Óbudai Egyetem **Alba Regia Műszaki Kar**				
Tantárgy neve és kódja: Informatikai biztonság (AMEIB1IBNE) **Kreditérték: 4** Nappali tagozat 2023/24. tanév 2. félév				
Szakok, melyeken a tárgyat oktatják: Mérnökinformatikus alapszak (BSc)				
Tantárgyfelelős oktató:	Dr. Póser Valéria PhD	Oktató:	Lukács Balázs	
Előtanulmányi feltételek: (kóddal)				
Heti óraszámok:	Előadás: 2	Tantermi gyak.: 0	Laborgyakorlat: 2	Konzultáció: -
Számonkérés módja:	vizsga			

A tananyag

Oktatási cél: Az információ fogalomköre, továbbítása és tárolása és ezek során az információt fenyegető sérülések, támadások, valamint betekintés az információ-védelem módszereibe. A hallgatók gyakorlati felkészítése e problémakör identifikációjára és a még kezelhető módszerek elsajátítására Cél a gyakorlati módszerek elméleti alapjainak a megtanítása is.
Gyakorlatok: Az informatikai biztonság alapjai tárgy keretében megismert informatikai biztonsággal kapcsolatos problémák gyakorlati megismerése és kezelése.

Tematika:

Témakör	Óraszám
Előadások:	
1. Az információ és fogalomköre. Az informatikai biztonság tárgya, eszközei, módszerei.	2
2. Az informatikai biztonság összetevői, aspektusai.	2
3. Az informatikai biztonság alapmodelljei.	2
4. Biztonsági rendszerek tervezése, alapfogalmak A rendszer elemei, a védelem tervezése, eszköztára, módszerei A megbízható informatikai rendszer funkciói Állandó fenyegetettség és védekezés.	2
5. Védelmi szabványok.	2
6. 1. Zárthelyi dolgozat.	2
7. Kriptográfia, szükségessége, eredete, fejlődése Kriptográfia célja, eszközei napjainkban.	2
8. Kriptográfia, szükségessége, eredete, fejlődése Kriptográfia célja, eszközei napjainkban.	2
9. A kriptográfia elemei, kriptogenerációk, protokollok. A kriptográfia 2. generációja, asszimetrikus titkosítás.	2
10. A kriptográfia elemei, kriptogenerációk, protokollok. A kriptográfia 2. generációja, asszimetrikus titkosítás.	2
11. Kriptográfiai technikák és a szimmetrikus titkosítás.	2
12. Kulcsmenedzsment, Alkalmazások, kriptográfia szolgáltatásai.	2
13. 2. Zárthelyi dolgozat.	2
14. Pótlások.	2

Gyakorlatok:	
Az informatikai biztonság fontossága, társadalmi beágyazottsága. Az információbiztonsági alapfogalmak, alapelvek, ökölszabályok.	2
Bizalmasság, Sértetlenség, Rendelkezésre állás = Confidentiality, Integrity, Availability (CIA). A CIA és a védelmi kontrollok.	2
Információbiztonsági szerepek, szervezeti feltételrendszer. Kölcsönösen egymást kizáró szerepek. Kockázatértékelés, kockázatkezelés. Példák.	2
Az üzletmenet folytonosság alapjai. Alapfogalmak. Az üzletmenet folytonossági -, katasztrófa elhárítási-, helyreállítási terve. PDCA elv (Plan-Do-Check-Act ciklusok). ISMS (Information Security Management System) kialakítása, működtetése.	2
Szabvány alapú információbiztonság (ITIL,COBIT,ISO 27000). Nemzetközi követelmény-rendszer (HIPPA, PCI DSS, GLBA, BÁZEL II-III, SOX/SOA).	2
Zárthelyi dolgozat. Social Engineering – emberi sebezhetőség.	2
Fenyegetettségek, a védelem feladata, eszközei. A leggyengébb láncszem, különféle szerepek. Fizikai biztonság kialakítása, szervezete. Azonosítási technikák, elektronikus dokumentumok védelme.	2
Kriptográfia (ismétlés), kriptogenerációk. Nyílt szövegek titkosítása. Történelmi áttekintés: kódolási technikák. A kriptográfia alapvető szolgáltatásai. Titkosító kulcsok, algoritmusok.	2
Harmadik generációs módszerek (A XX. század elejétől a XX. század második feléig). Elektromechanikus módszerek (Enigma, Purple). Több ABC használata, Navaho kódolás.	2
Kriptográfiai protokollok. Matematikai alapok. Alkalmazott transzformációk, Stream cipher, kulcsfolyam, keverések. Példák.	2
Elektronikus levelek. Felépítésük, kézbesítésük, kockázatok. SSH/SSL alkalmazása. Elektronikus titkosítások.	2
Zárthelyi dolgozat. Elektronikus titkosítások.	2
Pótlás, javítás.	2

Félévközi követelmények	
Az előadások és a gyakorlatok látogatása kötelező. 2 db nagy zárthelyi van betervezve (6. és 13. hét). Az eredmény a zárhelyi dolgozatok érdemjegyének számtani átlaga. Az aláíráshoz az elégséges szint a maximálisan elérhető pontérték 50%-a. Pótlás: Utolsó alkalmat az elmaradások pótlására tartjuk fenn.	
Aláírás feltétele:	Az előadások és laborgyakorlatok rendszeres látogatása és az előadásokkal kapcsolatos számonkérés félévközi eredménye (vagy a pótlása) eléri el a 50%-ot.
A vizsga módja:	Írásbeli, 50 % az elégséges szint, nem egyértelműség esetén szóbeli vizsga.

Irodalom:	
Kötelező:	Az egyetem e-learning rendszerébe (folyamatosan) e tárgyhoz feltöltött valamennyi elektronikus tananyag (mind az előadások prezentációi, mind az elektronikus jegyzetek) rendszeres, előadásról-előadásra való figyelése, elolvasása és megtanulása.

Ajánlott:	1. Virasztó Tamás: Titkosítás és adatrejtés, NetAcademia Kft. 2004t, ISBN 963 214 253 5. 2. Dr. Berta István Zsolt: Nagy e-szignó könyv, Microsec Kft. 2011, ISBN 978 963 08 1168 2 (Ez a könyv és egyes részei is internetről is letölthetők.) 3. Niels Ferguson & Bruce Schneier: Practical Cryptography, Wiley Publishing Inc. 2003. ISBN 0-471-22357-3 (Paperback) NAGYON JÓ! 4. Nagy Sándor: Elektronikus leveleink védelme, Computerbooks, 2005. 5. Himansu Dwivedi: SSH a gyakorlatban,Kiskapu, 2004. 6. Tom Thomas: Hálózati biztonság, Panem Kft. 2005. 7. Buttyán Levente-Vajda István :Kriptográfia és alkalmazásai, Typotex Kiadó, 2004. Opcionális szakirodalmat és linkeket találhat e tárgy e-learning webkikötőjén is.