Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar	**Gépészeti és Biztonságtudományi Intézet**

Tantárgy neve és kódja: **Információbiztonsági Irányítási Rendszer alapjai** ***BGBII1VNND***
nappali tagozat **Kreditérték: 2**

Szakok melyeken a tárgyat oktatják: **minden karon, minden szakon, szabadon választható tárgyként**

Tantárgyfelelős oktató:	**Dr. Horváth Zsolt László**	Oktatók:	**Dr. Horváth Zsolt László**

Előtanulmányi feltételek: (kóddal)	**---**

Heti óraszámok:	Előadás: **2**	Tantermi gyak.: **0**	Laborgyakorlat: **0**	Konzultáció:

Számonkérés módja (s,v,f):	**Évközi jegy – írásbeli ZH (egyszerű feleletválasztós tesztkérdések, elégséges szintje 60 %)**

A tananyag

Oktatási cél: **Az információbiztonság és az információbiztonsági irányítási rendszer fogalmáról, céljáról, jelentőségéről, területei és működtetési követelményeiről egy részletes áttekintés nyújtása.**

Témakör:	**Óraszám:**	
Bevezetés az információbiztonságba (az információbiztonság fogalma, jelentősége, adathordozók fajtái, az információvédelem célja és jellemzői, az információvédelem megvalósításának 5 szakmai területe, rövid jellemzésük)	**1.**	**2**
Az IBIR, mint menedzsmentrendszer jellemzése (menedzsmentrendszer fogalma és jellemzése, menedzsmentrendszerek közös elemei, PDCA, az IBIR bevezetésének lépései, az IBIR működtetése, ellenőrzése és fejlesztése, az információbiztonság szervezete – szerepek, feladatok, felelősségek, fórumok, az IBIR dokumentációja és azok funkciói)	**2.**	**2**
Megfelelés a jogszabályi követelményeknek (információbiztonsággal kapcsolatos főbb jogszabályok áttekintése, közokiratok, közlevéltárak iratai védelme, közérdekű adatok nyilvánossága, személyes adatok védelme, üzleti titok védelme, nemzeti minősített adat védelme, … és a büntetések tarifái)	**3.**	**2**
A védendő vagyon meghatározása és kezelési követelményei (védendő vagyon fogalma, kategóriái, lehetséges fenyegetéseik bemutatása, vagyonelemek feltérképezési módjai, az információbiztonsági kockázatok elemzési módjai, módszerei, a kockázatelemzés alapvető lépései, bekövetkezési valószínűség és kárérték becslések, kockázati értékek meghatározása, kockázatok kezelése, kockázatkezelés folyamatossága)	**4.**	**2**
A terület és objektum-védelem (célja az információbiztonságban, funkciói, alkalmazott területei, biztonsági zónák kialakításának szempontjai, beléptetés ellenőrzésének követelményei, behatolás elleni védelem követelményei, mozgás ellenőrző eszközök követelményei)	**5.**	**2**
A személyvédelem és a humán biztonság (a személyvédelem célja, az emberi tényezőből fakadó kockázatok, a Social Engineering fogalma, célja, eszköztára, a Social Engineering támadás fázisai, védekezési módszerek, a személyügyi munka (HR) IB aspektusai – HR szempontok előzetes átvilágításhoz, szerződéskötéshez, belső tudatosító képzéshez, kockázati tényezők észleléséhez, munkaköri változások és megszűnések kezeléséhez)	**6.**	**2**
Dokumentumok, iratok védelme (iratkezelés fogalma és életciklusa, papíralapú és elektronikus formátumú iratok, iratok osztályozásának irányelvei, iratkezelési osztályoknak megfelelő eljárásrendek kialakítása, alkalmazási irányelvek, példák)	**7.**	**2**
Az informatikai fizikai biztonság (IT üzemeltetéssel szembeni elvárások, berendezések elhelyezése és védelme, rendszerüzem védelme, karbantartás, selejtezés és újrafelhasználás, vagyonelemek eltávolítása, berendezések telephelyen kívüli védelme, őrizetlenül hagyott felhasználói berendezések)	**8.**	**2**

Az informatikai üzemeltetés és kommunikáció biztonsága (IT üzemeltetés szabályozása, üzemelő szoftverek felügyelete, műszaki sebezhetőségek kezelése, védelem rosszindulatú szoftverek ellen, naplózás, monitoring, mentések, titkosítások alkalmazása, jogosultságok / hozzáférési rend kialakítása, üzemeltetése és felügyelete, hálózatbiztonság, információ átvitele)	**9.**	**2**
Információs rendszerek biztonsági követelményei (információs rendszerek biztonsági követelményei (követelmények elemzése, meghatározása), nyilvános hálózatokon nyújtott alkalmazás-szolgáltatások biztonsága, az alkalmazás-szolgáltatások tranzakcióinak védelme , biztonság a szoftver-fejlesztési és -támogatási folyamatokban, tesztadatok védelme)	**10.**	**2**
Incidenskezelés és üzletmenet-folytonossági követelmények (az IS-incidens fogalma, példák, az IS-incidens folyamata, tanulás az IS incidensekből, BCP és DRP fogalma, értelmezése, BCP/DRP típusai (felhasználói és informatikai megközelítések), BCP/DRP lépései)	**11.**	**2**
A dolgozókra vonatkozó biztonsági szabályok (biztonság betartása munkahelyen (céges infrastruktúra elemek használatának biztonsági irányelvei), munkahelyen kívüli biztonság, külső szereplőkkel való együttműködés, biztonsági események esetén)	**12.**	**2**
Összefoglalás **Sikertelen tesztdolgozatok pótlása**	**13.**	**2**
--- (rektori szünet hét) ----	**14.**	---

Félévközi követelmények

Nappali: A hallgatók a félév során 3 alkalommal írásbeli tesztdolgozatot írnak, aminek eredménye alkotja az évközi jegyet. Az írásbeli dolgozatok az adott anyagrészhez kapcsolódó rövid tesztdolgozatok, amelyek teljesítési feltétele dolgozatonként a 60 – 60 %. (Ha a dolgozatok közül mindhárom sikertelen, akkor a hallgató nem teljesítette a félév követelményeit, a Neptun rendszerben letiltásra kerül. Ha egy vagy kettő sikertelen, akkor azok egy alkalommal, az utolsó órán pótolhatók.)

Irodalom:

Kötelező:

- Dr. Horváth Zsolt László: Az információbiztonsági irányítási rendszer alapjai c. jegyzet

Ajánlott:

- MSZ ISO/IEC 27001:2014 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények
- ISO/IEC 27002:2013 Information technology — Security techniques. Code of practice for information security management