

Kiberfizikai Rendszerek Intézet			Mintatanterv szerinti 3 félév 2026-27-1			
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, Dobrovodsky Patrik						
Előtanulmányi feltételek:	NSXPP1HMLF	Programozási paradigmák és adatszerkezetek				
Számonkérés módja:	vizsga					
A tananyag						
Oktatási cél:	A kurzus célja, hogy a hallgatók átfogó ismereteket szerezzenek a mesterséges intelligencia és a gépi tanulás alapvető módszereiről, valamint azok kibervédelmi alkalmazási lehetőségeiről. A hallgatók megismerkednek a korszerű AI-alapú kibervédelmi megoldásokkal, különös tekintettel az anomáliadetekcióra, a malware-elemzésre, a red teaming támogatására, valamint a generatív mesterséges intelligencia és a nagyméretű nyelvi modellek biztonsági vonatkozásaira. A kurzus célja továbbá, hogy a hallgatók gyakorlati készségeket szerezzenek a mesterséges intelligencia módszereinek alkalmazásában, értékelésében és biztonsági szempontú elemzésében.					
Tematika:	A kurzus áttekintést nyújt a mesterséges intelligencia, a gépi tanulás és a neurális hálózatok alapvető fogalmairól, valamint bemutatja azok alkalmazását a kibervédelem különböző területein. A hallgatók megismerkednek a klasszikus gépi tanulási algoritmusokkal és azok felhasználásával többek között anomáliadetekciós, és malware-detekciós feladatokban. A kurzus kiemelten foglalkozik a megerősítéses tanulás kibervédelmi alkalmazásaival, az AI-alapú red teaming megoldásokkal, a generatív mesterséges intelligencia és a nagyméretű nyelvi modellek (LLM-ek) működésével, valamint az ezekkel szembeni támadások és védekezési technikák vizsgálatával. A tantárgy továbbá bemutatja a magyarázható mesterséges intelligencia (XAI) szerepét a biztonsági döntéstámogatásban és az AI-rendszerek megbízhatóságának növelésében. A kurzus projektfeladatra épülő gyakorlati elemeket is tartalmaz, amelyek során a hallgatók valós kibervédelmi problémákon alkalmazhatják a megismert módszereket.					

Féléves ütemezés	
Oktatási hét (konzultáció)	Témakör
1.	Általános bevezető a mesterséges intelligenciába
2.	Gépi tanulás alapjai I. - Alapfogalmak
3.	Gépi tanulás alapjai II. – Klasszikus algoritmusok
4.	Gépi tanulás alapjai III. – Klasszikus algoritmusok
5.	Anomália detekció
6.	Megerősítéssel tanulás alapú kibervédelmi megoldások, Red Teaming
7.	Malware detektálás és elemzés
8.	Generatív AI, LLM
9.	ML és LLM elleni támadások és védekezések
10.	Értelmezhető AI (XAI) a kiberbiztonságban
11.	MI megoldások a kibervédelemben

12.	Rektori szünet		
13.	Projektmunka beszámoló		
14.	Projektmunka beszámoló		
Félévközi követelmények			
Évközi jegy / aláírás megszerzésének feltételei:		Az aláírás feltétele a projektmunka sikeres bemutatása.	
Zárthelyi dolgozatok			
Oktatási hét	Témakör		
13.	Projektmunka beszámoló		
14.	Projektmunka beszámoló		
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)			
Írásbeli vizsga			
Vizsgajegy kialakítása (csak vizsgás tantárgy esetében töltendő ki)			
Projektmunka és az írásbeli vizsga eredményeinek átlaga, de mindkettőből feltétel az elégséges jegy megszerzése.			
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:			