|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Óbudai EgyetemBánki Donát Gépész és Biztonságtechnikai Mérnöki Kar | | | | | | | | | | | | | | | | | Biztonságtudományi és Kiberbiztonsági Intézet | | | | | | | | | | | |
| **Tantárgy címe és kódja:** | | | | | | | | **Információbiztonsági kockázatok kezelése IT-támogatással BBXIK16BNF** | | | | | | | | | | | | | | | | **Kreditérték:** | | | | 4 |
| Nappali munkarend | | | | |  | | | | | | tanév | | |  | | félév | | | | | | | | | | | | |
| **Szakok melyeken a tárgyat oktatják:** | | | | | | | | | | | | Biztonságtechnikai mérnök BSc. | | | | | | | | | | | | | | | | |
| **Tantárgyfelelős oktató:** | | | | | | | Prof. Dr. Michelberger Pál | | | | | | | | | | | **Oktatók:** | Prof. Dr. Michelberger Pál | | | | | | | | | |
| **Előtanulmányi feltételek (kóddal):** | | | | | | | | | | | | | - | | | | | | | | | | | | | | | |
| **Heti óraszámok** | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Előadás: | 2 | | | | | Tantermi gyak.: | | | | | | | 0 | | | | Laborgyakorlat: | | | | | 2 | Konzultáció: | | | |  | |
| **Félévzárás módja:** | | | | | | Évközi jegy | | | | (Írásbeli és szóbeli) | | | | | | | | | | | | | | | | | | |
| ***Online konzultáció*** *(amennyiben szükséges):* | | | | | | | | | | | | | | | *… (BBB link)* | | | | | | | | | | | | | |
| **Oktatási cél**: | | | Kockázatmenedzsment az információbiztonságban. Kockázatelemzési módszerek és alkalmazásuk. CRAMM módszer sajátosságai. Védendő adat- és információvagyon elemei. Sebezhetőségek. Konfiguráció- portfolió menedzsment. Szoftver- és hardverbeszerzés információvédelmi szempontjai. IT eszközök a kockázatkezelésben. Felhasználók monitorozása. Tűzfal menedzselés. Automatikus napló- és log elemzés (adathozzáférések monitorozása). Belső sérülékenység vizsgálat (hálózaton belüli eszközök felderítése, osztályozása, kockázat értékelés…). Internetes alkalmazások automatikus biztonsági ellenőrzése Wi-Fi biztonság ellenőrzése. Hálózati hozzáférés ellenőrzése (felhasználói hitelesítés, illetéktelen hozzáférési végpontok kizárása). Behatolás jelzés. Érzékeny adatok kiemelt kezelése. SIEM (Security Information and Event Management) rendszerek. | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Ütemezés** | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Oktatási hét | | **Témakörök** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1. | | Kockázatmenedzsment és információbiztonság (információbiztonsági kockázatok strukturálása és értékelése, folyamatos kockázatkezelés és elemzés) | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2. | | Védendő adat- és információ vagyon | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3. | | Sebezhetőségek | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4. | | Konfiguráció és portfolió menedzsment | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 5. | | Szoftver- és hardverbeszerzés információvédelmi szempontjai | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 6. | | IT eszközök a kockázatkezelésben (felhasználók monitorozása, tűzfal-menedzselés, automatikus napló- és log elemzés, belső sérülékenység vizsgálat) | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 7. | | Internetes alkalmazások automatikus biztonsági ellenőrzése, Wi-Fi biztonság ellenőrzése | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 8. | | Hálózati hozzáférés ellenőrzése (felhasználói hitelesítés, illetéktelen hozzáférési végpontok kizárása). | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 9. | | Érzékeny adatok kiemelt kezelése | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 10. | | Információbiztonsági irányítási rendszer IT támogatása | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 11. | | Emberi tényezők az információbiztonságban (belépés, titoktartás, felhasználói tudatosság, kilépés, áthelyezés, képzés), fizikai és környezeti biztonság (infrastruktúra, közművek) | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 12. | | SIEM (Security Information and Event Management) rendszerek | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 13. | | Integrált GRC (Governance – Risk Managememt – Compilance) rendszerek + zárthelyi | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 14. | | Csoportos beszámolók | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Félévközi követelmények** | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Zárthelyi dolgozat | | | | | | | | | Csoportos beadandó feladat | | | | | | | | | | | | Labormérés | | | | | | | |
| száma | | | | időpontok | | | | | száma | | | | | | | | határidők | | | | száma | | | | időpontok | | | |
| 1 db | | | | 13 | | | | | 1db | | | | | | | | 13.hét | | | | db | | | |  | | | |
| **Az értékelés, a lebonyolítás, a pótlás módja, a jegy kialakításának szempontjai**  *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*  *Értékelés:* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| A szabályzatokban nem szabályozott foglalkozásokon való egyéb részvételi követelmények, és megkötések a pótlásokra vonatkozóan: | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Minden csoportos részfeladatot a választott csoportvezetőnek fel kell tölteni az egyetemi Moodle rendszerbe. A csoportos részfeladatok 1-5-ig osztályozásra / pontozásra kerülnek. A záró csoportos prezentációt a 14. héten meg kell tartani a csoportoknak.  A pótlás módja (HKr 45. §, 46. §)  A félév során az elmaradó (késve beadott) részfeladat a vizsgaidőszak első hetéig pótolható évközi jegypótló vizsga keretében. A késés az értekelés során adott pontszámban / osztályzatban figyelembevételre kerül. Pótzárthelyi a 14. héten nem órarendi időpontban kerül meghírdetésre.  Aláírás pótlása vizsgaidőszakban: A megtagadott aláírást a vizsgaidőszak első 10 munkanapja során egy alkalommal lehet pótolni az évközi pótlás feltételeinek megfelelően. | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Zárthelyi dolgozat** | | | | | | | | | **Beadandó csoportos feladat** | | | | | | | | | | | Labormérés | | | | | | | | |
| elérhető max pontszám | | | | minimum pontszám a teljesítéshez/zh(kapott osztályzat kétszerese) | | | | | elérhető max pontszám | | | | | | | | | minimum pontszám a teljesítéshez/ feladat | | elérhető max pontszám | | | | | | minimum pontszám a teljesítéshez/mérés | | |
| 10…pont | | | | 4…pont | | | | | …5pont | | | | | | | | | 2…pont | | …pont | | | | | | …pont | | |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **A szemeszterben megszerezhető összes pontszám:** | | | | | | | …15pont | | |
| **Ponthatárok** | **elégséges**  6… ponttól | | | | **közepes**  9… ponttól | | | **jó**  11… ponttól | **jeles**  13… ponttól |
| Egyéb értékelési szempontok: A zh-nak és a csoportos beadandó feladatnak legalább elégséges (2) osztályzatot / pontot el kell érnie. | | | | | | | | | |
|  | | | | | | | | | |
| **Letiltva bejegyzést kap:** | | | |  | | | | | |
| **Kötelező irodalom:** | | | Horváth Zsolt László: Integrált vállalati kockázatkezelés. Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar, 2015. | | | | | | |
| **Ajánlott irodalom:** | | Abonyi János – Fülep Tímea: Biztonságkritikus rendszerek. Pannon Egyetem, 2014. <https://www.tankonyvtar.hu/hu/tartalom/tamop412A/2011-0042_biztonsagkritikus_rendszerek/adatok.html>  Michelberger Pál: Információ-, folyamat- és vállalatbiztonság. Óbudai Egyetem, ÓE-KGK-4086, Budapest, 2022. | | | | | | | |
| **A tárgy minőségbiztosítási módszerei:** | | | | | |  | | | |

Kelt: Budapest, 2023. 06. 15.

Szöveg beírásához kattintson vagy koppintson ide.

………………………………………………………

Szöveg beírásához kattintson vagy koppintson ide.