A TANTÁRGY ADATLAPJA

1. A képzési program adatai

1.1 Felsőoktatási intézmény	**Babeș-Bolyai Tudományegyetem**
1.2 Kar	**Matematika és Informatika**
1.3 Intézet	**Magyar Matematika és Informatika**
1.4 Szakterület	**Informatika**
1.5 Képzési szint	**Alapképzés**
1.6 Szak / Képesítés	**Informatika**

2. A tantárgy adatai

2.1 A tantárgy neve		**IT biztonság**					
2.2 Az előadásért felelős tanár neve				**Dr. Kolumbán Sándor egyetemi adjunktus**			
2.3 A szemináriumért felelős tanár neve				**Dr. Kolumbán Sándor egyetemi adjunktus**			
2.4 Tanulmányi év	**3**	2.5 Félév	**6**	2.6. Értékelés módja	**Vizsga**	2.7 Tantárgy típusa	**Opcionális**
2.8 A tantárgy kódja		**MLM5255**					

3. Teljes becsült idő (az oktatási tevékenység féléves óraszáma)

3.1 Heti óraszám	**3**	Melyből: 3.2 előadás	**2**	3.3 szeminárium/labor	**1**
3.4 Tantervben szereplő össz-óraszám	**36**	Melyből: 3.5 előadás	**24**	3.6 szeminárium/labor	**12**
A tanulmányi idő elosztása:					óra
Félévközi készülés órákra					**20**
Felkészülés parciális vizsgára					**30**
Házi feladat elkészítése					**20**
Kijelölt írásos tananyag elsajátítása					**14**
Vizsgafelkészülés					**30**
Más tevékenységek:					**-**
3.7 Egyéni munka össz-óraszáma	**114**				
3.8 A félév össz-óraszáma	**150**				
3.9 Kreditszám	**6**				

4. Előfeltételek (ha vannak)

4.1 Tantervi	● Nincsen.
4.2 Kompetenciabeli	● Programozás alapjai ● Java és C/C++ programozási nyelvek ● Operációs rendszerek ● Kommunikációs hálózatok

5. Feltételek (ha vannak)

5.1 Az előadás lebonyolításának feltételei	● Táblával és videoprojektorral felszerelt előadóterem.
5.2 A szeminárium / labor lebonyolításának feltételei	● Számítógépekkel és megbízható vezeték nélküli hálózattal felszerelt laborterem ● Áramellátási lehetőség hordozható számítógépeknek

6. Elsajátítandó jellemző kompetenciák

Szakmai kompetenciák	C1 Programozás magas-szintű nyelveken C1.3 Megfelelő forráskód fejlesztése egy ismert programozási nyelvben és a komponensek egységes tesztelése adott tervezési specifikáció alapján C1.4. Alkalmazások tesztelése adott tesztelési terv alapján C6 Számítógépes hálózatok tervezése és adminisztrálása C6.5 Számítógépes hálózati projektek készítése
Transzverzális kompetenciák	CT3 Hatékony módszerek és technikák használata tanulásra, információszerzésre, kutatásra és a tudásszerzési kapacitások fejlesztésére, egy dinamikus társadalom igényeinek való megfelelésre, román és egy nemzetközi nyelven történő kommunikációra

7. A tantárgy célkitűzései (az elsajátítandó jellemző kompetenciák alapján)

7.1 A tantárgy általános célkitűzése	A tárgy célja, hogy növelje az informatikus hallgatók biztonságtudatosságát, formálja a biztonsággal kapcsolatos szemléletüket, valamint felkészítse őket az IT biztonsággal kapcsolatos gyakorlati kihívásokra, és áttekintést adjon a gyakorlatban használt IT biztonsági megoldásokról. Ennek érdekében, a tárgy bevezető szintű áttekintést nyújt az IT biztonság különböző területeiről, és leíró jelleggel bemutatja az egyes területek kihívásait és azok megoldásait. Néhány kiemelt területen (pl. szoftverbiztonság, webes rendszerek biztonsága, kriptográfia) gyakorlati feladatok megoldására is sor kerül laborkörnyezetben, így ezeken a területeken a tárgy az előadásokon elhangzott módszerek megértésén túl, azok alkalmazását is célul tűzi ki. A tárgy további célja, hogy alapozást nyújtson azon hallgatók számára, akik IT biztonsággal kapcsolatos ismereteiket egy MSc program keretében szeretnék majd elmélyíteni.
7.2 A tantárgy sajátos célkitűzései	

8. A tantárgy tartalma

8.1 Előadás	Didaktikai módszerek	Megjegyzések

IT biztonsággal kapcsolatos alapfogalmak, az IT biztonság kockázat alapú megközelítése: alapvető biztonsági célok (CIA, AAA); támadó modellek, sérülékenységek, biztonsági mechanizmusok áttekintése; kockázatmenedzsment, security engineering és security operations folyamata; etikai kérdések az IT biztonságban. (2x45 perc)	előadás, vetítés, magyarázat, példák	
A kriptográfia története: alapvető kriptográfiai fogalmak bevezetése történelmi példákon keresztül, egyúttal a kriptográfia története főbb mérföldköveinek bemutatása. Modern kriptográfiai algoritmusok: szimmetrikus és aszimmetrikus kulcsú rejtjelezés, hash függvények, üzenet hitelesítés, digitális aláírás, véletlenszám generálás, kulcscsere protokollok, PKI. Modern kriptográfiai alkalmazások áttekintése, a kriptográfiai rendszerek gyakorlati problémái. (6x45 perc)	előadás, vetítés, magyarázat, példák	
Hitelesítés fogalma, módszerei, alkalmazása: a napjainkban használt tudás-, birtok- és tulajdonságalapú hitelesítési módszerek bemutatása. Ezek működési elvei, előnyei és hátrányai. Lehetséges támadások az egyes módszerekkel szemben, védekezés a támadások ellen. Két- és többfaktoros hitelesítés. Esettanulmányok. Néhány, hitelesítéssel kapcsolatos szabvány, keretrendszer és protokoll (pl. OpenID, Kerberos, FIDO) fogalmainak és működésének bemutatása. Engedélyezés fogalma, módszerei, alkalmazása: az engedélyezés célja, megközelítések. Néhány fontosabb, engedélyezéssel kapcsolatos szabvány, keretrendszer és protokoll (pl. OAuth, SAML) fogalmainak és működésének bemutatása; példák mindennapjainkból, esettanulmányok. (4x45 perc)	előadás, vetítés, magyarázat, példák	
A hozzáférés-szabályzás és kapcsolódó fogalmai. A hozzáférés-szabályzás általános modellje és két fő megközelítése: DAC, MAC. Engedélyezés és hozzáférés-szabályzás Linux alapú operációs rendszereken: felhasználók, csoportok, engedélybitek; POSIX ACL-ek, SELinux, AppArmor. Engedélyezés és hozzáférés-szabályzás Windows operációs rendszereken: felhasználók, csoportok, fájlrendszer- és megosztásszintű engedélyek. (2x45 perc)	előadás, vetítés, magyarázat, példák	

Szoftverekkel kapcsolatos biztonsági kihívások: a tervezés, fejlesztés, tesztelés és üzemeltetés során felmerülő lehetséges problémák és azok megoldásai. Az alkalmazás fejlesztési folyamat lépései során megjelenő biztonsági kihívások bemutatása; a tervezés biztonsági kihívásai; szoftverek biztonsági elemzése és tesztelése (code review, architekturális kockázatelemzés, software penetration testing, fuzzing), néhány tesztelést segítő eszköz bemutatása. Implementációs kihívások alacsony szintű programozási nyelvek esetén: memória korrupciós hibák oka és kihasználása (a programozási hibákból származó biztonsági problémák típusai, a hibákat kihasználó exploit technikák működése, illusztratív példák, pl: buffer overflow, heap overflow, format string, ROP, stb.); a támadásokat megnehezítő védelmi megoldások bemutatása. Implementációs kihívások webes rendszerekben: az alkalmazásokra veszélyt jelentő kliens és szerver oldali támadások (SQL injection, XSS, CSRF, stb.) és a lehetséges védelmi megoldások (SOP, CSP, stb.) bemutatása. (8x45 perc)	előadás, vetítés, magyarázat, példák	
Hálózatbiztonsági kihívások: tipikus hálózati támadás fázisai (felderítés, behatolás, backdoor telepítés, lateral movement és priviledge escalation, root-ra törés), az egyes fázisokban alkalmazott módszerek és eszközök; hálózatok biztonsági tesztelése (penetration testing, etikus hacking). (2x45 perc)	előadás, vetítés, magyarázat, példák	
Hálózatbiztonsági megoldások: határvédelem tűzfalakkal, tűzfalak típusai, működésük, tipikus konfigurációs beállítások, és tipikus hibák; behatolás detektáló és SIEM rendszerek fajtái, működésük, virtuális magánhálózatok. (4x45 perc)	előadás, vetítés, magyarázat, példák	
Kártékony programok (malware) fogalma, működése: Rosszindulatú szoftverek típusai (vírusok, férgek, trójaiak, stb.), működésük, terjedési és rejtőzködési technikák (rootkit-ek), alkalmazások (kiberbűnözés, botnetek, célzott támadások). Kártékony programok detekciója. (2x45 perc)	előadás, vetítés, magyarázat, példák	
IT rendszerek biztonságának üzemeltetési kérdéssei: Sérülékenységek menedzsmentje, frissítés, back-up. Biztonsági incidensek kezelése: malware fertőzések detektálása, malware alapú incidensek kezelése, logelemzés, memória és disk forensics alapjai. (2x45 perc)	előadás, vetítés, magyarázat, példák	

Személyes adatok védelme (privacy): Adatvédelem (privacy) és a személyes adat fogalma, motivációs példák. Webes nyomonkövetési technikák (pl. browser fingerprinting, third party cookie-k). Anonim kommunikációs rendszerek működése, alkalmazási területek. Query auditing. Anonimizáció, pszichológiai profilozás. (2x45 perc)	előadás, vetítés, magyarázat, példák	
A gépi tanulás biztonsági kihívásai: Motivációs példák. CIA (confidentiality, integrity, availability) problémák a gépi tanulásban, gépi modellek auditálása, jogi háttér. Confidentiality: Modell inverzió, Membership támadás. Integrity: Támadó minták (evasion), tanulóadat szennyezése (targeted pollution). Availability: Sponge minták generálása, nem célzott szennyezés (untargeted pollution). (4x45 perc)	előadás, vetítés, magyarázat, példák	
A biztonság és a privacy közgazdasági megközelítése: Egyéni és szervezeti gazdasági ösztönzők szerepe az információbiztonságban. Aszimmetrikus információ: kontraszelekció, erkölcsi kockázat, tragacspiac. Ösztönzők összehangolásának hiánya: példák, IT biztonsági eszközök és szolgáltatások piaca. Externáliák: biztonság mint externália, biztonsági keresztfüggések. Sérülékenységek gazdaságtana. Kiberbiztosítás. Privacy gazdasági kérdései, privacy keresztfüggések, példák: Facebook, Google, genom, lokáció, k-anonim rendszerek. (4x45 perc)	előadás, vetítés, magyarázat, példák	

Könyvészet

1. Előadásokhoz rendelt online olvasnivalók (könyvfejezetek, cikkek, blogsorozatok)
2. The Cyber Security Body Of Knowledge (CyBOK) on-line gyűjtemény fejezetei (https://www.cybok.org/)

8.2 Laborok	**Didaktikai módszerek**	**Megjegyzések**
1. labor: Kriptográfiai programkönyvtár használata: Kriptográfiai mechanizmusokat (rejtjelezés, digitális aláírás) használó programok készítése alkalmas kriptográfiai programkönyvtár használatával.	Feladatmegoldás	
2. labor: Inputvalidáció: A támadási felületen át érkező adatok megfelelő ellenőrzésének elsajátítása olyan alkalmazás készítésével, mely képes a megadott, potenciálisan veszélyes bemeneteket helyesen kezelni.	Feladatmegoldás	
3. labor: Szoftverek biztonsági tesztelése: A különböző technológiákkal fejlesztett alkalmazások esetén felmerülő tesztelési módszerek megismerése és elsajátítása, kiemelt hangsúllyal az alacsony szintű nyelveken fejlesztett alkalmazásokra.	Feladatmegoldás	

4. labor: Webes rendszerek biztonsága: Webes alkalmazásokat fenyegető támadások megértése és kipróbálása; a támadásokat megállító lehetséges védelmek kiválasztása vagy alkalmazása.	Feladatmegoldás	
5. labor: Incidens kezelés, digitális elemzés (forensics): Logelemzés, rögzített hálózati forgalom (packet capture) elemzése, memóriakép és háttértár digitális elemzése (memory and disk forensics).	Feladatmegoldás	
6. labor: Személyes adatok védelme (privacy): Query auditor fejlesztése alkalmas lineáris algebra könyvtár használatával.	Feladatmegoldás	
Könyvészet 1. Előadásokhoz rendelt online olvasnivalók (könyvfejezetek, cikkek, blogsorozatok) 2. The Cyber Security Body Of Knowledge (CyBOK) on-line gyűjtemény fejezetei (https://www.cybok.org/)		

9. A tantárgy tartalmának összhangba hozása az episztemikus közösségek képviselői, a szakmai egyesületek és a szakterület reprezentatív munkáltatói elvárásaival

- A tantárgy tematikája nagy átfedést mutat az egyetemi oktatásban a fontosabb egyetemeken oktatott hasonló tematikájú tantárgyak tartalmával.
- A tananyagok kidolgozása a nemzetközileg legelismertebb szerzők munkái alapján történt, az ajánlott könyvészet szintén a terület legrelevánsabb munkái alapján van összeállítva.
- A tantárgy keretein belül oktatott témák szükségesek az aktuális grafikai szoftverfejlesztői iparban történő elhelyezkedéshez, a cégek elvárják az ilyen jellegű ismereteket.

10. Értékelés

Tevékenység típusa	10.1 Értékelési kritériumok	10.2 Értékelési módszerek	10.3 Aránya a végső jegyben
10.4 Előadás	1 db nagy zárthelyi (sikeres teljesítés feltétele: a zárthelyin megszerezhető pontszám min. 40%-nak elérése)		33,(3)%
	Írásbeli vizsga (sikeres teljesítés feltétele: a vizsgán megszerezhető pontszám min. 40%-nak elérése)		66,(6)%
10.5 Szeminárium / Labor	6 db labor esetén legalább 4 db labor sikeres teljesítése (ha a félév során valamelyik labor elmarad, akkor 3 db labor sikeres teljesítése) szükséges az aláírás megszerzéséhez (sikeres teljesítés feltétele: a labor gyakorlat során megszerezhető pontszám min. 75%-nak elérése)		0%
10.6 A teljesítmény minimumkövetelményei			
Az átmenő jegy feltételei: ● A zárthelyi és a vizsga pontszámainak min. 40%-nak megszerzése. ● A labor gyakorlat során megszerezhető pontszám min. 75%-nak elérése.			

Kitöltés dátuma	Előadás felelőse	Szeminárium felelőse
2024. július 18.	Dr. Kolumbán Sándor egyetemi adjunktus	Dr. Kolumbán Sándor egyetemi adjunktus

Az intézeti jóváhagyás dátuma	Intézetigazgató
2024. július 18.	Dr. András Szilárd Károly egyetemi docens