NEMZETKÖZI KIBERBIZTONSÁGI TANULMÁNYOK MESTERKÉPZÉSI SZAK

A) A szak alapadatai

1. A mesterképzési szak megnevezése:
a) magyar nyelven: nemzetközi kiberbiztonsági tanulmányok
b) angol nyelven: International Cybersecurity Studies master programme

2. A mesterképzési szak szakirányai: -

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

4. A mesterképzési szak profilja:
4.1. képzési terület szerinti besorolása: államtudományi képzési terület, nemzetközi és európai közszolgálati 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: kiemelten elméletorientált (70–80 százalék)

B) A képzés szerkezeti és kimeneti jellemzői

5. A képzési idő félévekben: 2 félév

6. A mesterfokozat megszerzéséhez összegyűjtendő kreditek száma: 60 kredit
6.1. A szakdolgozathoz vagy diplomamunka elkészítéséhez rendelt kreditek száma: 5 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. A képzés célja: A képzés célja olyan felsőfokú végzettséggel rendelkező szakemberek felkészítése, akik a hazai és külföldi állami és nemzetközi szervezeteknél, gazdasági társaságoknál 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 alkalmassá válnak szakterületüknek megfelelően kutatási, fejlesztési és tervezési feladatok ellátására, védelmi problémakörök tudományos igényű elemzésére és következtetések kialakítására.

A képzés a European Cybersecurity Skills Framework szerinti Chief Information Security Officer (CISO), Cyber Legal, Policy & Compliance Officer, és Cybersecurity Risk Manager szerepkörök betöltésére képesít.

[The aim of the training is to prepare professionals with higher education qualifications who are

able to effectively plan, organise and manage cybersecurity tasks in managerial and expert positions in domestic and foreign public and international organisations and companies. The Master's programme focuses on the cybersecurity issues, current and future challenges facing both the public and private sectors and society. Students will acquire a broad knowledge of the theoretical and practical aspects of cybersecurity, its security, environmental, social and economic aspects. The differentiated professional curriculum will enable them to carry out research, development and planning tasks in their area of expertise, to analyse security problems in a scientific manner and to draw conclusions.

The training will qualify the student for the roles of Chief Information Security Officer (CISO), Cyber Legal, Policy & Compliance Officer, and Cybersecurity Risk Manager, as defined in the European Cybersecurity Skills Framework.]

7.2. Az elsajátítandó szakmai kompetenciák:

7.2.1. Tudás:

– Ismeri a kiberbiztonsági politikákat. (Is familiar with cybersecurity policies.)

– Ismeri a kiberbiztonsági szabványokat, módszertanokat és keretrendszereket. (Is familiar with cybersecurity standards, methodologies and frameworks.)

– Ismeri a kiberbiztonsági ajánlásokat és jó gyakorlatokat. (Is familiar with cybersecurity recommendations and best practices.)

– Ismeri a kiberbiztonsági joganyagot. (Is familiar with cybersecurity related laws, regulations and legislations.)

– Ismeri a kiberbiztonsági tanúsítványokat. (Is familiar with cybersecurity-related certifications.)

– Ismeri az etikus kiberbiztonsági szervezeti követelményeket. (Is familiar with ethical cybersecurity organisation requirements.)

– Ismeri a kiberbiztonsági érettségi modelleket. (Is familiar with cybersecurity maturity models.)

– Ismeri a kibertámadás esetén alkalmazandó eljárásokat. (Is familiar with procedures in case of cyber attacks)

– Ismeri az erőforrás-menedzsmentet. (Is familiar with resource management.)

– Ismeri a menedzsment gyakorlatokat. (Is familiar with management practices.)

– Ismeri a kockázatmenedzsment szabványokat, módszertanokat és keretrendszereket. (Is familiar with risk management standards, methodologies and frameworks.)

– Ismeri a jogi, szabályozási és jogszabályi megfelelési követelményeket, ajánlásokat és legjobb gyakorlatokat. (Is familiar with legal, regulatory and legislative compliance requirements, recommendations and best practices.)

– Ismeri az adatvédelmi hatásvizsgálati szabványokat, módszertanokat és keretrendszereket. (Is familiar with privacy impact assessment standards, methodologies and frameworks.)

– Ismeri a kockázatkezelési eszközöket. (Is familiar with risk management tools)

– Ismeri a kockázatkezelési ajánlásokat és jó gyakorlatokat. (Is familiar with risk management recommendations and best practices.)

– Ismeri a kiberfenyegetéseket. (Is familiar with cyber threats.)

– Ismeri a számítógépes rendszerek sebezhetőségeit. (Is familiar with computer systems vulnerabilities.)

– Ismeri a kiberbiztonsági kontrollokat és megoldásokat. (Is familiar with cybersecurity controls and solutions.)

– Ismeri a kiberbiztonsági kockázatokat. (Is familiar with cybersecurity risks.)

– Ismeri a kiberbiztonsági kontrollok hatékonyságának nyomon követését, tesztelését és értékelését. (Is familiar with monitoring, testing and evaluating cybersecurity controls' effectiveness.)

– Ismeri a kiberbiztonsággal kapcsolatos technológiákat. (Is familiar with cybersecurity-related technologies.)

7.2.2. Képesség:

– Képes a szervezet kiberbiztonsági helyzetének értékelésére és javítására. (Is capable of assessing and enhancing an organisation's cybersecurity posture.)

– Képes a kiberbiztonsági irányelvek, tanúsítványok, szabványok, módszertanok és keretrendszerek elemzésére és végrehajtására. (Is capable of analysing and implementing cybersecurity policies, certifications, standards, methodologies and frameworks.)

– Képes a kiberbiztonsággal kapcsolatos törvények, rendeletek és egyéb jogszabályok elemzésére és betartására. (Is capable of analysingand complying with cybersecurity-related laws, regulations and legislations.)

– Képes a kiberbiztonsági ajánlások és jó gyakorlatok végrehajtására. (Is capable of implementing cybersecurity recommendations and best practices.)

– Képes a kiberbiztonsági erőforrások kezelésére. (Is capable of managing cybersecurity resources.)

– Képes a kiberbiztonsági stratégia kidolgozására, támogatására és végrehajtásának irányítására. (Is capable of developing, championing and leading the execution of a cybersecurity strategy.)

– Képes az Információbiztonsági irányítási rendszer (ISMS) kialakítására, alkalmazására, ellenőrzésére és felülvizsgálatára vagy közvetlenül, vagy annak kiszervezésének irányításával. (Is capable of designing, applying, monitoring and reviewing Information Security Management System (ISMS) either directly or by leading its outsourcing.)

– Képes a biztonsági dokumentumok, jelentések, SLA-k felülvizsgálatára és javítására, valamint a biztonsági célkitűzések biztosítására. (Is capable of reviewing and enhancing security documents, reports, SLAs and ensure the security objectives.)

– Képes a kiberbiztonsággal kapcsolatos problémák azonosítására és megoldására. (Is capable of identifying and solving cybersecurity-related issues.)

– Képes a kiberbiztonsági terv kidolgozására. (Is capable of establishing a cybersecurity plan).

– Képes a szervezet információbiztonsági stratégiája szükséges módosításainak előrejelzésére és új tervek kidolgozására. (Is capable of anticipating required changes to the organisation’s information security strategy and formulate new plans.)

– Képes a kiberbiztonsági irányítás érettségi modelljeinek meghatározására és alkalmazására. (Is capable of defining and applying maturity models for cybersecurity management.)

– Képes a kiberbiztonsági fenyegetések, igények és közelgő kihívások előrejelzése. (Is capable of anticipating cybersecurity threats, needs and upcoming challenges.)

– Képes az üzleti stratégia, modellek és termékek átfogó megértésére és a jogi, szabályozási és szabványkövetelmények figyelembevételére. (Is capable of comprehensive understanding of the business strategy, models and products and is able to factor into legal, regulatory and standards’ requirements.)

– Képes a szervezeti folyamatok, a pénzügyi és az üzleti stratégia megvalósításával kapcsolatos adatvédelmi kérdések gyakorlati megvalósítására. (Is capable of carrying out working-life practices of the data protection and privacy issues involved in the implementation of the organisational processes, finance and business strategy.)

– Képes az üzleti igényeket és a jogi követelményeket kiegészítő megfelelő kiberbiztonsági és adatvédelmi irányelvek és eljárások kidolgozásának vezetésére; továbbá annak elfogadásának, megértésének és végrehajtásának biztosítására, valamint kommunikálására az érintett felek között. (Is capable of leading the development of appropriate cybersecurity and privacy policies and procedures that complement the business needs and legal requirements; further of ensuring its acceptance, comprehension and implementation and communicate it between the involved parties.)

– Képes az adatvédelmi hatásvizsgálatok elvégzésére, nyomon követésére és felülvizsgálatára szabványok, keretrendszerek, elismert módszerek és eszközök felhasználásával. (Is capable of conducting, monitoring and reviewing privacy impact assessments using standards, frameworks, acknowledged methodologies and tools.)

– Képes adatvédelmi és adatvédelemmel kapcsolatos témák ismertetésére és kommunikálására az érdekelt felek és a felhasználók felé. (Is capable of explaining and communicating data protection and privacy topics to stakeholders and users.)

– Képes a jogi keretrendszer változásának a szervezet kiberbiztonsági és adatvédelmi stratégiájára

és politikáira gyakorolt hatásainak megértésére. (Is capable of understanding legal framework modifications implications to the organisation’s cybersecurity and data protection strategy and policies.)

– Képes a kiberbiztonsági kockázatkezelési keretrendszerek, módszertanok és iránymutatások végrehajtására, valamint a szabályozásoknak és szabványoknak való megfelelés biztosítására. (Is capable of implementing cybersecurity risk management frameworks, methodologies and guidelines and ensuring compliance with regulations and standards.)

– Képes a szervezet minőség- és kockázatkezelési gyakorlatának elemzésére és konszolidálására. (Is capable of analysing and consolidating organisation’s quality and risk management practices.)

– Képes a kiberbiztonsági kockázattudatos környezet kialakítására. (Is capable of building a cybersecurity risk-aware environment.)

7.2.3. Attitűd:

– Befolyásolja a szervezet kiberbiztonsági kultúráját. (Influence an organisation’s cybersecurity culture.)

– Érti, gyakorolja és betartja az etikai követelményeket és szabványokat. (Understand, practice and adhere to ethical requirements and standards.)

7.2.4. Autonómia és felelősség:

– Lehetővé teszi az üzleti eszközök tulajdonosai, a vezetők és más érdekeltek számára, hogy kockázati információkkal alátámasztottan döntsenek a kockázatok kezelése és mérséklése érdekében. (Enable business assets owners, executives and other stakeholders to make risk-informed decisions to manage and mitigate risks.)

– Kommunikál, prezentál és jelent a megfelelő érdekelt felek felé. (Communicate, present and report to relevant stakeholders.)

– Kommunikál, koordinál és együttműködik a belső és külső érdekelt felekkel. (Communicate, coordinate and cooperate with internal and external stakeholders.)

– Kockázatmegosztási lehetőségeket javasol és kezel. (Propose and manage risk-sharing options.)

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: A képzés angol nyelven folyik.

8.2.4. Egyéb: -

---->>----->>--<<-----<<----