KIBERBIZTONSÁGI MESTERKÉPZÉSI SZAK

A) A szak alapadatai

1. A mesterképzési szak megnevezése:
a) magyar nyelven: kiberbiztonsági mesterképzési szak
b) angol nyelven: Cyber Security master programme

2. A mesterképzési szak szakirányai: -

3. A mesterképzési szakon szerezhető szakképzettség oklevélben szereplő megnevezése:
a) magyar nyelven: okleveles kiberbiztonsági szakértő
b) angol nyelven: Cyber Security Expert

4. A mesterképzési szak profilja:
4.1. képzési terület szerinti besorolása: államtudományi képzési terület, államtudományi és közigazgatási felsőoktatás
4.2. a végzettségi szint besorolása:
a) mesterfokozat (magister, master of arts, rövidítve: MA)
b) ISCED 2011 szerint: 767
c) Magyar Képesítési Keretrendszer/Európai Képesítési Keretrendszer szerint: 7
4.3. a szakképzettség képzési területek egységes osztályozási rendszere szerinti tanulmányi területi besorolása ISCED–F 2013 szerint: 0312
4.4. a szak orientációja: kiegyensúlyozott (40–60 százalék)

B) A képzés szerkezeti és kimeneti jellemzői

5. A képzési idő félévekben: 4 félév

6. A mesterfokozat megszerzéséhez összegyűjtendő kreditek száma: 120 kredit
6.1.[1] A szakdolgozat vagy diplomamunka elkészítéséhez rendelt kreditek száma: 20 kredit
6.2. Szakmai gyakorlati képzéshez rendelt kreditek száma: -
6.3. A szakirány elvégzésével összegyűjtendő kreditek minimális száma: -

7. A mesterképzési szak képzési célja, a szakmai kompetenciák leírása:
7.1.[2] A képzés célja: 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, kritikus elektronikus információs rendszerek védelme) alkalmassá válnak szakterületüknek megfelelően kutatási, fejlesztési és tervezési feladatok ellátására, védelmi problémakörök tudományos igényű elemzésére és következtetések kialakítására.

---

[1] Módosította: 151/2025. (VI. 19.) Korm. rendelet 5. § 57.
[2] Módosította: 474/2024. (XII. 31.) Korm. rendelet 172. § d).

7.2. Az elsajátítandó szakmai kompetenciák:

7.2.1.[3] Tudás:

– Ismeri azokat a fontosabb előírásokat a kiberbiztonsággal kapcsolatos hazai és nemzetközi 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 kritikus szervezetek, kritikus infrastruktúrák, valamint az ország védelme és biztonsága szempontjából jelentős szervezetek, az ország védelme és biztonsága szempontjából jelentős infrastruktúrák 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.

7.2.2. Képesség:

– 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.

7.2.3. Attitűd:

– Megérti és elfogadja a nemzetközi kiberjog komplexitását, ennek köszönhetően a munkája

[3] Módosította: 474/2024. (XII. 31.) Korm. rendelet 172. § e).

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.

7.2.4. Autonómia és felelősség:

– Tudatosan törekszik a kiberbiztonság sajátosságainak megfelelő, korszerű ismeretek hazai és nemzetközi szinten történő gyakorlati alkalmazására.

– 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 a kiberbiztonsági szakterületen folyó kutatások eredményeit.

7.3. Az elsajátítandó szakirányú kompetenciák: -

C) A képzés további jellemzői

8. A mesterképzés jellemzői:

8.1. Idegennyelvi követelmény: A jelentkezéshez és a felvételhez szükséges idegennyelvi követelményt a Nemzeti Közszolgálati Egyetemről, valamint a közigazgatási, rendészeti és katonai felsőoktatásról szóló 2011. évi CXXXII. törvény felhatalmazása alapján kiadott jogszabály határozhat meg.

8.2. A szak speciális képzésszervezési, módszertani jellemzői:

8.2.1. Szakmai gyakorlatra vonatkozó követelmények: -

8.2.2. Munkarend: -

8.2.3. Idegen nyelven folyó képzés: -

8.2.4. Egyéb: -