MAGYARORSZÁG KORMÁNYA

Közli: Magyar Közlöny

A K O R M Á N Y

----

rendelete

az államtudományi képzési területen szerezhető képesítések jegyzékéről és a képzések képzési és kimeneti követelményeiről szóló 222/2019. (IX. 25.) Korm. rendelet módosításáról

A Kormány a Nemzeti Közszolgálati Egyetemről, valamint a közigazgatási, rendészeti és katonai felsőoktatásról szóló 2011. évi CXXXII. törvény 44. § (1) bekezdés e) pontjában kapott felhatalmazás alapján, az Alaptörvény 15. cikk (1) bekezdésében meghatározott feladatkörében eljárva a következőket rendeli el:

1. §

Az államtudományi képzési területen szerezhető képesítések jegyzékéről és a képzések képzési és kimeneti követelményeiről szóló 222/2019. (IX. 25.) Korm. rendelet (a továbbiakban: R.) 9. §-a a következő (11) és (12) bekezdéssel egészül ki:

„(11) A 2. és 3. mellékletnek az államtudományi képzési területen szerezhető képesítések jegyzékéről és a képzések képzési és kimeneti követelményeiről szóló 222/2019. (IX. 25.) Korm. rendelet módosításáról szóló …/2023. (… …) Korm. rendelettel (a továbbiakban: MódR2.) módosított rendelkezéseit – a (12) bekezdésben foglalt kivétellel – a tanulmányaikat a 2022/2023. tanévben vagy azt követően megkezdő hallgatókra kell alkalmazni, illetve hatályon kívül helyezett rendelkezéseit a tanulmányaikat a 2022/2023. tanévben megkezdő hallgatókra sem kell alkalmazni.

(12) E rendeletnek a MódR2. által megállapított 3. melléklet „MESTERKÉPZÉSEK ÉS MESTERKÉPZÉSBEN, OSZTATLAN KÉPZÉSBEN SZEREZHETŐ SZAKKÉPZETTSÉGEK JEGYZÉKE” című fejezetben foglalt táblázat 21. sorát és 3. melléklet „A MESTERKÉPZÉSI SZAKOK KÉPZÉSI ÉS KIMENETI KÖVETELEMÉNYEI” című fejezet 20. alcímét a tanulmányaikat a 2024/2025. tanévben vagy azt követően megkezdő hallgatókra kell alkalmazni.”

2. §

(1) Az R. 2. melléklete az 1. melléklet szerint módosul.

(2) Az R. 3. melléklete a 2. melléklet szerint módosul.

3. §

Hatályát veszti az R.

1. 2. melléklet „AZ ALAPKÉPZÉSI SZAKOK KÉPZÉSI ÉS KIMENETI KÖVETELMÉNYEI” című fejezet
   - 1.1. 1. alcím 8. pont 8.2. alpontja,
   - 1.2. 2. alcím 8. pont 8.2. alpontja,
   - 1.3. 3. alcím 8. pont 8.2. alpontja,
   - 1.4. 4. alcím 8. pont 8.2. alpontja,
   - 1.5. 5. alcím 8. pont 8.2. alpontja,
   - 1.6. 6. alcím 8. pont 8.2. alpontja,
   - 1.7. 7. alcím 8. pont 8.2. alpontja,
   - 1.8. 8. alcím 8. pont 8.2. alpontja,
   - 1.9. 9. alcím 8. pont 8.2. alpontja,
   - 1.10. 10. alcím 8. pont 8.2. alpontja,
   - 1.11. 11. alcím 8. pont 8.2. alpontja,
   - 1.12. 12. alcím 8. pont 8.2. alpontja,
   - 1.13. 13. alcím 8. pont 8.2. alpontja,
   - 1.14. 14. alcím 8. pont 8.2. alpontja,
   - 1.15. 15. alcím 8. pont 8.2. alpontja,
2. 3. melléklet „A MESTERKÉPZÉSI SZAKOK KÉPZÉSI ÉS KIMENETI KÖVETELEMÉNYEI” című fejezet
   - 2.1. 1. alcím 8. pont 8.2. alpontja,
   - 2.2. 2. alcím 9. pont 9.2. alpontja,
   - 2.3. 3. alcím 9. pont 9.2. alpontja,
   - 2.4. 4. alcím 9. pont 9.2. alpontja,
   - 2.5. 5. alcím 9. pont 9.2. alpontja,
   - 2.6. 6. alcím 9. pont 9.2. alpontja,
   - 2.7. 7. alcím 9. pont 9.2. alpontja,
   - 2.8. 8. alcím 9. pont 9.2. alpontja,
   - 2.9. 9. alcím 9. pont 9.2. alpontja,
   - 2.10. 10. alcím 9. pont 9.2. alpontja,
   - 2.11. 11. alcím 9. pont 9.2. alpontja,
   - 2.12. 12. alcím 9. pont 9.2. alpontja,
   - 2.13. 13. alcím 9. pont 9.2. alpontja,
   - 2.14. 14. alcím 9. pont 9.2. alpontja,
   - 2.15. 15. alcím 9. pont 9.2. alpontja,
   - 2.16. 16. alcím 9. pont 9.2. alpontja,
   - 2.17. 17. alcím 9. pont 9.2. alpontja,
   - 2.18. 18. alcím 9. pont 9.2. alpontja.

4. §

Ez a rendelet a kihirdetését követő napon lép hatályba.

(Orbán Viktor)
miniszterelnök

1. melléklet a .../2023 ( ) Korm. rendelethez

1. Az R. 2. melléklet 9. alcím 8. pontja a következő 8.4. alponttal egészül ki:

„**8.4. A képzést megkülönböztető speciális jegyek**: Az alapképzésben a szakképzettséghez angol nyelvből középszintű STANAG katonai szaknyelvi tudást kell elérni.”

2. Az R. 2. melléklet 10. alcím 8. pontja a következő 8.4. alponttal egészül ki:

„**8.4. A képzést megkülönböztető speciális jegyek**: Az alapképzésben a szakképzettséghez angol nyelvből középszintű STANAG katonai szaknyelvi tudást kell elérni.”

3. Az R. 2. melléklet 11. alcím 8. pontja a következő 8.4. alponttal egészül ki:

„**8.4. A képzést megkülönböztető speciális jegyek**: Az alapképzésben a szakképzettséghez angol nyelvből középszintű STANAG katonai szaknyelvi tudást kell elérni.”

4. Az R. 2. melléklet 12. alcím 8. pontja a következő 8.4. alponttal egészül ki:

„**8.4. A képzést megkülönböztető speciális jegyek**: Az alapképzésben a szakképzettséghez angol nyelvből középszintű STANAG katonai szaknyelvi tudást kell elérni.”

5. Az R. 2. melléklet 13. alcím 8. pontja a következő 8.4. alponttal egészül ki:

„**8.4. A képzést megkülönböztető speciális jegyek**: Az alapképzésben a szakképzettséghez angol nyelvből középszintű STANAG katonai szaknyelvi tudást kell elérni. Az állami légijármű-vezető és a katonai repülésirányító szakirányon a szakképzettséghez továbbá angol nyelvből legalább négyes szintű ICAO repülés-szakmai szaknyelvi tudást kell elérni.”

2. melléklet a .../2023 ( ) Korm. rendelethez

1. Az R. 3. melléklet „MESTERKÉPZÉSEK ÉS MESTERKÉPZÉSBEN, OSZTATLAN KÉPZÉSBEN SZEREZHETŐ SZAKKÉPZETTSÉGEK JEGYZÉKE” című fejezetben foglalt táblázat a következő 21. sorral egészül ki:

	(A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*
1.	*Képzési terület*	*Képzési terület angol nyelvű megneve-zése*	*Felsőoktatá-si terület*	*Felsőok-tatási terület angol nyelvű megneve-zése*	*Mester-képzési szak*	*Osztat-lan szak*	*Mesterképzés i szak, osztatlan szak angol nyelvű megnevezése*	*Szak-képzettség*	*Mesterképzés-ben szerezhető szakképzettség angol nyelvű megnevezése*	*EKKR és MKKR szint)*

”

21.	állam-tudomá nyi	Political Science and Public Governance	nemzet-közi és európai közszolgá -lati	Political Science and Public Governance	International Cybersecurity Studies	-	International Cybersecurity Studies	International Cybersecurity Expert	International Cybersecurit y Expert	7

”

2. Az R. 3. melléklet „A MESTERKÉPZÉSI SZAKOK KÉPZÉSI ÉS KIMENETI KÖVETELEMÉNYEI” című fejezet 6. alcím 9. pont 9.5. alpontja helyébe a következő rendelkezés lép:

„**9.5. A képzést megkülönböztető speciális jegyek (Die Besonderheiten der Ausbildung)**: A képzés kizárólag német nyelven folyik.”

3. Az R. 3. melléklet „A MESTERKÉPZÉSI SZAKOK KÉPZÉSI ÉS KIMENETI KÖVETELEMÉNYEI” című fejezete a következő 20. alcímmel egészül ki:

„20. INTERNATIONAL CYBERSECURITY STUDIES MESTERKÉPZÉSI SZAK

1. A mesterképzési szak megnevezése: International Cybersecurity Studies

2. A mesterképzési szakon szerezhető végzettségi szint és a szakképzettség oklevélben szereplő megjelölése
- végzettségi szint: mester- (magister, master; rövidítve: MA-) fokozat
- szakképzettség: International Cybersecurity Expert

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

4. A mesterképzésbe történő belépésnél előzményként elfogadott szakok
4.1. Teljes kreditérték beszámításával vehető figyelembe:

az államtudományi, jogi, gazdaságtudományi képzési területen, illetve az ezekhez besorolható, de már megszűnt vagy átalakult szakokon, illetve képzési ágakban szerzett egyetemi képzés vagy mesterképzési szak, illetve annak külföldi megfelelője.

4.2. A 9. pont 9.3. alpontjában meghatározott kreditek teljesítésével elsősorban számításba vehető: a gazdaságinformatikus, a mérnökinformatikus, a programtervező informatikus, az autonómrendszer-informatikus, a védelmi infokommunikációs rendszertervező és a villamosmérnöki mesterszakok.

4.3. A 9. pont 9.3. alpontjában 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: 2 félév / 2 semesters

6. A mesterfokozat megszerzéséhez összegyűjtendő kreditek száma: 60 kredit / ECTS
- a szak orientációja: kiemelten elméletorientált (70-80 százalék)
- a diplomamunka készítéséhez rendelt kreditérték: 5 kredit
- a szabadon választható tantárgyakhoz rendelhető minimális kreditérték: 4 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 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.)

8.1. Az elsajátítandó szakmai kompetenciák

8.1.1. Az okleveles nemzetközi kiberbiztonsági szakértő / The International Cybersecurity Expert

a) tudása / knowledge

Ismeri / (is familiar with)

- a kiberbiztonsági politikákat (Cybersecurity policies),
- a kiberbiztonsági szabványokat, módszertanokat és keretrendszereket (Cybersecurity standards, methodologies and frameworks),
- a kiberbiztonsági ajánlásokat és jó gyakorlatokat (Cybersecurity recommendations and best practices),
- a kiberbiztonsági joganyagot (Cybersecurity related laws, regulations and legislations),
- a kiberbiztonsági tanúsítványokat (Cybersecurity-related certifications),
- Etikus kiberbiztonsági szervezeti követelményeket (Ethical cybersecurity organisation requirements),
- a kiberbiztonsági érettségi modelleket (Cybersecurity maturity models),
- a kiberbiztonsági eljárásokat (Cybersecurity procedures),
- az erőforrás-menedzsmentet (Resource management),
- a menedzsment gyakorlatokat (Management practices),
- a kockázatmenedzsment szabványokat, módszertanokat és keretrendszereket (Risk management standards, methodologies and frameworks),
- a jogi, szabályozási és jogszabályi megfelelési követelményeket, ajánlásokat és legjobb gyakorlatokat (Legal, regulatory and legislative compliance requirements, recommendations and best practices),
- az adatvédelmi hatásvizsgálati szabványokat, módszertanokat és keretrendszereket (Privacy impact assessment standards, methodologies and frameworks),
- a kockázatkezelési eszközöket (Risk management tools),
- a kockázatkezelési ajánlásokat és jó gyakorlatokat (Risk management recommendations and best practices),
- a kiberfenyegetéseket (Cyber threats),
- a számítógépes rendszerek sebezhetőségeit (Computer systems vulnerabilities),
- a kiberbiztonsági kontrollokat és megoldásokat (Cybersecurity controls and solutions),
- a kiberbiztonsági kockázatokat (Cybersecurity risks),
- a kiberbiztonsági kontrollok hatékonyságának nyomon követését, tesztelését és értékelését (Monitoring, testing and evaluating cybersecurity controls' effectiveness),
- a kiberbiztonsággal kapcsolatos technológiákat (Cybersecurity-related technologies).

b) képességei

Képes (Is capable of)

- a szervezet kiberbiztonsági helyzetének értékelésére és javítására (Assess and enhance an organisation’s cybersecurity posture),

- a kiberbiztonsági irányelvek, tanúsítványok, szabványok, módszertanok és keretrendszerek elemzésére és végrehajtására (Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks),
- a kiberbiztonsággal kapcsolatos törvények, rendeletek és egyéb jogszabályok elemzésére és betartására (Analyse and comply with cybersecurity-related laws, regulations and legislations),
- a kiberbiztonsági ajánlások és jó gyakorlatok végrehajtására (Implement cybersecurity recommendations and best practices),
- a kiberbiztonsági erőforrások kezelésére (Manage cybersecurity resources),
- a kiberbiztonsági stratégia kidolgozására, támogatására és végrehajtásának irányítására (Develop, champion and lead the execution of a cybersecurity strategy),
- az információbiztonsági irányítási rendszer (ISMS) kialakítására, alkalmazására, ellenőrzésére és felülvizsgálatára vagy közvetlenül, vagy annak kiszervezésének irányításával (Design, apply, monitor and review Information Security Management System (ISMS) either directly or by leading its outsourcing),
- a biztonsági dokumentumok, jelentések, SLA-k felülvizsgálatára és javítására, valamint a biztonsági célkitűzések biztosítására (Review and enhance security documents, reports, SLAs and ensure the security objectives),
- a kiberbiztonsággal kapcsolatos problémák azonosítására és megoldására (Identify and solve cybersecurity-related issues),
- a kiberbiztonsági terv kidolgozására (Establish a cybersecurity plan),
- a szervezet információbiztonsági stratégiája szükséges módosításainak előrejelzésére és új tervek kidolgozására (Anticipate required changes to the organisation's information security strategy and formulate new plans),
- a kiberbiztonsági irányítás érettségi modelljeinek meghatározására és alkalmazására (Define and apply maturity models for cybersecurity management),
- a kiberbiztonsági fenyegetések, igények és közelgő kihívások előrejelzése (Anticipate cybersecurity threats, needs and upcoming challenges),
- az üzleti stratégia, modellek és termékek átfogó megértésére és a jogi, szabályozási és szabványkövetelmények figyelembevételére (Comprehensive understanding of the business strategy, models and products and ability to factor into legal, regulatory and standards' requirements),
- a szervezeti folyamatok, a pénzügyi és az üzleti stratégia megvalósításával kapcsolatos adatvédelmi kérdések gyakorlati megvalósítására (Carry out working-life practices of the data protection and privacy issues involved in the implementation of the organisational processes, finance and business strategy),
- 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 (Lead the development of appropriate cybersecurity and privacy policies and procedures that complement the business needs and legal requirements; further ensure its acceptance, comprehension and implementation and communicate it between the involved parties),
- az adatvédelmi hatásvizsgálatok elvégzésére, nyomon követésére és felülvizsgálatára szabványok, keretrendszerek, elismert módszerek és eszközök felhasználásával (Conduct,

monitor and review privacy impact assessments using standards, frameworks, acknowledged methodologies and tools),
- az adatvédelmi és adatvédelemmel kapcsolatos témák ismertetésére és kommunikálására az érdekelt felek és a felhasználók felé (Explain and communicate data protection and privacy topics to stakeholders and users),
- a jogi keretrendszer változásának a szervezet kiberbiztonsági és adatvédelmi stratégiájára és politikáira gyakorolt hatásainak megértésére (Understand legal framework modifications implications to the organisation's cybersecurity and data protection strategy and policies),
- a kiberbiztonsági kockázatkezelési keretrendszerek, módszertanok és iránymutatások végrehajtására, valamint a szabályozásoknak és szabványoknak való megfelelés biztosítására (Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards),
- a szervezet minőség- és kockázatkezelési gyakorlatának elemzésére és konszolidálására (Analyse and consolidate organisation's quality and risk management practices),
- a kiberbiztonsági kockázattudatos környezet kialakítására (Build a cybersecurity risk-aware environment).

c) attitűdje / his/her personal attitude is characterized by

- befolyásolja a szervezet kiberbiztonsági kultúráját (Influence an organisation's cybersecurity culture),
- motiválja és bátorítja az embereket (Motivate and encourage people),
- érti, gyakorolja és betartja az etikai követelményeket és szabványokat (Understand, practice and adhere to ethical requirements and standards),
- együttműködik más csapattagokkal és kollégákkal (Collaborate with other team members and colleagues).

d) autonómiája és felelőssége / autonomy and responsibility

- 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).

9. A mesterképzés jellemzői

9.1. Szakmai jellemzők

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

- szakterületi jogi ismeretek 5-10 kredit,
- információbiztonsági ismeretek 10-20 kredit,
- nemzetközi tanulmányok, vezetési és kommunikációs szakismeretek 10-25 kredit,
- rendészeti, katonai és védelmi szakismeretek 10-25 kredit.

9.2. A szakmai gyakorlat követelményei

A szakmai gyakorlat kritériumkövetelményként előírható, amelynek időtartama – egybefüggően – legalább 4 hét, amelyet kifejezetten kiberbiztonsággal foglalkozó szakmai környezetben kell a hallgatónak teljesítenie. A szakmai gyakorlat részletes követelményeit a szak tanterve határozza meg.

(An internship may be required as a criterion requirement, the duration of which shall be at least 4 weeks consecutively, to be completed in a professional environment specifically dealing with cybersecurity. The detailed requirements for the internship are specified in the curriculum of the degree program.)

9.3. A 4. pont 4.2. és 4.3. alpontjában 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 (20 kredit): a szoftvertechnológia, a rendszertechnika és az adatbázisok és információs rendszerek ismeretkörei, kriptográfia alkalmazása, információbiztonság, számítógépek architektúrája és számítógépes hálózatok témakörei;
- államtudományi és társadalomtudományi ismeretek (40 kredit): közigazgatási jog, alkotmányjog, büntetőjog, közigazgatási büntetőjog, közigazgatási rendtartás, európai közjog, nemzetközi jog, államtan, közgazdaságtan, politológia, pszichológia, vezetés- és szervezéselmélet, adatvédelem.

A mesterképzésbe való felvétel feltétele, hogy a felsorolt ismeretkörökben legalább 50 kredittel rendelkezzen a jelentkező. A mesterképzésbe való belépéshez szükséges kreditekből 25 kredit munkatapasztalat vagy nem formális tanulás eredménye alapján is beszámítható. A hiányzó krediteket a mesterfokozat megszerzésére irányuló képzéssel párhuzamosan, a felsőoktatási intézmény tanulmányi és vizsgaszabályzatában meghatározottak szerint meg kell szerezni.

(The minimum number of credits required for entry to the Master's programme from previous studies is 60 credits in the following areas:

- computer science (20 credits): software engineering, systems engineering, database and information systems, application of cryptography, information security, computer architecture and computer networking;
- Public and social sciences (40 credits): administrative law, constitutional law, criminal law, administrative criminal law, administrative processes, administrative regulation, European public law, international law, public administration, economics, political science, psychology, management and organisation theory, data protection.

To be admitted to the Master's programme, applicants must have at least 50 credits in the subjects listed. Of the credits required for admission to the Master's programme, 25 credits may be acknowledged on the basis of work experience or non-formal learning outcomes. The missing credits must be acquired in parallel with the Master's degree course, as specified in the study and examination regulations of the higher education institution.)

9.4. A képzést megkülönböztető speciális jegyek

A képzés kizárólag angol nyelven folyik. (The program is conducted in English.)”