|  |  |
| --- | --- |
| Óbudai EgyetemBánki Donát Gépész és Biztonságtechnikai Mérnöki Kar | Az oktatást végző kar/szervezeti egység:BGK/ Biztonságtudományi és Kibervédelmi Intézet |
| **Tantárgy neve és kódja: Információbiztonsági kockázatok IT támogatással (BBXIT16BNE)**, Kreditérték**: 2****Nappali 2022/2023 tanév 2. félév** |
| *Szakok, amelyeken a tárgyat oktatják:* **Biztonságtechnikai Mérnök Bsc.**  | Ea: lásd ÜtemezésGy: lásd Ütemezés |
| *Tantárgyfelelős oktató:* | **Prof. Dr. Michelberger Pál** | *Oktatók:* | **Prof. Dr. Michelberger Pál**  |
| Előtanulmányi feltételek:(kóddal) | nincs |
| Heti óraszámok: | Előadás: **2** | Tantermi gyak.: **0** | Laborgyakorlat: **0** | Konzultáció: 0 |
| *Számonkérés módja* (s,v,f): | félévközi jegy |
| **A tananyag** |
| *Oktatási cél:* A továbbiakban részletezett területek megismerése és a kockázatkezelő eszközök, technikák, alkalmazások elsajátítása. Kockázatmenedzsment tárgya és célja az információbiztonságban. Kockázatelemzési módszerek és alkalmazásuk. A CRAMM módszer sajátosságai. Védendő adatvagyon elemei, kategóriái. Felelősségek és az adatvagyon sebezhetőségei. Konfiguráció- és portfolió menedzsment. Információbiztonsági kockázatok fajtái, felvétele, elemzése és értékelése. A kockázatkezelés gyakorlata. IT eszközök szerepe a kockázatkezelésben.   |
| *Tematika: lásd ütemezés* |
| **Ütemezés:** |
| *Okt. hét (konzult.)* | *Az előadások témakörei* |
| 1 |   | Tantárgyi tematika és követelmények ismertetése |
| 2 |  | Információbiztonsági kockázatmenedzsmenttel foglalkozó szabványok és ajánlások áttekintése (ISO 31000, ISO/IEC 27005, CRAMM módszer, MIL-STD-882-E) |
| 3 |  | Információbiztonsági kockázatok strukturálása és értékelése, folyamatos kockázatkezelés és elemzés |
| 4 |  | IT alkalmazások és eszközök nyilvántartása és védelme (ITIL, ill. ISO/IEC 20000 alapján) |
| 5 |  | Információbiztonsági irányítási rendszer IT támogatása. Új védelmi intézkedések kidolgozása és megvalósítása (szoftver- és hardverbeszerzés információvédelmi szempontjai)  |
| 6 |  | Emberi tényezők az információbiztonságban (belépés, titoktartás, felhasználói tudatosság, kilépés, áthelyezés, képzés) |
| 7 |  | Fizikai és környezeti biztonság (infrastruktúra, közművek) |
| 8 |  | Papíralapú dokumentumok információvédelme |
| 9 |  | IT eszközök, szoftverek átvétele, mobil eszközök tudatos felhasználása, adathordozók azonosítása, szállítása, használata, megsemmisítése  |
| 10 |  | Hálózatok igénybevétele, felhasználók monitorozása, SIEM rendszerek |
| 11 |  | zárthelyi  |
| 12 |  | Konzultáció és / vagy pótzárthelyi |
| 13 |  | Évközi hallgatói beszámoló és prezentáció a kiadott feladatról |
| 14 |  | Félév zárása |

|  |
| --- |
| **Félévközi követelmények** *(feladat, zh., jegyzőkönyv stb.)* |
| Oktatási hét | A gyakorlatok legfontosabb témakörei: jegyzőkönyvek, feladatok |
| 11.  | zárthelyi megírása |
| 12. vagy 13. | Csoportos feladatmegoldások leadása |
| 13. vagy 14.  | Csoportos prezentáció megtartása  |
| *A pótlás módja: lásd a tárgy tanulmányi és vizsgakövetelményei, valamint a HKR rendelkezései* |
| **Hiányzás szabályozása:****HKR 46. §** **(3) Amennyiben a hallgató hiányzásai valamely kötelezően látogatandó tárgyból meghaladják a tárgy félévi óraszámának 30%-át, a hallgató aláírást, illetve évközi jegyet nem kaphat.****(2) A jelenlét ellenőrzésének formáját és a hiányzások igazolásának módját a Tanulmányi Ügyrend tartalmazza.****Az évközi jegy megszerzésének és az aláírás feltételei:*** Részvétel a foglalkozásokon
* A csoportos beadandó anyag elkészítése és prezentáció megtartása
* A zárthelyi / pótzárthelyi eredményes megírása

A kifejtős kérdéseket tartalmazó zárthelyi értékelése: 0 – 49,99%: elégtelen (1) 50 – 59,99%: elégséges (2) 60– 69,99%: közepes (3) 70 – 79,99%: jó (4)80 – 100%: jeles (5)Elégtelen zárthelyi esetén pótzárthelyi írható. Az aláírás feltétele a legalább elégséges zárthelyi/pótzárthelyi megírása. Az aláírást a vizsgaidőszak első 10 napjáig – aláíráspótló vizsga jelleggel - még pótolni *lehet*. A sikertelen pótlás az aláírás **végleges** megtagadását vonja maga után**.**Alakítsanak 2-3 fős csoportokat.! Vizsgálják meg és értékeljék egy-egy vállalati IT rendszerelem (operációs rendszer, adatbáziskezelő, alkalmazás, hardver eszköz, szerver, hálózati elem, periféria) „beépített” kockázati szintet mérséklő megoldásait, ill. azok kihasználtságát! Tegyenek javaslatot a jobb - költséghatékony és kockázati szintet minimalizáló - felhasználásra. Készítsenek egy 15-20 perces prezentációt a félév végéig az elvégzett munkáról!A prezentációkat a többi csoport is értékeli (1-5-ig). Ezekből számtani átlagot számolunk…A hallgatók végleges évközi jegyét a zárthelyin elért eredmény és a csoport prezentációra kapott jegyből határozzuk meg. A zh. kétszeres, a prezentáció egyszeres súllyal esik latba. **A számonkérés módja:** évközi jegy |
| **Irodalom:** |
| Michelberger Pál: Információ-, folyamat- és vállalatbiztonság. ÓE-KGK-4086, 2022. 3. kiadásHorváth Zsolt László: Integrált vállalati kockázatkezelés. ÓE-KVK, 2015Abonyi János – Fülep Tímea: Biztonságkritikus rendszerek. Pannon Egyetem, 2014 <https://www.tankonyvtar.hu/hu/tartalom/tamop412A/2011-0042_biztonsagkritikus_rendszerek/adatok.html>  |