### TANTÁRGYI KÖVETELMÉNYEK

|  |  |
| --- | --- |
| Tantárgy kódja és neve: | „ BPI2240” Informatikai Biztonság |
| Oktató neve: | Halász Attila / Molnár Zsuzsanna |
| Meghirdetés féléve: | 2019/2020 I. félév |
| Kredit: | 3 |
| Heti óraszám: | 3 |
| Értékelés módja: | aláírás, kollokvium |
| Óra időpontja és helye: | Neptun szerint |
| Oktató elérhetősége: | halasz.attila@nye.hu, [monar.zsuzsanna@nye.hu](mailto:monar.zsuzsanna@nye.hu) 42 599 400 /2828 |

Az előadások látogatása nem kötelező.

Az aláírás megszerzésének feltételei:

* Zárthelyi dolgozatok (1) minimum 60 %-os teljesítése.

A zárthelyi dolgozatokat a megadott időpontban lehet megírni ill. a következő órán lehet javítani. Esetleges pótlására csak a hiányzást követő első órán az orvosi igazolás bemutatása után van lehetőség. Aki a zárthelyin puskázik 0 pontot kap a dolgozatára.

Írásbeli vizsga a vizsgaidőszakra meghirdetett időpontokban.

Értékelés:

1. 0–59 %

2. 60-69%

3. 70-79%

4. 80-89%

5. 90-100%

Az írásbeli vizsga kiváltható a kiadott gyakorlati feladtok bemutatásával.

A félév tervezett témakörei: a kiosztott tanmenet szerint.

**A tantárgy célkitűzései:** A tárgy célja a hallgatók bevezetése az informatikai rendszerek tipikus biztonsági problémáinak és azok elhárítási lehetőségeinek témakörébe.

Témakörök

Általános bevezető az informatika biztonságba

• Alapfogalmak

• A legfontosabb biztonsági alapelvek

• A biztonság összetevői, az információvédelem és az informatikai biztonság.

• IT biztonsági oktatás és tanúsítványok

• Megelőző intézkedések

A számítógépes hálózatok biztonsági kérdései

• E-mail és web biztonság.

• Vírusok és egyéb számítógépes visszaélések, fenyegetések és támadások.

• A fontosabb kommunikációsés authentikációs protokollok.

• Néhány fontosabb biztonsági hiba és elkerülése

• Hálózati támadások típusai.

• Tűzfalak típusai, tulajdonságaik

• Az infrastruktúra felépítése hálózati a határvédelem tervezése

Operációs rendszerek biztonsági kérdései

• Speciális védelmi rendszerek

• A Linux biztonságos telepítése és üzemeltetése

• Webszerver biztonságos telepítése és üzemeltetése

Kriptológia alapok/ Titkosítások

* Alapfogalmak
* A legfontosabb titkosítási alapelvek
* A titkosítási algoritmusok családfája
* A szimmetrikus (egykulcsos) titkosítási algoritmusok működése:DES, 3DES, AES.
* Az aszimmetrikus (két kulcsos, nyílt kulcsú) algoritmusok működése, DH, RSA
* A Diffie-Hellman kulcsleosztási protokoll megértése
* Az RSA-algoritmus
* Digitális aláírás és nyílt kulcsú titkosítás RSA-val
* Tikosítások gyakorlati alkalmazásai : VPN,SSL/Tls, SSH, IpSec megoldások működésének áttekintése.

Kötelező ill. ajánlott irodalom:

Oktatói jegyzet: [http://moodle.nyf.hu](http://moodle.nyf.hu/) # Informatikai Biztonság – 2019/20

1. Virasztó Tamás: Titkosítás és adatrejtés. NetAcademia, Bp : 2004. ISBN:9789632142531  
2. SZENES K. (szerk.): Az informatikai biztonság kézikönyve, Dashöfer, Budapest, 2010. ISBN:9639313122  
3. GYÖRFI L. - GYŐRI S. - VAJDA I.: Információ- és kódelmélet. Typotex Kiadó, Budapest, 2010. ISBN: 9789632791159  
4. J. DYKSTRA: Essential Cybersecurity Science. O'Reilly Media, 2015. ISBN: 9781491920947  
5. N. DHANJANI: Abusing the Internet of Things. O'Reilly Media, 2015. ISBN: 9781491902899