ÓBUDAI EGYETEM
NEUMANN JÁNOS INFORMATIKAI KAR

| **Biomatika és Alkalmazott Mesterséges Intelligencia Intézet** | | | Mintatanterv szerinti 2. félév 2025-26-2 | | | |
|---|---|---|---|---|---|---|
| Tantárgy neve: | Kódja: | Kredit: | Óraszám | | | |
| | | | | ea | tgy | lab |
| **Informatikai rendszerek biztonságtechnikája** | NBXIB1HMNE | 5 | nappali heti | 2 | 0 | 2 |
| Tárgyfelelős: Dr. Póser Valéria | | | Beosztás: egyetemi docens | | | |
| Oktató(k): Dr. Póser Valéria, Prof. Dr. Ferenci Tamás | | | | | | |
| Előtanulmányi feltételek: | | | | | | |
| Számonkérés módja: | vizsga | | | | | |

| **A tananyag** | |
|---|---|
| Oktatási cél: | A tárgy keretében a hallgatók megismerkednek az informatikai rendszerek elemeinek sérülékenységeivel, azok biztonsági problémáival, védelmi módszerekkel, eszközökkel és gyakorlati alkalmazási lehetőségükkel. |
| Tematika: | Fontosabb témakörök: Az informatikai rendszerek elemei, sérülékenységei. Titkosítási alapfogalmak. Szimmetrikus, aszimmetrikus titkosítási módszerek. Hasító függvények. Blokkrejtjelezési módszerek, folyamtitkosítók. Üzenethitelesítés. Az operációs rendszerek biztonsági szolgáltatásai. Titkosítás, digitális aláírás gyakorlati megvalósításai. Biztonságos levelezés és adattárolás, kulcsmenedzselés, kulcsok hitelesítése, levelek titkosítása, digitális aláírása, visszafejtése. Hitelesítési problémák, jelszó alapú partnerhitelesítés. Felhasználók azonosítása, hitelesítése, engedélyezés, hozzáférés-vezérlés. Felhasználó-menedzsment. Biztonságos távoli munkavégzési technikák. Nyilvános kulcsú infrastruktúra, elemei és működése. Tanúsítványkezelés. Tűzfalak, behatolás detektálás, vírusvédelem, adatszivárgás elleni védelem, mentés és archiválás. |

| **Féléves ütemezés** | |
|---|---|
| Oktatási hét (konzultáció) | Témakör |
| 1. | Az informatikai rendszerek elemei, azokkal kapcsolatos sérülékenységek. Titkosítási alapfogalmak. Történelmi példák. |
| 2. | Szimmetrikus titkosítási módszerek. A DES, TripleDES algoritmus. AES (Rijndael ) algoritmus. |
| 3. | Aszimmetrikus titkosítási módszerek, előnyei hátrányai. RSA algoritmus. Prímszámkeresés, prímtesztek. |
| 4. | Hasító függvények. Születésnapi paradoxon. Diszkrét logaritmus. Hasító függvények jósága. MD4 MD5 SHA1 hasító függvények ismertetése és kritikai analízise. |
| 5. | Blokkrejtjelezési módszerek ECB, CBC, CFB, OFB és CTR mód. Folyamtitkosítók. |
| 6. | Az operációs rendszerek biztonsági szolgáltatásai. |
| 7. | SZÜNET |
| 8. | Titkosítás, hitelesítés, digitális aláírás gyakorlatban. Biztonságos levelezés és adattárolás lemezen (PGP).<br>Munkavégzés tartományban. |
| 9. | Felhasználó menedzsment. Felhasználók azonosítása, hitelesítése. Jelszavak problémái. |
| 10. | Biztonságos kommunikáció és fájlátvitel. |
| 11. | Nyilvános kulcsú infrastruktúra, elemei és működése. Tanúsítványkezelés |
| 12. | Adatmentés, adatvédelem. |
| 13. | ZH |
| 14. | Pótlás/javítás |

| **Félévközi követelmények** |
|---|

| | |
|---|---|
| Évközi jegy / aláírás megszerzésének feltételei: | Az aláírás feltétele egy elméleti kérdéseket és/vagy gyakorlati feladatokat tartalmazó zárthelyi sikeres (legalább elégséges) megírása.<br>Az előadások és laborgyakorlatok látogatása kötelező. |

**Zárthelyi dolgozatok**

| **Oktatási hét** | Témakör |
|---|---|
| **13.** | ZH |
| **14.** | Pótlás/javítás |

**Az *évközi jegy* kialakításának módszere** (csak évközi jegyes tárgyak esetében töltendő ki)

-

**Pótlás módja**

| | |
|---|---|
| A ZH / évközi jegy / aláírás pótlásának módja: | Az aláírás pótlásának módja: a vizsgaidőszak első 10 munkanapjának egyikére meghirdetett időpontban egy alkalommal. |

**Vizsga módja** (csak vizsgás tantárgy esetében töltendő ki)

szóbeli vizsga

**Vizsgajegy kialakítása** (csak vizsgás tantárgy esetében töltendő ki)

A vizsga érdemjegye a hallgató szóbeli teljesítménye és az évközi, elméleti és/vagy gyakorlati zárthelyi dolgozatának átlaga alapján kerül meghatározásra. A vizsga eredményének is el kell érnie az elégséges szintet.

**Az egyes érdemjegyek ponthatárai:**

| % | Az érdemjegy |
|---|---|
| 86-100 | jeles (5) |
| 74-85 | jó (4) |
| 62-73 | közepes (3) |
| 50-61 | elégséges (2) |
| 0-49 | elégtelen (1) |

**Irodalom**

| | |
|---|---|
| Kötelező: | • A Moodle rendszerben elhelyezett előadás és labor prezentációk |
| Ajánlott: | • Buttyán Levente, Vajda István: Kriptográfia és alkalmazásai, Typotex, 2012<br>• Szentgyörgyi Tibor – Filkor Csaba – Borbély Balázs: Modern munkakörnyezet építése Windows Server 2012 és Windows 8 és Office 365 alapokon, Jedlik Oktatási Stúdió Budapest, 2012 (elektronikus jegyzet)<br>• Gregg Kreizman: An Introduction to Information Security Architecture, Gartner The Future of IT Conference, 2011 (elektronikus jegyzet)<br>• Heys, Howard M.: "A tutorial on linear and differential cryptanalysis." Cryptologia 26.3, 189-221. 2002 (elektronikus jegyzet)<br>• John McCabe with the Windows Server team: Introducing Windows Server 2016, Microsoft Press, 2016<br>• Microsoft: Windows Server Security documentation, https://learn.microsoft.com/en-us/windows-server/security/security-and-assurance |
| Egyéb segédletek: | |