KIBERBIZTONSÁGI MESTERKÉPZÉSI SZAK

1. A mesterképzési szak megnevezése: kiberbiztonsági (Cyber Security)

2. A mesterképzési szakon szerezhető végzettségi szint és a szakképzettség oklevélben szereplő megjelölése

- végzettségi szint: mester- (magister, master; rövidítve: MA-) fokozat
- szakképzettség: okleveles kiberbiztonsági szakértő
- a szakképzettség angol nyelvű megjelölése: Cyber Security Expert

3. Képzési terület, az NKE tv. 3. §-ában meghatározott felsőoktatási terület: államtudományi, államtudományi és közigazgatási

4. A mesterképzésbe történő belépésnél előzményként elfogadott szakok

4.1. Teljes kreditérték beszámításával vehető figyelembe: -

4.2. A 9.4. pontban meghatározott kreditek teljesítésével elsősorban számításba vehető: az államtudományi osztatlan mesterképzési szak, a bűnügyi igazgatási, a gazdaságinformatikus, a had- és biztonságtechnikai mérnöki, a katasztrófavédelem, a katonai gazdálkodási, a katonai logisztika, a katonai üzemeltetés, a katonai vezetői, a közigazgatás- szervező, a mérnök informatikus, a nemzetbiztonsági, a nemzetközi biztonság- és védelempolitikai, a biztonság- és védelempolitikai, a nemzetközi igazgatási, a polgári nemzetbiztonsági, a programtervező informatikus és a rendészeti igazgatási alapképzési szak.

4.3. A 9.4. pontban meghatározott kreditek teljesítésével vehetők figyelembe továbbá azok az alapképzési és mesterképzési szakok, illetve a felsőoktatásról szóló 1993. évi LXXX. törvény szerinti szakok, amelyeket a kredit megállapításának alapjául szolgáló ismeretek összevetése alapján a felsőoktatási intézmény kreditátviteli bizottsága elfogad.

5. A képzési idő félévekben: 4 félév

6. A mesterfokozat megszerzéséhez összegyűjtendő kreditek száma: 120 kredit

- a szak orientációja: kiegyensúlyozott (40-60 százalék)
- a diplomamunka készítéséhez rendelt kreditérték: 20 kredit
- a szabadon választható tantárgyakhoz rendelhető minimális kreditérték: 10 kredit

7. A szakképzettség képzési területek egységes osztályozási rendszere szerinti tanulmányi területi besorolása:

0312

8. A mesterképzési szak képzési célja és a szakmai kompetenciák

A képzés célja olyan felsőfokú végzettséggel rendelkező szakemberek felkészítése, akik a közigazgatás, a védelmi igazgatás, a külügyi igazgatás területeihez tartozó szervezeteknél vezetői és szakértői munkakörökben képesek a kiberbiztonsági feladatok tervezését, szervezését és irányítását eredményesen végrehajtani. A mesterképzés azokra a kiberbiztonsági kérdésekre, aktuális és jövőbeli kihívásokra fókuszál, amelyekkel az állami és a magánszférának, illetve a társadalomnak egyaránt szembe kell néznie. A hallgatók széles körű ismereteket szereznek a

kiberbiztonság elméleti és gyakorlati oldaláról, biztonsági, környezeti, társadalmi és gazdasági aspektusairól. A differenciált szakmai tananyag elsajátítása során (nemzetközi kapcsolatok a kiberbiztonságban, közszolgálati kiberbiztonság-menedzsment, létfontosságú elektronikus információs rendszerek védelme) alkalmassá válnak szakterületüknek megfelelően kutatási, fejlesztési és tervezési feladatok ellátására, védelmi problémakörök tudományos igényű elemzésére és következtetések kialakítására.

8.1. Az elsajátítandó szakmai kompetenciák

8.1.1. Az okleveles kiberbiztonsági szakértő

***a)* tudása**

- Ismeri azokat a fontosabb előírásokat a szabályozásokból, amelyek a mindennapi munkáját befolyásolják.
- Ismeri a nemzetközi jog alkalmazhatóságát a kibertérben.
- Átlátja, hogy milyen védelmi megoldások vannak a kibertámadás ellen.
- Ismeri a kibertámadás esetén alkalmazandó eljárásokat.
- Ismeri a létfontosságú rendszerelemek fogalmát.
- Átlátja a munkáltatók által meghatározott belső szabályzatok megalkotásának szükségességét az információs rendszerekben tárolt adatok sértetlensége és a rendelkezésre állás tekintetében.
- Tisztában van a nyomozóhatóság feladataival az egyes állami szervezetek, vállalatok és intézményeket érő támadások esetén.
- Átlátja a kibertérrel kapcsolatos diplomáciai, illetve politikai információmegosztás folyamatát, valamint az esetleges válaszlépéseket.
- Tisztában van az információmegosztás folyamatával bűncselekmény felmerülése esetén.
- Ismeri a fedett környezetből történő információgyűjtés eljárásait.
- Tisztában van az emberi tényező szerepével a kibertámadások kivitelezése során.
- Ismeri a kártékony kódok fogalmát és hatásmechanizmusát.
- Tisztában van az állami kibervédelmi rendszerrel.
- Megérti a szervezeti feladatokat a kibervédelemben.

***b)* képességei**

- Képes értelmezni a jogszabályokból eredő követelményeket.
- Képes megszerezni a szervezet vezetőinek támogatását a jogszabályi megfelelőség kiépítéséhez.
- Képes átlátni a kibertér speciális jogállását.
- Képes a szükséges mértékben alkalmazni a kibertérre vonatkozó nemzetközi jogot kibertámadások esetén.
- Képes olyan védelmi intézkedések meghozatalára, amelyek segítik a humán fenyegetettségből eredő kockázatok csökkentését.
- Képes olyan technológiai védelmi intézkedések meghozatalára, amelyek a cyber kill chain egyes elemeihez kapcsolódnak.
- Képes felmérni a belső munkavállalók jelentette kiberbiztonsági kockázatokat.
- Képes olyan szabályzatok alkotására, amelyek a belső munkavállalók jelentette fenyegetések kezelésére vonatkoznak.
- Képes együttműködni a nyomozóhatósággal a kiberbiztonsági eseményeket érintő nyomozások során.

- Képes a szervezeténél keletkezett információkat oly módon megosztani külső szereplővel, hogy az ne sértse saját szervezetének érdekét, de hatékonyan tudja támogatni a külső felet.
- Képes a keletkezett információk megosztásának szükségességével kapcsolatban komplex következtetések levonására.
- Képes átlátni a kibertér aktuális fenyegetéseit.
- Képes támogatni szervezetét a kibervédelmi képességek kialakításában.
- Képes megfelelően támogatni szervezetét és a külső feleket egy kibertámadás kezelésében.

***c)* attitűdje**

- Munkája során figyelembe veszi és alkalmazza a kiberbiztonsággal kapcsolatos jogszabályokat.
- Megérti és elfogadja a nemzetközi kiberjog komplexitását, ennek köszönhetően a munkája során törekszik ennek a komplexitásnak a kezelésére.
- A maga komplexitásában tervezi meg az információbiztonsági irányítási rendszert.
- Hatékony lépéseket tesz a kibertámadások megelőzése érdekében, így csökkentve a szervezete kitettségét.
- Kiemelt kockázatként kezeli a belső munkavállalókat, és ennek megfelelően tervezi meg az információbiztonsági folyamatokat.
- Szükség esetén támogatja a külső feleket a szervezeténél keletkezett információk megosztásával.
- Partner abban, hogy se a szervezete, se ő maga ne váljon kibertámadás áldozatává.

***d)* autonómiája és felelőssége**

- Tudatosan törekszik a kiberbiztonság sajátosságainak megfelelő, korszerű ismeretek hazai és nemzetközi szinten történő gyakorlati alkalmazására.
- Önállóan dolgozza fel az új és összetett információkat, problémákat, illetve jelenségeket rendszerszerű és kritikus módon.
- Kezdeményező módon lép fel az alternatív, eredeti megoldások kidolgozásában, bemutatásában és a bonyolult, nem tipikus helyzetekben történő adekvát döntések meghozatalában.
- Vállalja a szakterület, a szakmai praxis módszertanának fejlesztéséhez szükséges elméleti, tudományos kutatási és gyakorlati információk beszerzésének, értékelésének és hasznosításának végrehajtását.
- Felelősséget vállal a kiberbiztonság összefüggő ismeretének és a meghatározó jogi, szabályozási és gazdasági összefüggések ismeretének alapján a szakmai javaslatok kidolgozásában.
- Értékkötelezett módon vesz részt a kibertér komplexitásának és kölcsönhatásainak ismerete által a különböző hivatásrendek feladatainak szervezésében.
- Önállóan és pontosan vesz részt a kiberbiztonsági fenyegetések technológiai, politikai és adminisztratív megoldásában.
- Vállalja a kiberbiztonsági fenyegetések kezelésének felelősségét.
- Kezdeményezőként dolgozik a technikai és operatív teendők stratégiai célokká való konvertálásában.
- Gyakorlatába beépíti és alkalmazza az e szakterületen folyó kutatások eredményeit.

9. A mesterképzés jellemzői

9.1. Szakmai jellemzők

9.1.1. A szakképzettséghez vezető tudományágak, szakterületek, amelyekből a szak felépül

- államtudományi, jogi és közigazgatás-szervezési ismeretek (jogi és közigazgatási ismeretek, a magyar közigazgatás szervezeteinek és szakigazgatási rendszereinek működése, közmenedzsment, elektronikus közszolgáltatások, kiberbiztonsági szabályozások és szabványok, adatvédelem, adatbiztonság) 10-15 kredit,
- információbiztonsági és biztonságszervezési ismeretek (kockázatértékelés, kockázatmenedzsment, Irányítási rendszerek, kiberbiztonsági stratégia és vezetés, információs rendszerek és hálózatok biztonsága, biztonságtechnika, incidensmenedzsment) 25-30 kredit,
- nemzetközi tanulmányok és biztonságpolitikai ismeretek (biztonságpolitika, kiberdiplomácia, a kibertér aktorai) 10-15 kredit,
- rendészeti szakismeretek (kiberbűnözés, hírszerzés a kibertérben, digitális nyomrögzítés) 10-15 kredit,
- alkalmazott infokommunikációs szakismeretek (adatbányászat, biztonsági technológiák alkalmazása, kriptográfia a közszolgálatban, biztonsági tesztelés) 10-15 kredit,
- katonai és védelmi szakismeretek (kiberhadviselés, létfontosságú rendszerek védelme) 10-15 kredit,
- vezetési és kommunikációs szakismeretek (vezetéselmélet, válságmenedzsment és kommunikáció, a kiberbiztonság pszichológiai aspektusai, a kiberbiztonság humán tényezői) 10-15 kredit.

9.2. *

9.3. A szakmai gyakorlat követelményei

A szakmai gyakorlat kritériumkövetelmény, amelynek időtartama - egybefüggően - legalább 10 hét, amelyet kifejezetten kiberbiztonsággal foglalkozó szakmai környezetben kell a hallgatónak teljesítenie. A szakmai gyakorlat részletes követelményeit a szak tanterve határozza meg.

9.4. A 4.2. és 4.3. pontban megadott oklevéllel rendelkezők esetén a mesterképzési képzési ciklusba való belépés minimális feltételei

A mesterképzésbe való belépéshez a korábbi tanulmányokból szükséges minimális kreditek száma 60 kredit az alábbi területekről:

- informatikai ismeretek (30 kredit): a szoftvertechnológia, a rendszertechnika és az adatbázisok és információs rendszerek ismeretkörei, kriptográfia alkalmazása, számítógépek architektúrája és számítógépes hálózatok témakörei;
- államtudományi és társadalomtudományi ismeretek (30 kredit): közigazgatási jog, alkotmányjog, büntetőjog, közigazgatási büntetőjog, közigazgatási rendtartás, alkotmány- és jogtörténet, európai közjog, nemzetközi jog, államtan, közgazdaságtan, szociológia, politológia, pszichológia, vezetés- és szervezéselmélet.

A mesterképzésbe való felvétel feltétele, hogy a felsorolt ismeretkörökben legalább 30 kredittel rendelkezzen a jelentkező. A hiányzó krediteket a mesterfokozat megszerzésére irányuló képzéssel párhuzamosan, a felsőoktatási intézmény tanulmányi és vizsgaszabályzatában meghatározottak szerint meg kell szerezni.