| Tantárgy neve: **Kiberbiztonság** | Kreditértéke: **4** |
|---|---|
| A tantárgy besorolása: kötelező | |
| A tanóra típusa: 0 óra előadás, 4 óra gyakorlat, összesen 48 óra az adott félévben<br>Az adott ismeret átadásában alkalmazandó további (*sajátos*) módok, jellemzők *(ha vannak)*: | |
| A számonkérés módja (kollokvium / évközi jegy / egyéb): évközi jegy<br>Az ismeretellenőrzésben alkalmazandó további (*sajátos*) módok *(ha vannak)*: hallgatói esszé és prezentáció | |
| A tantárgy tantervi helye: 2. félév | |
| Előkövetelmények: - | |
| Tantárgyleírás: Kiberbiztonság | |
| A félév során a hallgatók betekintést nyernek korunk legdinamikusabban fejlődő, életünk minden területét átható mesterséges közegének kifejezetten biztonsági aspektusából történő tanulmányozásába. A kurzus során a hallgatók megismerik és a későbbi mindennapi használat érdekében elsajátítják a legfontosabb általános- és kiberbiztonsági fogalmakat, stratégiai koncepciókat, jogszabályokat, szabványokat és keretrendszereket, valamint esettanulmányokkal kiegészítve megismerhetik az általános és ipari környezeti, valamint IPAR 4.0 és a mechatronikai területet érintő kibertevékenységeket, a kibertér kártékony szereplőit, azok lehetséges motivációit, céljait és alkalmazott eljárásait. Mindemellett pedig általánosan képet kapnak a jelenlegi felforgató/feltörekvő technológiákról is. A megszerzett tudásanyag révén a hallgatók bármely mérnöki területen versenyképes nemzetközi tudással rendelkeznek majd a kiberbiztonság és a biztonsági kockázatok tekintetében, amely segítségével képessé válnak a tervezéstől a kivitelezésig bármely munkafolyamat során kibertudatos megoldások kidolgozására és beépítésére, valamint az alkalmazó szervet általános kiberbiztonságának növelésére, vonatkozó szabványok és standardok alkalmazására. | |
| Irodalom | |
| Kötelező irodalom: | |


- **Muha Lajos – Krasznay Csaba**: *Az elektronikus információs rendszerek biztonságának menedzselése* – Budapest, NKE, 2018.
- **Christopher J. Hadnagy**: *Social Engineering - The Science of Human Hacking.* John Wiley & Sons, 2010. (angol)
- **Fehér Krisztián:** *Kezdő hackerek kézikönyve - Avagy informatikai támadások és kivédésük***.** BBS-INFO Könyvkiadó és informatikai Kft, Budapest, 2016.
- **Fekete Imre**: *Modern átverések - avagy IT biztonság a hétköznapokban.* BBS-INFO Könyvkiadó és informatikai Kft, Budapest, 2019.
- **Kovács László**: *A kibertér védelme*. Dialóg Campus Kiadó, Budapest, 2018.
- **Kovács László**: *Kiberbiztonság és -stratégia.* Dialóg Campus Kiadó, Budapest, 2020.
- **Nagy Róbert**: *DarkNet – avagy az internet sötét oldala.* BBS-INFO Könyvkiadó és informatikai Kft, Budapest, 2021.
- **Tim Rains:** *Cybersecurity Threats, Malware Trends, and Strategies: Learn to mitigate exploits, malware, phishing, and other social engineering attacks.* Packt Publishing, 2020. (angol)
- **Török Bernát** (szerk.): *Információ- és kiberbiztonság.* Dialóg Campus Kiadó, Budapest, 2020.
- **Csege Gyula:** *A terrorizmussal kapcsolatba hozható internetes megosztások kezelése és megoldása hazánkban,* Belügyi Szemle folyóirat 2017. 65./6. szám
- **Magyar Informatikai Biztonság Ajánlások** (MIBA) – KIB 25 . számú ajánlás, Budapest, 2008.

- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- 2009. évi CLV. törvény a minősített adat védelméről

Ajánlott irodalom:


- **Bárfai Barnabás, Fehér Krisztián, Dr. Kökényesi Bartos Attila**: *Mesterséges intelligencia, avagy Pandora digitális szelencéje.* BBS-INFO Könyvkiadó és informatikai Kft, Budapest, 2020.
- **Fehér Krisztián:** *Hackertechnikák - Útmutató valódi hacker módszerek biztonságos kipróbálásához.* BBS-INFO Könyvkiadó és informatikai Kft, Budapest, 2019.
- **Fehér Krisztián**: *Kibervédelmi tesztalkalmazások programozása.* BBS-INFO Könyvkiadó és informatikai Kft, Budapest, 2020.
- **Haig Zsolt**: *Információs műveletek a kibertérben,* Dialóg Campus Kiadó, Budapest, 2019.
- **Kevin D. Mitnick, William L. Simon**: *A legendás hacker - A megtévesztés művészete.* Prefact-Pro Kft., Budapest, 2003.
- **Kiss Tibor** (szerk.): *Kibervédelem a bűnügyi tudományokban.* Dialóg Campus Kiadó, Budapest, 2020.
- **Mezei Kitti**: *A kiberbűnözés aktuális kihívásai a büntetőjogban.* BBS-INFO Könyvkiadó és informatikai Kft, Budapest, 2021.
- **Yuri Diogenes, Erdal Ozkaya:** Cybersecurity – *Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics* (English Edition). Packt Publishing, 2018. (angol)


Előírt szakmai kompetenciák, kompetencia-elemek

***a)* tudása**

- Összefüggéseiben ismeri és alkalmazza a kiberbiztonsági szakmához kötött természettudományos és elméleti ismereteket, ok-okozati összefüggéseket.
- Elsajátította az elméletileg megalapozott, rendszerszemléletű gyakorlatorientált kiberbiztonsági gondolkodásmódot, ezzel képessé válik bekapcsolódni az őt alkalmazó szervezet kiberbiztonsági stratégiájának, eljárásainak megalkotásába, vagy akár képesség válik önálló kiberbiztonsági belső szabályrendszer és eljárásrend kidolgozására.
- Megismeri és munkája során alkalmazza a COBIT-keretrendszert és a Secure by Design koncepciókat.
- Ismeri a kiberbiztonsági területen alkalmazott legfontosabb stratégiákat, házi és nemzetközi jogszabályokat, koncepciókat, azok alkalmazási területeit.
- Ismeri a hazai és nemzetközi szabványokat, előírásokat, azokat munkája során alkalmazza, ezt munkatársaitól is megköveteli.
- Ismeri a kiberbiztonsági szakterülethez kapcsolódó információs és kommunikációs technológiákat.
- Ismeri korunk lefontosabb felforgató/feltörekvő kibertechnológiáit és trendjeit, azok egyes előnyeit és hátrányait, kiberbiztonsági megoldásait.
- Munkája során a kiberbiztonsági szemléletmódot szem előtt tartva képessé válik napjaink felforgató/feltörekvő technológiáinak beépítésére, alkalmazására már a tervezési folyamattól kezdődően.
- Ismeri a kiberbiztonsági kártékony szereplőit, különbséget tud tenni a hacker, az APT és a hacktivizmus és más szakterületi fogalmak között.
- Ismeri a leggyakrabban alkalmazott kártékony kibertevékenységeket, megoldásokat és képessé válik az ezek elleni védekezésre.
- Ismeri a legfontosabb kiberbiztonsági operációs rendszer disztribúciókat.
- Ismeri az OT-rendszerek és alrendszerek kiberbiztonsági aspektusait.

Munkája során képessé válik a megismert kiberbiztonsági tudásanyag átadására a kollégái számára.

***b)* képességei**

- Képes bekapcsolódni az alkalmazó cég kiberbiztonsági stratégiájának kidolgozásába.
- Képes a tervezés és kivitelezés során előzetes kibervédelmi mechanizmusok implementálására.
- Képes átlátni a kiberbiztonság szerepét az OT-rendszereken és azok alrendszerein belül.
- Képes hatékony kommunikációt folytatni az alkalmazó szervezet más kibervédelmi szervezeti egységeivel és együttesen közreműködni az esetleges problémák megoldásában.
- Képes hatékony kommunikációt folytatni az alkalmazó szervezet nevében a hatósági szervezetekkel és együttesen közreműködni az esetleges problémák megoldásában.
- Képes kibervédelmi jogalkotói tevékenység mérnöki szemléletmód által történő támogatására.
- Képes az élethosszig tartó tanulásra és elkötelezett a sokszínűség és az értékalapúság mellett.

- Felkészült, hogy szakterületén, anyanyelvén és legalább egy idegen nyelven publikációs, prezentációs tevékenységet és tárgyalásokat folytasson kibervédelmi témában.
- Elkötelezett a kiberbiztonság munkahelyi és mindennapi alkalmazása, valamint a kibertudatos szemléletmód más személyekben történő kialakítása iránt.

***c)* attitűdje**

- Megszerzett ismereteire alapozva integrátori szerepet tölt be a műszaki (elsősorban gépészetmérnöki, villamosmérnöki, informatikai) tudományok integrált és a kiberbiztonsági szakma ismeretanyagának alkalmazásában, valamint minden olyan tudományterület kiberbiztonsági támogatásában, ahol az adott szakterület szakemberei kiberbiztonsági alkalmazásokat, megoldásokat igényelnek.
- Munkája során vizsgálja a kiberbiztonsági kutatási, fejlesztési és innovációs célok kitűzésének lehetőségét, és törekszik azok megvalósítására; elkötelezett arra, hogy bármely mérnöki területet új kiberbiztonsági ismeretekkel, tudományos eredményekkel gyarapítsa.
- Törekszik arra, hogy a munkáját rendszerszemléletű és folyamatorientált gondolkodásmód alapján komplex kiberbiztonsági megközelítésben is végezze.
- Törekszik a kiberbiztonság tervezőasztaltól kezdődő, költség- és munkahatékonyságot növelő követelményeinek érvényesítésére.
- Törekszik a kiberbiztonságra vonatkozó feladatait szakmailag magas szinten önállóan vagy munkacsoportban megtervezni és végrehajtani.
- Törekszik a kiberbiztonsági kompetenciáinak fejlesztésére.
- Kiberbiztonsági tekintetben törekszik továbbá az önművelésre, önfejlesztésre aktív, egyéni, autonóm tanulással.
- Elkötelezett a magas színvonalú, kiberbiztonsági szemléletmód kialakítására és törekszik e szemléletet munkatársai felé is közvetíteni.
- Munkája és döntései során betartja a kiberbiztonság (és általánosan a biztonság) alapelveit, jogi szabályozás, valamint a kiberbiztonság vonatkozó előírásait.
- Szakmai munkája során kiberbiztonsági tekintetben megfelel a minőségügy, a fogyasztóvédelem, a termékfelelősség és a kiberetika követelményeinek.
- Megfelelően nyitott, ismeri és alkalmazza az egyenlő esélyű hozzáférés elvét.

***d)* autonómiája és felelőssége**

- Megszerzett kiberbiztonsággal kapcsolatos tudását és tapasztalatait formális, nem formális és informális információátadási formákban megosztja szakterülete művelőivel.
- Kezdeményező szerepet vállal a műszaki területet érintő kiberbiztonsági problémák megoldásában.
- Kiberbiztonsági szempontból értékeli beosztottjai munkáját, kritikai észrevételeinek megosztásával elősegíti szakmai fejlődésüket.
- Kiberbiztonsági szakmai problémák megoldása során önállóan és kezdeményezően lép fel.
- Munkatársait és beosztottjait felelős és etikus kiberbiztonsági szemléletmódra neveli.
- Felelősséggel viseltetik a fenntarthatóság, a munkahelyi egészség- és biztonságkultúra, valamint a környezettudatosság iránt.
- Kiberbiztonsági kérdéseket illető döntéseit körültekintően, más (elsősorban jogi, gazdasági, energetikai, villamosmérnöki, informatikai és orvosi) szakterületek képviselőivel konzultálva, önállóan hozza, amelyekért felelősséget vállal.
- Új, komplex megközelítést kívánó, kiberbiztonsági területhez kapcsolódó stratégiai döntési helyzetekben, illetve nem várt élethelyzetekben is törekszik a jogszabályok és etikai normák teljes körű figyelembevételével dönteni.
- Döntései során figyelemmel van a környezetvédelem, a minőségügy, a fogyasztóvédelem, a termékfelelősség, az egyenlő esélyű hozzáférés elvére és alkalmazására; a munkahelyi egészség és biztonság, a műszaki-, gazdasági- és jogi szabályozás, valamint a mérnöketika alapvető előírásaira.

Tantárgy felelőse: Dr. Csege Gyula, MBA

Tantárgy oktatásába bevont oktató(k): Dr. Csege Gyula, MBA

| Tantárgy neve: Kiberbiztonság | | Tantárgy kódja: MK5KIBER04R217 |
|---|---|---|
| Kredit: 4 | Követelmény: évközi jegy | Tanszék: Mechatronikai Tanszék |
| Óraszám: 0 + 4 | Előkövetelmény: hallgatói esszé és prezentáció | |
| Tantárgyfelelős: Dr. Csege Gyula, MBA | | Tantárgy oktatói: Dr. Csege Gyula, MBA |

| HÉT | ELŐADÁS | GYAKORLAT |
|---|---|---|
| 1. | | Kiberbiztonsági és információbiztonsági alapvetések, a kiberbiztonság diszciplináról általánosan, ISO szabványok, COBIT keretrendszer, általános és speciális szabályozók. |
| 2. | | Kiberbiztonsági stratégia alkotás, nemzetközi stratégiák, magyar vonatkozású jogszabályok és Magyarország kiberbiztonsági stratégiája. |
| 3. | | A kiberbiztonsági ipari aspektusai (OT rendszerek és alrendszerek), szektorális érintettségek, Kritikus infrastruktúrák, Secure by Design koncepció, felforgató/feltörekvő technológiák és trendek (AI, IoT, Cloud Computing, Big Tech, Big Data, Blokklánc, Kriptovaluták) előnyökkel és hátárnyokkal. |
| 4. | | Kiberbűnözés és egyéb kártékony kibertevékenységek, Dark Web, Deep Web, illegális szolgáltatások és esettanulmányok (Silk Road 1.0, 2.0, MaaS platforomok és egyéb szolgáltatások). |
| 5. | | Tor böngésző működési elve és gyakorlati bemutatása, Nyílt forrású hírszerzés (OSINT). |
| 6. | | Hackerek fogalma és csoportosítása, kiemelkedő hackerek bemutatása esettanulmányokkal, APT hacking és APT-csoportok és azok célpontjai, motivációi, Hacktivizmus és hactivista csoportok, azok céljai, motivációi. |
| 7. | | Kiberbiztonsági operációs (teszt)rendszerek (Linux disztríbúciók). |
| 8. | | Alkalmazott hacker technikák és esettanulmányok (Hamis segítségnyújtás, Kölcsönösség kihasználása, Megszemélyesítés, Shoulder Surfing). |
| 9. | | Alkalmazott hacker technikák és esettanulmányok (Piggybacking, Tailgating, Kukabúvárkodás, Scam). |

| | | |
|---|---|---|
| 10. | | Alkalmazott hacker technikák és esettanulmányok ( Phising technikák, Spam, Keylogger,). |
| 11. | | Alkalmazott hacker technikák és esettanulmányok (DDOS-támadások fajtái, Zsarolóvírusok), kiberbiztonsági tippek a mindennapokban. |
| 12. | | Hallgatói esszék és prezentációk ismertetése és bemutatása (tantárgyi zárókövetelmények). |
| 13. | Hallgatói esszék és prezentációk ismertetése és bemutatása (tantárgyi zárókövetelmények) | |
| KÖVETELMÉNYEK | | |
| Az aláírás feltétele: Hallgatói gyakorlati feladat, kutatás önálló végrehajtása | | |
| Teljesítményértékelés, az érdemjegy megszerzésének feltétele: Gyakorlati feladat bemutatás és megvédése | | |