Óbudai Egyetem	**Alba Regia Egyetemi Központ**

Tantárgy neve és kódja: Az információbiztonság alapjai NRKIB0SSND Kreditérték: 4
Nappali tagozat 2014/2015. tanév 2. félév

Szakok, melyeken a tárgyat oktatják: mérnök informatikus alapszak				
Tantárgyfelelős oktató:	Dr. Hermann Gyula	Oktató:	Lukács Balázs	
Előtanulmányi feltételek: (kóddal)		NRKIB1SSNC	Az informatikai biztonság alapjai I.	
Heti óraszám: 2	Előadás: 0	Tantermi gyak.: 0	Laborgyakorlat: 2	Konzultáció: 0
Számonkérés módja (s,v,f):		évközi jegy		

A tananyag

Oktatási cél: Az informatikai biztonság alapjai I. tárgy keretében megismert informatikai biztonsággal kapcsolatos problémák gyakorlati megismerése és kiegészítése további módszerekkel.

Laboratóriumi gyakorlatok	**Óraszám**
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

6. és 13. hét	Zárthelyi dolgozat

A laboratóriumi gyakorlatok látogatása kötelező. Az évközi jegy a két zárthelyi érdemjegyének számtani átlaga alapján kerül megállapításra, nem egyértelműség esetén szóbeli felmérés után.

Ajánlott irodalom

Nagy Sándor: Elektronikus leveleink védelme, Computerbooks, 2005

Himansu Dwivedi: SSH a gyakorlatban,Kiskapu, 2004

Tom Thomas: Hálózati biztonság, Panem Kft. 2005

Buttyán Levente-Vajda István :Kriptográfia és alkalmazásai, Typotex Kiadó, 2004

Székesfehérvár, 2015. február 1. …….

Lukács Balázs