| **Óbudai Egyetem**Bánki Donát Gépész- és Biztonságtechnikai Mérnöki Kar | Biztonságtudományi és Kibervédelmi Intézet |
| --- | --- |
|  **Tantárgy címe és kódja: Információbiztonság IT-gyakorlata** *BBXIG16BNE* **Kreditérték*: 4****Nappali tagozat 2. tanév 2 . félév*  |
| Szakok melyeken a tárgyat oktatják: **Biztonságtechnikai mérnök szak** |
| Tantárgyfelelős oktató: | **Dr. Kollár Csaba** | Oktatók: | **Dr. Rajnai Zoltán** |
| Előtanulmányi feltételek (kóddal) | Informatika I. BBXIA11BNE |
| Heti óraszámok:  | Előadás: 1 | Tantermi gyak.: 1 | Laborgyakorlat:  | Konzultáció:  |
| Félévzárás módja:(követelmény) | **Vizsga**  |
| **A tananyag** |
| Oktatási cél: A hallgatók ismerjék meg azokat az információbiztonság IT-gyakorlatát. A tantárgy mélyrehatóan foglalkozik az információbiztonság kulcsfontosságú területeivel. A kurzus során hallgatóink megismerik a social engineering, OSINT, GDPR, valamint információbiztonsági rendeletek és szabványok kihívásait. Gyakorlati esettanulmányok és szimulációs gyakorlatok segítségével fejlesztjük a hallgatók képességeit az incidenskezelésben és a kockázatmenedzsmentben.  |
| Ütemezés: |
| Oktatási hét(konzultáció) | Témakör |
| 1. | Bevezető előadás, a félévi követelmények ismertetéseA biztonság alapelvei és szükségessége az informatikai környezetben |
| 2. | Alapfogalmak: támadás, védelem, kockázatJogszabályi háttér és felelősségek az információbiztonság területén |
| 3. | Social engineering alapelvek és technikák 1.Támadói profilok és motivációk |
| 4. | Social engineering alapelvek és technikák 2.Ellenintézkedések és prevenció a social engineering ellen |
| 5. | OSINT alapelvek és gyakorlati alkalmazások |
| 6. | Nyilvános források és azok kihasználásaAdatgyűjtés és elemzés a védelmi szempontból |
| 7. | Beszámoló a féléves komplex feladat haladásából |
| 8. | Az emberi tényező szerepe az információbiztonságbanFelhasználói oktatás és tudatosság fejlesztésHumán erőforrás ellenőrzési mechanizmusok |
| 9. | Mutatószámok és teljesítménymérők az információbiztonság területénGDPR alapelvek és követelményekGDPR-ba való illeszkedés és az adatvédelem fontossága |
| 10. | Nemzetközi és iparági információbiztonsági szabványok áttekintéseRendeletek és irányelvek értelmezése és betartásaBiztonsági auditok és azok folyamatai |
| 11. | Kockázatok az informatikai környezetbenKockázatértékelés és kockázatkezelési stratégiákKockázatmenedzsment eszközök és módszerek |
| 12. | Szimulációs gyakorlat |
| 13. | Konzultáció a féléves komplex feladat beadása előtt |
| 14. | A kiscsoportok komplex feladatainak prezentálása, A félév értékelése, zárása |
| **Félévközi követelmények** *(feladat, zh. dolgozat, esszé, stb)* |
| Oktatási hét(konzultáció) | A 7. héten a féléves komplex feladat haladásából beszámoló. A 14. héten a komplex feladat bemutatása. |
|  | 1 db. kiscsoportos hallgató előadás1 db. kiscsoportos komplex feladataktív részvétel a szimulációs gyakorlaton |
| *Az értékelés, a lebonyolítás, a pótlás módja, a jegy kialakításának szempontjai* |
| A foglalkozásokon való részvételt a TVSZ III.23.§ (1)-(4) pontja szabályozza. Az aláírás megszerzésének feltétele az évközi feladatok legalább elégséges szintre való teljesítése. Az aláírás szorgalmi időszakon túli pótlásának módjáról a Tanulmányi Ügyrend III.6.1.(3)/III.6.2.(3) pontja rendelkezik.Valamennyi, jelen dokumentumban nem szabályozott, kérdésben az Óbudai Egyetem Tanulmányi és Vizsgaszabályzata valamint Tanulmányi Ügyrendjének rendelkezései az irányadók.**Az előadásokon a megjelenés kötelező. Aki az előadások több, mint 30%-án hiányzott, aláírást nem kap és nem is pótolhatja.** |
| **A félévzárás módja** *(vizsga módja: írásbeli, szóbeli, teszt, stb.)* |
| A félév elején kiadott kiscsoportos, komplex feladat időben történő elkészítése és beadása. Az aláírás feltétele a kiscsoportos hallgatói előadás, illetve a komplex feladatból készített prezentáció. A félévi jegy 25%-ban a kiselőadásból, 25%-ban a komplex feladat prezentációjából, 50%-ban pedig a komplex feladat írásos változatának értékeléséből tevődik össze.  |
| **Kötelező irodalom**: 1. Az oktató által készített, a hallgatók rendelkezésére bocsátott elektronikus jegyzet
2. Kollár, Csaba: Az információbiztonság humán aspektusai: A biztonságtudatossági ellenőrzés során alkalmazott social engineering technikák elemzése a SPEAKING modell segítségével. BELÜGYI SZEMLE: A BELÜGYMINISZTÉRIUM SZAKMAI TUDOMÁNYOS FOLYÓIRATA (2010-)<https://ojs.mtak.hu/index.php/belugyiszemle/article/view/4333/3343>
 |
| **Ajánlott irodalom:**1. Kollár, Csaba ; Zakar, Ákos: A social engineering és a manipulációs technikák és módszerek - kutatási jelentés. BIZTONSÁGTUDOMÁNYI SZEMLE 2 : 3 pp. 31-46. , 16 p. (2020)

https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/70/621. Kollár, Csaba ; Zakar, Ákos: A social engineering és a manipulációs technikák és módszerek. BIZTONSÁGTUDOMÁNYI SZEMLE 2 : 2 pp. 23-38. , 16 p. (2020)

https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/58/50 1. David J. Wetherall Andrew S. Tanenbaum: Számítógép-hálózatok. Panem Kft. 2013.
2. Jim Geier: Vezeték nélküli hálózatok. Panem Kft. 2005.
3. Hétpecsét Egyesület kiadványai (Hétpecsétes történetek) itt találhatók:<https://hetpecset.hu/site/>
 |
| **Egyéb segédletek:**  |
|  |
| **A tárgy minőségbiztosítási módszerei:** |

 ……………………………… ……………………………

 tantárgyfelelős dékán