

# TANTÁRGYI TEMATIKA ÉS TELJESÍTÉSI KÖVETELMÉNYEK

## 2023/2024 2. FÉLÉV

	Cím	Kiberbiztonság
Tárgykód		IVB165MNMI
Heti óraszám: ea/gy/lab		2/0/0
Kreditpont		2
Szak(ok)/ típus		Mérnökinformatikus
Tagozat		Nappali
Követelmény		vizsga
Meghirdetés féléve		tavasz
Előzetes követelmény(ek)		IP alapú rendszerek és alkalmazások 1.
Oktató tanszék(ek)		Rendszer- és Szoftvertechnológiai Tanszék
Tárgyfelelős		Gyurák Gábor
Oktatók		Gyurák Gábor

## TÁRGYLEÍRÁS

A tantárgy célja, hogy a hallgatók informatika biztonságtudatosságának növelése valamint a védelmi és támadói képességek kialakítása.

A főbb témakörök: Információs rendszerek általános modellje, veszélyforrások. A védelem néhány szabványos (tanúsítható) modellje. Titkosító eljárások, hálózati infrastruktúra. Felhasználóazonosító eljárások. Hozzáférésvédelem.

Megbízható működés. Biztonsági osztályok meghatározása. Védelmi szabványok. Operációs rendszerek behatolásvédelme. Hálózatok behatolásvédelme. Elosztott rendszerek védelme. Kockázatkezelés. Informatikai rendszerek támadása.

## TÁRGYTEMATIKA

### 1. AZ OKTATÁS CÉLJA

A tantárgy célja, hogy a hallgatók informatika biztonságtudatosságának növelése valamint a védelmi és támadói képességek kialakítása.

### 2. A TANTÁRGY TARTALMA

#### TÉMAKÖRÖK

#### ELŐADÁS

1. Alapfogalmak
2. Védelmi modellek
3. Veszélyek
4. Logikai védelem
5. Fizikai védelem
6. Adminisztratív védelem
7. Authentikáció
8. Authorizáció
9. Audit
10. Biztonsági protokollok
11. Tűzfalak
12. Behatolásjelző rendszerek
13. Kriptográfia alapok
14. Kriptográfiai alkalmazások

#### LABOR- GYAKORLAT

1. Jogi és etikai héttér
2. Az informatikai rendszerek támadásának komplex rendszere
3. Az informatikai rendszerek védelmének komplex rendszere

## RÉSZLETES TANTÁRGYI PROGRAM ÉS A KÖVETELMÉNYEK ÜTEMEZÉSE

*Jelezzük az oktatási szüneteket is!*

### ELŐADÁS

Okta- tási hét	Téma	Kötelező irodalom hivatkozás, oldalszám (-tól-ig)	Teljesítendő feladat (beadandó, zárthelyi, stb.)	Teljesítés ideje, határideje
1.	Követelményrendszer, bevezetés	[1] 2.1. fejezet	-	-
2.	Veszélyek és védelmi modellek	[1] 2.3 fejezet	-	-
3.	Magas rendelkezésre állás	[1] 2.2 fejezet	-	-
4.	IAAA modell	[1] 3. fejezet	-	-
5.	Security Operations Center	[1] 3. fejezet	-	-
6.	DDoS védelem	[1] 4. fejezet	-	-
7.	Kriptográfia alapfogalmak	[2] 3. fejezet	-	-
8.	Szimmetrikus kriptográfia	[2] 3. fejezet	-	-
9.	Őszi szünet	-	-	-
10.	Aszimmetrikus kriptográfia	[2] 3. fejezet	-	-
11.	Digitális aláírás	[2] 3. fejezet	-	-
12.	PKI	[2] 3. fejezet	-	-
13.	Zárthelyi	-	ZH	-
14.	Pót-zárthelyi	-	PótZH	-

### 3. SZÁMONKÉRÉSI ÉS ÉRTÉKELÉSI RENDSZER

#### JELLENLÉTI ÉS RÉSZVÉTELI KÖVETELMÉNYEK

A PTE TVSz 45.§ (2) és 9. számú melléklet 3§ szabályozása szerint a hallgató számára az adott tárgyból érdemjegy, illetve minősítés szerzése csak abban az esetben tagadható meg hiányzás miatt, ha nappali tagozaton egy tantárgy esetén a tantárgyi tematikában előírányzott foglalkozások több mint 30%-áról hiányzott.

#### A jelenlét ellenőrzésének módja

Jelenléti ív

#### SZÁMONKÉRÉSEK

##### Vizsgálóval záruló tantárgy

#### Félévközi ellenőrzések, teljesítményértékelések és részarányuk a vizsgára bocsájtás feltételének minősítésben

(A táblázat példái törlendőek.)

Típus	Értékelés	Részarány a vizsgára bocsájtás feltételének minősítésben
ZH	max 100 pont	100%

#### Az aláírás megszerzésének feltétele

40%-os évközi minősítés zárthelyi megírásával

#### Pótlási lehetőségek az aláírás megszerzéséhez (PTE TVSz 50§(2))

A zárthelyi pótlására az utolsó héten van lehetőség.

**Vizsga típusa (írásbeli, szóbeli):** írásbeli és szóbeli

**A vizsga minimum** 40 %-os teljesítés esetén sikeres.

**Az érdemjegy kialakítása** (TVSz 47§ (3))

**50** %-ban az évközi teljesítmény, **50** %-ban a vizsgán nyújtott teljesítmény alapján történik.

**Az érdemjegy megállapítása az összesített teljesítmény alapján %-os bontásban**

Érdemjegy	Teljesítmény %-ban kifejezve
jeles (5)	85 % ...
jó (4)	70 % ... 85 %
közepes (3)	55 % ... 70 %
elégséges (2)	40 % ... 55 %
elégtelen (1)	40 % alatt

Az egyes érdemjegyeknél megadott alsó határérték már az adott érdemjegyhez tartozik.

## 1. IRODALOM

### KÖTELEZŐ IRODALOM ÉS ELÉRHETŐSÉGE

- [1.] Gyurák Gábor – Informatikabiztonság I., Pécs, 2015.
- [2.] Gyurák Gábor – Informatikabiztonság II., Pécs, 2015.
- [3.] William Stallings, Lawrie Brown - Computer Security Principles And Practices (2nd edition), Pearson, 2011.
- [4.] Brooks Charles – Cybersecurity Essentials, Wiley, 2018.

### AJÁNLOTT IRODALOM ÉS ELÉRHETŐSÉGE

- [1.] Randy Weaver - Guide to Tactical Perimeter Defense: Becoming a Security Network Specialist, Cengage Learning, 2007.