / aláírás pótlásának módja:	A HKR-ben előírtaknak megfelelően, a vizsgaidőszak első 10 munkanapjának valamelyikén az aláíráspótlás díj ellenében pótolható.		
Vizsga módja (csak vizsgás tantárgy esetében töltendő ki)			
Vizsgajegy kialakítása (csak vizsgás tantárgy esetében töltendő ki)			
Az egyes érdemjegyek ponthatárai:			
	Elérhető eredmény	Érdemjegy	
	0-50%	Elégtelen (1)	
	51-62%	Elégséges (2)	
	63-74%	Közepes (3)	
	75-86%	Jó (4)	
	87-100%	Jeles (5)	
Irodalom			
Kötelező:	Az Óbudai Egyetem Moodle rendszerébe feltöltött segédanyagok		
Ajánlott:	- 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 - Vhristoph Molnar: Interpretable Machine Learning: A guide for Making Black Box Models Explainable (2025), Third Edition		
Egyéb segédletek:			