

|                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                               |                                             |    |     |     |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|---------------------------------------------|----|-----|-----|
| Kiberfizikai Rendszerek Intézet       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                               | Mintatanterv szerinti 3. félév<br>2026-27-1 |    |     |     |
| Tantárgy neve:                        | Kódja:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Kredit:                       | Óraszám                                     |    |     |     |
|                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                               |                                             | ea | tgy | lab |
| MLSecOps                              | NKXML1HMLF                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 5                             | levelező<br>féléves                         | 5  | 5   | 10  |
| Tárgyfelelős: Dr. habil. Fleiner Rita |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                               | Beosztás: egyetemi docens                   |    |     |     |
| Oktató(k): Dr. Fried Zoltán           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                               |                                             |    |     |     |
| Előtanulmányi feltételek:             | NKXKO1HMLF                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 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.                                                                                                                                                                                                                                                                                                                                      |                               |                                             |    |     |     |

| <b>Féléves ütemezés</b>       |                                                                    |
|-------------------------------|--------------------------------------------------------------------|
| Oktatási hét<br>(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: 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.                                                                                                                                                                                                                                                                                                                                                                           | Zárthelyi dolgozat, Projekt feladat beadása/bemutatása                                                                                                                                                                                                                                                                                                                                                                                                 |
| 14.                                                                                                                                                                                                                                                                                                                                                                           | Zárthelyi dolgozat pótlása, Projekt feladat bemutatása                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Félévközi követelmények</b>                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Évközi jegy / aláírás megszerzésének feltételei:                                                                                                                                                                                                                                                                                                                              | A sikeres évközi jegy feltétele, hogy mind a zárthelyi dolgozaton legalább 50%-os, a projektfeladaton legalább 60%-os eredményt érjen el a hallgató.                                                                                                                                                                                                                                                                                                   |
| <b>Zárthelyi dolgozatok</b>                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Oktatási hét</b>                                                                                                                                                                                                                                                                                                                                                           | <b>Témakör</b>                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>13.</b>                                                                                                                                                                                                                                                                                                                                                                    | Zárthelyi dolgozat: Előadás anyagai                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>14.</b>                                                                                                                                                                                                                                                                                                                                                                    | Zárthelyi dolgozat pótlása: Előadás anyagai                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Az évközi jegy kialakításának módszere</b> (csak évközi jegyes tárgyak esetében töltendő ki)                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <p>Az <b>évközi jegy</b> a zárthelyi dolgozat és a projektfeladat eredményének átlaga alapján számolandó.</p> <p>88% –: jeles (5)<br/> 77% –: jó (4)<br/> 66% –: közepes (3)<br/> 55% –: elégséges (2)<br/> 0% –: elégtelen (1)</p> <p>A projektfeladat leadásában a késés a késési idővel arányos, 10%/nap-ban mért levonást jelent a projektfeladat végső eredményéből.</p> |                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Pótlás módja</b>                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| A ZH / évközi jegy / aláírás pótlásának módja:                                                                                                                                                                                                                                                                                                                                | 14. héten vagy a vizsgaidőszak első hetében a zárthelyi dolgozat pótolható.                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Vizsga módja</b> (csak vizsgás tantárgy esetében töltendő ki)                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| -                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Vizsgajegy kialakítása</b> (csak vizsgás tantárgy esetében töltendő ki)                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| -                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Irodalom</b>                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Kötelező:                                                                                                                                                                                                                                                                                                                                                                     | <ul style="list-style-type: none"> <li>– Bell, L., Brunton-Spall, M., Smith, R., &amp; Bird, J. (2017). Agile application security: enabling security in a continuous delivery pipeline. " O'Reilly Media, Inc.". ISBN-13: 978-1491938843</li> <li>– Órai előadásokhoz kapcsolódó prezentációk, jegyzetek, anyagok a Moodle-ben</li> </ul>                                                                                                             |
| Ajánlott:                                                                                                                                                                                                                                                                                                                                                                     | <ul style="list-style-type: none"> <li>– 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</li> <li>– TREVEIL, Mark, et al. Introducing MLOps. O'Reilly Media, 2020. ISBN-13: 978-1492083290</li> <li>– Gift, Noah., Deza, Alfredo. Practical MLOps. N.p.: O'Reilly Media, 2021. ISBN-13. 978-1098103019</li> </ul> |
| Egyéb segédletek:                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                        |