|  |  |
| --- | --- |
| Óbudai EgyetemBánki Donát Gépész és Biztonságtechnikai Mérnöki Kar  | Biztonságtudományi és Kibervédelmi Intézet  |
| **Tantárgy címe és kódja:** | **Elektronikus információbiztonság I. BBXEI15BNF**  | **Kreditérték:** | 4 |
| Nappali munkarend | 3 | tanév | 1 | félév  |
| **Szakok melyeken a tárgyat oktatják:** | **Biztonságtechnikai mérnök szak** |
| **Tantárgyfelelős oktató:** | Dr. habil. Kiss Gábor | **Oktatók:** | Dr. habil. Kiss Gábor |
| **Előtanulmányi feltételek (kóddal):** |  |
| **Heti óraszámok** |
| Előadás: | 2 | Tantermi gyak.:  | 0 | Laborgyakorlat:  | 2 | Konzultáció: |  |
| **Félévzárás módja:** | Évközi jegy |  (Válasszon) |
| ***Online konzultáció*** *(amennyiben szükséges):* | *… (BBB link)* |
| **Oktatási cél**: | *A tárgy oktatásának célja, hogy a hallgatók megismerjék az elektronikus rendszerek működését, biztonságukat érintő veszélyforrásokat. A különböző szoftveres és adminisztratív intézkedések megismerése a számítástechnikai rendszerek végpontjain. Mágneses, optikai adattárolás, flash adattárolók működése, adatvédelmi lehetőségeik. A keresztcsatolású Reed-Solomon kód alkalmazási területei, BIOS biztonság, vírusok működése.* *A napjainkban használt szimmetrikus kódoló algoritmusok működése. Aszimmetrikus kódolás menete. Hibrid titkosítás, HTTPS, tanúsítványkezelés.* *Titkosított fájlrendszerek használata, hitelesített driverek, memóriavédelem. PGP működése, használata.* *WIFI-nél használatos titkosítási algoritmusok működése, biztonsága (WEP, WPA, WPA2).**HASH függvények működése, felhasználási területeik..* |
| **Ütemezés**  |
| Oktatási hét | **Témakörök** |
| 1. | Flash memória biztonsága |
| 2. | Mágneses és optikai adattárolás biztonsága |
| 3. | Bios szerepe, védelme |
| 4. | Szimmetrikus kódolások (DES, AES) |
| 5. | Asszimetrikus kódolások (RSA), tanúsítványok |
| 6. | PGP, titkosított levélküldés |
| 7. | 1. Zh. |
| 8. | Vírusok, vírusvédelem |
| 9. | Hibrid titkosítás, HTTPS protokoll |
| 10. | VPN |
| 11. | Egyirányú függvények és alkalmazási területeik |
| 12. | Elliptikus görbék |
| 13. | Vezetéknélküli hálózatok védelme |
| 14. | 2. Zh. |
|  |  |
|  | **Labor témakörei** |
| 1. | BIOS védelem |
| 2. | BIOS védelem kiiktatási lehetőségei |
| 3. | MS Office adatvédelmi lehetőségei (jelszavas védelem) |
| 4. | MS Office adatvédelmi lehetőségei (jelszavas védelem kiiktatási lehetőségei) |
| 5. | Reed-Solomon kód védelmi szintje |
| 6. | Titkosított fájlrendszer (hordozható adattárolón |
| 7. | Titkosított fájlrendszer (MS Windows) |
| 8. | Titkosított fájlrendszer (Mac OS) |
| 9. | Titkosított hálózati adatforgalmazás (Böngészőbe integrált VPN, pl. Opera) |
| 10. | Titkosított hálózati adatforgalmazás (VPN szolgáltatók) |
| 11. | Titkosított hálózati adatforgalmazás (Osztott hálózat) |
| 12. | Titkosított e-mail küldés (PGP) |
| 13. | Titkosított e-mail küldés (levelező rendszerbe integrált) |
| 14. | Összefoglalás |
| **Félévközi követelmények**  |
| Zárthelyi dolgozat. | Beadandó feladat | Labormérés |
| száma | időpontok | száma | határidők | száma | időpontok |
| 2 db | félév elején egyeztetve | db |  | db |  |
| **Az értékelés, a lebonyolítás, a pótlás módja, a jegy kialakításának szempontjai** *Értékelés: Az évközijegy megszerzésének feltétele az évközi zárthelyik legalább elégséges szintre való teljesítése.**Elégséges>40%**Közepes>55%**Jó>70%**Jeles>85%**Zárthelyi dolgozatíráskor, ill. vizsgán a meg nem engedett segédeszközök (puska, mobiltelefon, stb.) használata, ill. arra tett kísérlet, továbbá bármilyen információcserére tett kísérlet az érintett hallgató(k) letiltását vonja maga után.**A szorgalmi időszak utolsó hetében lehetőség van a sikertelen, illetve igazoltan (pl. betegség) mulasztott zh-k pótlására.**Az évközi jegy/aláírás szorgalmi időszakon túli pótlásának módja: HKR 47. §**Hiányzás szabályozása: HKR 46. §**Valamennyi, jelen dokumentumban nem szabályozott, kérdésben az Óbudai Egyetem Hallgatói Követelményrendszere, valamint Tanulmányi Ügyrendjének rendelkezései az irányadók.* |

|  |  |
| --- | --- |
| **Letiltva bejegyzést kap:** | Aki eléri, illetve meghaladja a megengedett hiányzások számát, illetve egyik zárthelyi dolgozatot sem írta meg és nem igazolta megfelelően a hiányzását (pl. betegség esetén orvosi naplószámot tartalmazó igazolással). |
| **Kötelező irodalom:** | Előadás jegyzet |
| **Ajánlott irodalom:**  | Hans Delfs , Helmut Knebl: Introduction to Cryptography, Springer, ISBN: 978-3-662-47973-5, 2015 |
| **A tárgy minőségbiztosítási módszerei:** |  |

Kelt: Budapest, 2023. 06. 15.

Szöveg beírásához kattintson vagy koppintson ide.

………………………………………………………

Dr. habil. Kiss Gábor