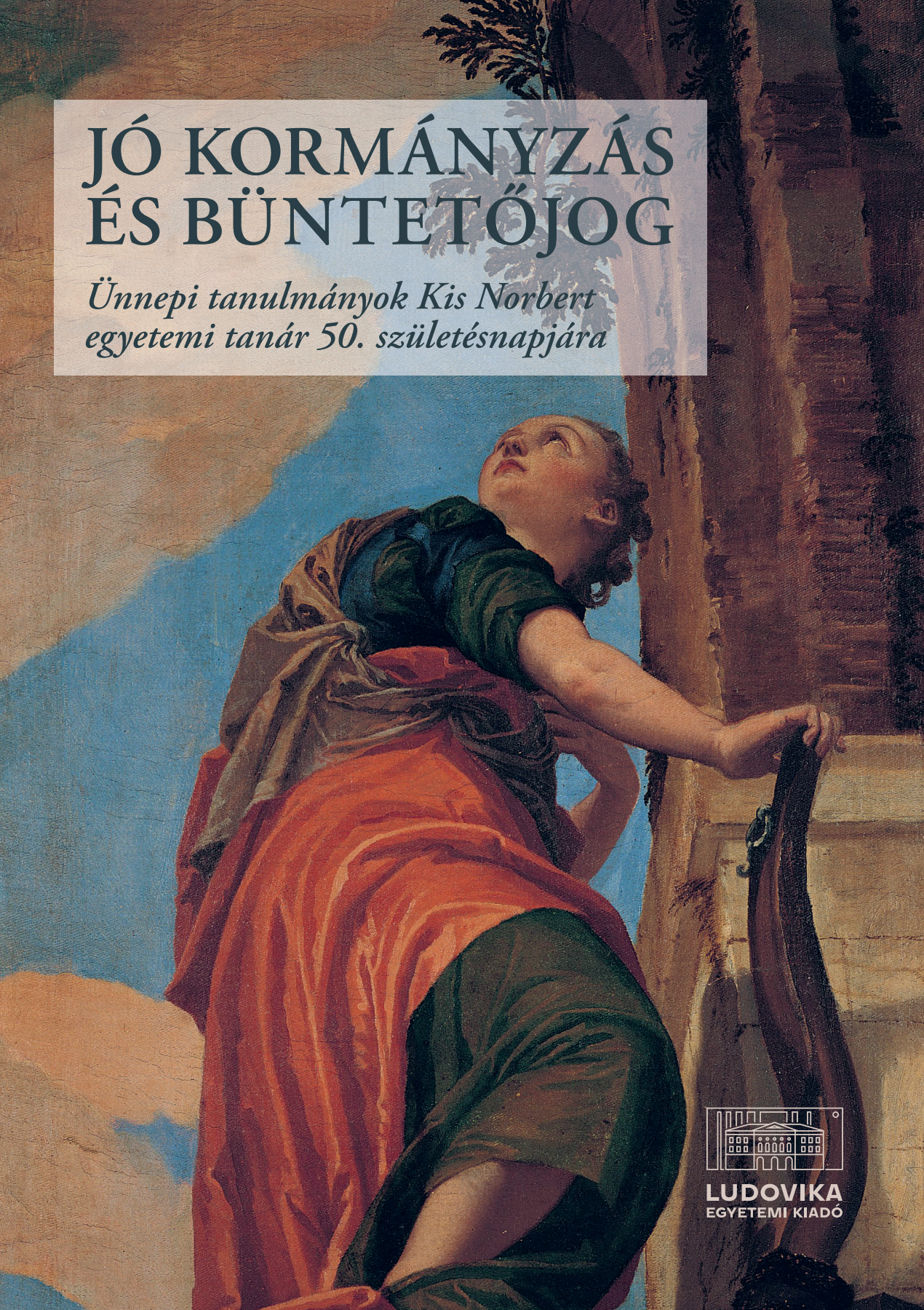
JÓ KORMÁNYZÁS ÉS BÜNTETŐJOG

Ünnepi tanulmányok Kis Norbert egyetemi tanár 50. születésnapjára



LUDOVIKA
EGYETEMI KIADÓ

Jó kormányzás és büntetőjog

Ünnepi tanulmányok Kis Norbert egyetemi tanár 50. születésnapjára

Jó kormányzás és büntetőjog

Ünnepi tanulmányok Kis Norbert egyetemi tanár 50. születésnapjára

Szerkesztette
Koltay András és Gellér Balázs

LUDOVIKA
EGYETEMI KIADÓ
Budapest, 2022

A kötet szerzői

Ambrus István
Bárányos Bernadett
Budai Balázs Benjámin
Christián László
Cs. Kiss Lajos
Csikány Tamás
Dávid Lilla
Deli Gergely
Elek Balázs
Fejes Zsuzsanna
Filó Mihály
Gellér Balázs
Gellérné Lukács Éva
Gombos Katalin
Hazafi Zoltán
Herke Csongor
Horváth Attila
Hutkai Zsuzsanna
Imre Miklós
Jacsó Judit
Kaiser Tamás
Kiss György Árpád
Klotz Balázs
Klotz Péter
Koller Boglárka
Koltay András
Korpics Márta
Kovács Éva Margit
Kovács Gábor
Krasznay Csaba
Kristó Katalin
Madai Sándor
Máthé Gábor
Méhes Tamás
Németh Imre
Patyi András
Pongrácz Alex
Sántha Ferenc
Sasvári Péter
Szabó Ádám
Tamás András
Téglási András
Varga Zs. András
Vastag Gyula

A borító Veronese (1528–1588) *Jó kormányzás (Il buon governo)* című festményének (1551–1552 között) felhasználásával készült. A kép Rómában, a capitoliumi múzeumokban található. Forrás: Wikimedia Commons.

Tartalom

Krasznay Csaba*

Kiberbiztonsági képzések a Nemzeti Közszolgálati Egyetemen

A kiberbiztonság mint multidiszciplináris tudományág

Informatizált világunkban a kibertér biztonsága egyre inkább meghatározóvá válik az élet minden területén. Ebből következik, hogy az információ- és kiberbiztonság az egyik legdinamikusabban fejlődő gazdasági terület, fejlesztése pedig az egyik legfontosabb nemzetbiztonsági célkitűzés. Magyarország 2020-ban elfogadott Nemzeti Biztonsági Stratégiája így fogalmazza meg hazánk biztonsági környezetét:

> „48. A hatalmi vetélkedés mindinkább kiterjed a globális közjavakra is: fokozódó küzdelem folyik a nemzetközi vizek és az ott található erőforrások, az északi sarkvidék és a világűr ellenőrzéséért, valamint a kibertér dominanciájáért. Az emberiség technológiai szintjének rohamos fejlődésével [digitalizáció, ötödik generációs vezeték nélküli hálózat (5G), űrtechnológia stb.] folyamatosan új lehetőségek és kihívások jelennek meg, amelyek hatást gyakorolnak hazánk biztonságára. Az 5G jelentette technológia olyan forradalmi fejlesztéseket tehet lehetővé perspektivikusan, amelyek számottevő változásokat generálhatnak társadalmunk és gazdaságunk viszonylatában. […]
> 69. A technikai fejlődéssel és vívmányainak elterjedésével folytatódik a biztonságot veszélyeztető, nehezen kontrollálható nem állami szereplők – például szervezett bűnözői körök, nemzetközi terrorszervezetek, kiberbűnözői csoportok, szélsőséges vallási közösségek, magán biztonsági cégek, egyes nem kormányzati szervezetek és egyéb transznacionális hálózatok – súlyának növekedése a nemzetközi biztonságpolitikában. Ezek mögött sokszor nehezen azonosítható érdekek és csoportok húzódnak meg, és könnyen szolgálhatnak rejtett állami szándékokat. Mindez átrendezi és áttekinthetetlenebbé teszi egyes térségek biztonsági helyzetét, ami hazánk számára is kihívást jelent.
> 70. Az információs technológia rohamos fejlődéséből és terjedéséből kifolyólag az állam és a társadalom működése egyre inkább a digitalizációra épül. Az elektronikus információs rendszerek sérülékenységei ezért biztonsági kockázatot hordoznak

* Egyetemi docens (Nemzeti Közszolgálati Egyetem Államtudományi és Nemzetközi Tanulmányok Kar).

> magukban. Világméretű tendencia, hogy a kibertérben végzett, ártó szándékú tevékenységek egyre gyakoribbak, egyre kifinomultabbak és egyre nagyobb kárral járnak. 71. Növekvőben van azoknak az államoknak és nem állami szereplőknek a száma, amelyek a kiberteret kritikus adatok illegális megszerzésére, valamint az elektronikus információs rendszerekben vagy azokon keresztül történő – akár fizikai – károkozásra használják. Ezért a kibertér ma már a szárazföld, a tengerek, a levegő és a világűr mellett külön műveleti térnek számít. A jövőbeli konfliktusok nagy valószínűséggel még inkább ki fognak terjedni a kibertérre."[1]

Magyarország 2013-ban elfogadott Nemzeti Kiberbiztonsági Stratégiájának megújítása a jelen tanulmány írásának idején előkészítés alatt áll, azonban egyértelműen megfogalmazódik az a kívánalom, hogy ez reflektáljon a fenti biztonsági kihívásokra. Az egyik fontos célkitűzés ezért a kiberbiztonsági képességfejlesztés, ezzel kapcsolatban pedig le kell szögezni, hogy a képességfejlesztés nemcsak az állami szervek számára fontos, hanem jelentős gazdasági potenciál is rejlik benne. Magyarországon és a régió más országaiban is jellemző ugyanis az úgynevezett *near-shoring* jelenség, számos nyugati ország telepíti a régióba azon szolgáltató központjait *(shared service center),* amelyek információbiztonsági szolgáltatást nyújtanak az anyavállalatnak vagy fontos ügyfeleknek. Ezek a biztonsági műveleti központok *(security operation center)* jelentős munkaadók, jelenleg is ezekben dolgozik a magyar információbiztonsági szakemberek többsége.

Megfelelő munkaerőképzéssel és összehangolt külgazdasági tevékenységgel további központok telepíthetők Magyarországra, ami egyben a magyar munkaerő külföldre szivárgásának mértékét is csökkenteni tudja. További jelentős gazdasági lehetőség van a kutatási-fejlesztési, innovációs központok hazánkba telepítésében, különösen azokon a területeken, ahol a kiberbiztonságtól függetlenül is jelentős előrelépések történtek (például autóipar). De meg kell említeni a *start-up* ökoszisztémában és a védelmi innovációban rejlő lehetőségeket is. Ha tehát a kiberbiztonság nemcsak operatív tevékenységként jelenik meg a magyar stratégiákban, hanem összehangolt gazdaságpolitikai lépések is történnek, és a kormányzat értékteremtő tevékenységként kezeli a területet, akkor a képességfejlesztés új dimenziói jelenhetnek meg.

A Nemzeti Közszolgálati Egyetem (NKE) kutatóinak becslése alapján jelenleg körülbelül 10 ezer szakember foglalkozik Magyarországon információ- és kiberbiztonsággal. A különböző képzőintézmények évente körülbelül 300 új szakembert tudnak a munkaerőpiacra bocsátani, amivel nagyjából ellensúlyozni tudják az „agyelszívás" hatásait, és ki tudják elégíteni a munkaadók igényeit. Problémát jelent viszont, hogy sokszor dömpingszerű felvételek vannak (egy munkaadó rövid idő alatt akar felvenni több tucat szakembert), ami kiszá-

[1] 1163/2020. (IV. 21.) Korm. hat. Magyarország Nemzeti Biztonsági Stratégiájáról.

míthatatlanná teszi a képzési időket. Nagyon hiányoznak a munkaerőpiacról a középfokú végzettséggel rendelkező technikusok, illetve a BProf vagy BSc végzettségű üzemeltetők. Emellett komoly gond, hogy bár a képzések számszakilag pótolni tudják a külföldre távozó szakembereket, a tapasztalatukat nem képesek helyettesíteni, így akár évtizedes rutinnal rendelkező mérnökök helyett juniorok kerülnek a munkakörökbe. Az igazán speciális szaktudásra pedig Magyarországon igen ritkán mutatkozik igény, ezért ehhez jellemzően nincsen szakértelem, ami komoly gátja az innovatív tevékenységek meghonosodásának.

Magyarországon tehát olyan információ- és kiberbiztonsági képzési rendszert érdemes létrehozni, amely reflektál a piaci és a közszolgálati igényekre is, egyben figyelembe veszi azt, hogy a szakterület ma már korántsem kizárólag a műszaki megközelítésről szól. A rendészet, a diplomácia, a katonai terület mind igényli azon szakemberek részvételét, akik a kibertér stratégiai és taktikai védelmében tudnak támogatást nyújtani, vagy éppen hídként tudnak működni a döntéshozók és a műszaki végrehajtók között. Kétségtelen tehát, hogy az egyes közszolgálati hivatásnemek művelői számára bizonyos kiberbiztonsági képességek fejlesztése szükséges, ez pedig indokolttá teszi, hogy az államtudományi területen is megjelenjen olyan képzés, amely közszolgálati-kormányzati fókuszú, és mivel nem az informatikai tudományok területén elvárt kompetenciák megszerzését tűzi ki célul, elsősorban arra törekedjen, hogy a „szükséges és elégséges" műszaki tudást adja át az alapvetően a gazdasági és a jogtudományok területén korábban alapszintű oklevelet szerzett hallgatóknak.

Kiberbiztonsági képzési előzmények a Nemzeti Közszolgálati Egyetemen

Már 2012-ben felismerték, hogy az NKE-n el kell indítani egy olyan képzést, amely az állami szervezetek információbiztonsági szintjének emelését szolgálja. Ebben az évben jött létre az NKE, és ekkor indult el az állami és önkormányzati szervezetek elektronikus információbiztonságáról szóló jogszabály kodifikálása is a Közigazgatási és Igazságügyi Minisztériumban, amelyben az új egyetem két oktatója, Muha Lajos és Krasznay Csaba is részt vett. Ennek a szerencsés együttállásnak köszönhető, hogy az elektronikus információbiztonságról szóló 2013. évi L. törvény (Ibtv.) 23. §-a olyan feladatokat határozott meg az NKE számára, amelyek megteremtették az államtudományi orientáltságú kiberbiztonsági képzés alapjait. A jogszabály szerint az NKE az alábbi feladatokat látja el:

– a jogszabályban meghatározott képzés érdekében kidolgozza és a közigazgatás-fejlesztésért felelős miniszter elé terjeszti a vezetők, az elektronikus információs rendszer biztonságáért felelős személyek képzési, továbbképzési követelményeit, oktatási programját;

– kidolgozza és a közigazgatás-fejlesztésért felelős miniszter elé terjeszti a jogszabályban meghatározott képzettségi követelményeket;
– gondoskodik a vezetők, az elektronikus információs rendszer biztonságáért felelős személyek és az általuk irányított szervezeti egységek munkatársai képzéséről és éves továbbképzéséről, együttműködik az eseménykezelő központ szakembereivel;
– közreműködik az információbiztonsági, a kibervédelmi és a létfontosságú információs rendszer védelmi gyakorlatokon.[2]

A törvény a vezetők kötelességévé tette, hogy gondoskodjanak az NKE képzésein keresztül az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maguk és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról. A törvény által előírt képzések egyike az elektronikus információbiztonsági vezető képesítést nyújtó akkreditált szakirányú továbbképzés. A törvény szerint az elektronikus információs rendszer biztonságáért felelős személy feladatait ellátóknak öt éven belül el kell végezniük a képzést. A képzés időtartama 300 óra, amelyet két félév alatt teljesít a hallgató.

A szakirányú továbbképzési szak 2014-ben indult, és 2022-ig már több mint 1000 hallgató végezte el a képzést, amely igen népszerűvé vált nemcsak a kötelezettek között, hanem a közszolgálati dolgozók szélesebb körében is. Jelenleg a hallgatók több mint fele nem az Ibtv. előírásai miatt iratkozott be, hanem saját szakmai életútját kívánja a kibervédelmi irányba elmozdítani. Mind a hallgatói, mind a szakmai visszajelzések azt igazolták, hogy a szakirányú továbbképzés ismeretanyaga és tapasztalata megfelelő alapot nyújt egy tágabb spektrumú, közszolgálati orientáltságú kiberbiztonsági mesterképzés elindításához.

A pozitív tapasztalatok nyomán az Egyetem Fenntartói Testülete 2016. júliusi ülésén megtárgyalta a nemzetközi kiberbiztonsági képzési és kutatási potenciál fejlesztéséről szóló koncepciót. Ez az NKE fejlesztési terveit illetően áttekintette Magyarország Nemzeti Kiberbiztonsági Stratégiájának és kibervédelmi szervezetrendszerének főbb kapcsolódási pontjait, bemutatta az NKE-n 2013 óta folyó, az állami intézmények vezetői és az elektronikus információs rendszer biztonságáért felelős személyek kibervédelmi képesítő képzését (elektronikus információbiztonsági vezető szakirányú továbbképzés) és továbbképzését, a kiberbiztonság területén folyó kutatásokat és a hazai és külföldi egyetemi partnerséget és partnerségi terveket. A koncepció a nemzetközi irányú fejlesztés elemeként egy angol nyelvű *Executive Master in Cyber Security* mesterképzést határozott meg (angol rövid munkanév: CYSECMAN).

[2] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

A Fenntartói Testület ezután a 2016. augusztusi ülésén megtárgyalta az alábbi tematikát:

– az NKE kari és intézeti szinergiáit is összefogó integrált kiberbiztonsági kutatás- és képzésfejlesztés;
– a CYSECMAN megalapítása, nemzetközi pozicionálása;
– nemzetközi minőség és minősítés;
– hazai kormányzati és szakmai partnerség fejlesztése;
– informatikai környezet fejlesztése, IT szimulációs „gyakorlótér" (kiberbiztonsági labor) kialakítása.

Majd a Fenntartói Testület a 2016. novemberi ülésén megtárgyalta egy kiberbiztonsági akadémia felállításának és működésének tervét, amely a testület által korábban támogatott nemzetközi kiberbiztonsági képzési és kutatási fejlesztések végrehajtása számára jelent szervezési keretet. A Fenntartói Testület arról döntött, hogy az egymásra épülő koncepciók és fejlesztési tervek egységes anyagban jelenjenek meg, és a fenntartói tárcavéleményeket is építsék be.

A Fenntartói Testület 2016. decemberi ülésén megtárgyalta, hogy az elektronikus információbiztonsági vezető szakirányú továbbképzés curriculuma és képzési tapasztalatai alapján ki kell dolgozni mesterképzésként a szakalapítás dokumentumait. Az államtudományi képzési területen, a nemzetközi és európai közszolgálati területen javasolt a szakot létesíteni. Ezt a 193/2016. számú határozatában fogadta el, majd az NKE rektorának a Kiberbiztonsági Akadémia létesítéséről és működéséről szóló 3/2017. számú utasítása értelmében a feladatszabást is meghatározta. Ezzel megnyílt az út egy újonnan létrehozandó, előzmények nélküli kiberbiztonsági mesterszak elindítása előtt, amelyet Kis Norbert dékánként és rektorhelyettesként kiemelten támogatott, és akinek áldozatos munkája nélkül az NKE kiberbiztonsági portfóliója sokkal szerényebb lenne.

Kitekintés: kiberbiztonsági mesterképzések külföldön

Mivel a képzés kialakításának időpontjában Magyarországon egyáltalán nem, és Európában is csak kevés hasonló oktatási program volt, el kellett végezni a nemzetközi összehasonlítást. Az NKE esetében az információbiztonsági képzések struktúrájának kialakítását annak multidiszciplináris jellege állítja kihívás elé, amelyben a műszaki szempontok helyett az államtudományi területnek kell dominálnia. A szakirodalmi áttekintés alapján először Eugene Spafford, a Purdue Egyetem professzora határozta meg azokat a területeket, amelyeket minden kiberbiztonsági képzésnek érintenie kell. Munkájában 18 résztémakört

különített el – ezen ismeretek eltérő tudományterületeken és képzési szinteken szerezhetők meg:[3]

1. adatbázisok kezelése (BA-szint);
2. ember és számítógép közötti interakciók elemzése;
3. filozófia és etika;
4. hadtudományok;
5. hálózatok (BA-szint);
6. az információ elméleti háttere;
7. információszerzés;
8. kriminológia és jog;
9. kriptográfia (BA-szint);
10. matematika (BA-szint);
11. menedzsmenti és üzleti aspektus;
12. mobil számítástechnika (BA-szint);
13. operációs rendszerek (BA-szint);
14. programozási nyelvek (BA-szint);
15. statisztika és valószínűségszámítás (BA-szint);
16. számítógépes architektúra (BA-szint);
17. szoftverfejlesztés (BA-szint);
18. webprogramozás (BA-szint).

A világ egyik legfejlettebb kibervédelmi oktatási rendszerével az Egyesült Királyság rendelkezik. Az ITU Global Cybersecurity Index 2020 felmérése alapján a kiberképességek fejlesztésében európai éllovas, már az elemi oktatási szinttől foglalkozik az utánpótlásképzéssel.[4] Ahogy Molnár Dóra fogalmaz cikkében:

> „A kiberismeretek oktatását már az alsó fokú oktatásban megkezdték: 800 általános iskola bevonásával mintegy 23 000 diák szerzett alapvető ismereteket 2012 óta. A felsőoktatásban valamennyi alapképzés esetében bevezettek egy kiberbiztonsági közös modultárgyat, a mesterképzésen pedig a GCHQ által kiadott standardnak megfelelően már 12 akkreditált kiber-mesterképzés létezik. Jelenleg három kutatóintézet rendelkezik kiberbiztonsági profillal, 13 kiválósági központot hoztak létre, és cél, hogy 2019-re 100 doktoranduszt tudjon magáénak a már működő két kiberbiztonsági doktori iskola."[5]

[3] Eugene F. Spafford: *Teaching the Big Picture of InfoSec. Proceedings of the 2nd National Colloquium for Information System Security Education.* Harrisonburg, James Madison University, 1998.

[4] International Telecommunication Union: Global Cybersecurity Index 2020, www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[5] Molnár Dóra: Mérföldkövek a brit kiberbiztonság fejlődésében I. Az elméleti háttér megalapozása: a kiberbiztonsági stratégia. *Hadmérnök,* 12. (2017), 2. különszám. 136–148.

A tanulmány írásának idején összesen 56 program rendelkezik akkreditációval, ebből 45 mesterszintű képzés.

Az NKE kiberbiztonsági mesterképzésének előkészítéseként Urbanovics Anna és Sasvári Péter részletes elemzést végzett azzal kapcsolatban, hogy pontosan milyen jellegű tárgyak tartoznak a kiberbiztonsági képzés alá a brit egyetemeken. A szerzők hét tantárgycsoportot azonosítottak:

1. kriptográfia és adatelemzés;
2. bűnügyi informatika;
3. hálózatbiztonság;
4. szoftverbiztonság;
5. hardverbiztonság;
6. informatika más aspektusból (jog, menedzsment és pszichológia);
7. kutatás és elméleti ismeretek.

Az Egyesült Királyság információ- és kiberbiztonsági képzési programjait az 1. táblázat mutatja be.[6]

1. táblázat. *Témakörönként, felsőfokú intézményenként meghirdetett kurzusok száma*

Intézmény/témakör/ kurzusok száma	*Kriptográfia és adatelemzés*	*Bűnügyi informatika*	*Network-biztonság*	*Szoftver-biztonság*	*Hardver-biztonság*	*Informatika más aspektusból*	*Kutatás és elmélet*
Cranfield University		3	2	4		3	2
Lancaster University		2	1	1		3	2
Edinburgh Napier University		1	2	2		1	1
Queen's University Belfast	1	2	1	1		1	
Royal Holloway University	3	2	1	3	2	3	2
University College London	3	2		2	1	3	3
University of Birmingham	3	1	3	6	1	1	3
University of Oxford	1	2	4	2		5	1
University of South Wales		3	1			2	1
University of Southampton	4	2		2	1	4	5
University of Surrey	3		2	2		3	
University of York	1	2	1			2	2

Forrás: a szerző szerkesztése

[6] Urbanovics Anna – Sasvári Péter: Az Egyesült Királyságban működő kiberbiztonsági képzésekbe bevont oktatók tudományos teljesítményének elemzése. *Információs Társadalom,* 18. (2018), 3–4. 105–124.

Az NKE 2017-ben tervezett kiberbiztonsági mesterképzéséhez nagyon hasonlót indított Hollandiában a leideni, a delfti és a hágai egyetem. Ez a tervezési időszakban talán az egyetlen olyan képzés volt Európában, amely a tisztán műszaki fókusz helyett tágabban értelmezte az oktatási spektrumot. A javasolt mesterképzés nagyban támaszkodik arra a tanmenetre, amelyet a három holland egyetem által indított Kiberbiztonsági Akadémia kialakított.

Jól látható tehát, hogy a kiberbiztonság több mint pusztán műszaki kérdés, ám Magyarországon az NKE által tervezetthez hasonló, multidiszciplináris aspektusokkal foglalkozó képzés nem indult. A külföldi példák pedig arra is rámutattak, hogy ha van is kiberbiztonsági képzés a közszolgálati szakemberek részére, nehezíti az egységes megközelítés kialakítását az, hogy a hivatásrendek képzése jellemzően különböző intézményekben történik, így egy komplex kiber-fizikai katasztrófaesemény során hiába kellene együttműködnie rendészeti, katasztrófavédelmi, titkosszolgálati, katonai és közszolgálati szakembereknek, hiányzik az a közös nyelv, amelyre az összehangolt védelmet építeni lehetne.

A kiberbiztonsági mesterképzés megalakítása

Az NKE kiberbiztonsági mesterszakának megalakítása során figyelembe kellett venni azt az intézményen belüli, hazai és nemzetközi környezetet, amely 2017–2018-ban hatással lehetett az oktatási programra. Az intézmény elsődleges feladata a közszolgálati igényeknek megfelelő oktatás biztosítása a graduális és posztgraduális hallgatók számára, így elsősorban ezt tartotta szem előtt. Emellett viszont lehetőség nyílt a nemzetközi együttműködések kiaknázására is, így egy olyan komplex oktatási program összeállítása vált lehetővé, amely kihasználja az egyes karok közötti szinergiát, választ ad a megrendelői elvárásokra, és európai szinten is kimagasló kurzuslistát szolgáltat az érdeklődőknek.

Mivel ezekben az években megújult a védelmi infokommunikációs mesterszak a Hadtudományi és Honvédtisztképző Karon (HHK), és az elektronikus információbiztonsági vezető szakirányú továbbképzés is, emellett 2020-ban elindult a kibernyomozó és az informatikai nyomozó szakirány a bűnügyi alapképzési szakon a Rendészettudományi Karon (RTK), illetve az európai uniós adatvédelmi szaktanácsadó szakirányú továbbképzés, minden korábbinál fontosabb volt az intézményen belüli együttműködés megerősítése. A kiberbiztonsági mesterképzés indításakor így számos szempontot figyelembe kellett venni, hogy egy komplex, minden érdeket és értéket figyelembe vevő képzés jöhessen létre.

1. Felkészülés a Kiberbiztonsági mesterképzésre: a szakakkreditáció 2019-ben történt, a mesterképzés pedig 2020 őszén indult el. A fenntartói döntés utáni kétéves időszakban a Kiberbiztonsági Akadémia azon dolgozott,

hogy az egyes tantárgyak a lehető legjobban illeszkedjenek egymáshoz és a megrendelői követelményekhez. Ennek érdekében:

a) egyeztetéseket szervezett a tárgyak felelősei, oktatói és az érdekelt külső felek között a tematika legjobb kialakításáért;

b) pilotoktatások keretében, kurzusjellegűen bemutatta a tárgyakat a Kiberbiztonsági Akadémia Szakmai Irányító Testületbe delegált szervezetek érintett munkatársainak;

c) a tematikákat egyeztette az észtországi tallinni műszaki egyetem (TalTech) munkatársaival, előkészítendő egy esetleges közös *joint/double degree* mesterképzést;

d) bizonyos tantárgyakat felajánlott a European Security and Defense College (ESDC) kiberbiztonsági platformja számára;

e) a Rendészettudományi Kar oktatóival közösen felkészült a kibernyomozó (4 éves nappali), illetve informatikai nyomozó (3 éves levelező) szakok indítására.

2. A már futó kurzusok fejlesztése: a folyamatos hallgatói utánpótlás biztosítása érdekében elérhetővé kellett tenni minél többek számára a kiberbiztonsági szakterületet megalapozó tantárgyakat. Emellett több olyan programfejlesztés is történt az egyetemen, amelyek indokolták a karok közötti összehangolt tevékenységeket. Mindezek támogatásához:

   a) áttekintették az NKE Államtudományi és Nemzetközi Tanulmányok (ÁNTK) karának elődkarain oktatott, kiberbiztonsági témájú tantárgyak tematikáit;

   b) új választható tantárgyakat írtak ki;

   c) egyeztetés indult az RTK-val a kibernyomozó és az informatikai nyomozó szakirány és a HHK-val a védelmi infokommunikációs mesterszak tantárgyi tematikájával kapcsolatban, a szinergiák kihasználása érdekében;

   d) megtörtént az elektronikus információbiztonsági vezető szakirányú továbbképzés, az európai uniós adatvédelmi szaktanácsadó szakirányú továbbképzés és a kiberbiztonsági mesterképzés tantárgyainak összehangolása;

   e) két kurzust is indítottak az ESDC-vel közös szervezésben;

   f) lépések történtek a megfelelő laborkörnyezet kialakítására.

3. Hallgatói tehetséggondozás: a kiberbiztonsági téma már ekkor is igen népszerű volt az NKE-n, számos hallgató érdeklődött a terület iránt, akik később felvételt is nyertek a kiberbiztonsági mesterszakra. A tudatos tehetséggondozás érdekében ezért már az alapszakoktól meg kellett kezdeni a kiberkarrierek felépítését, a tehetségek kiválasztását. A hallgatói érdeklődés növelése érdekében:

a) külön kiberbiztonsági szekció indult az intézményi tudományos diákköri konferencián, amelyre folyamatosan toborozták a hallgatókat;
b) frissítették a szakdolgozati és a diplomamunka-kiírásokat, elsősorban az ÁNTK-n, de az RTK-n és a HHK-n is;
c) kiberbiztonsági állásbörzét rendeztek, amelyen a frissdiplomások és a leendő munkaadók megismerhették egymást;
d) folytatódott az együttműködés a szakkollégiumokkal, így elsősorban a Nemzetbiztonsági és a Biztonságpolitikai Szakkollégiumok kiberbiztonsági sejtjeivel;
e) felmerült egy Kiberbiztonsági Szakkollégium létrehozásának ötlete is;
f) elkezdődött a más egyetemek szakkollégiumaival való kapcsolatfelvétel;
g) hallgatói konferenciát szerveztek az Európai Kiberbiztonsági Hónap keretében;
h) bátorítottuk hallgatóinkat az észtországi TalTech-hel kötött Erasmus-programban való részvételre;
i) a legtehetségesebb hallgatókat ösztönöztük az észtországi TalTech nyári, kiberbiztonsági workshopján való részvételre;
j) megtörtént a résztvevők toborzása és felkészítése az olyan versenyekre, mint az Év Információbiztonsági Szakdolgozata/Diplomamunkája pályázat, a Nemzeti Kiberverseny és a Cyber 9/12 nemzetközi kiberverseny.

A kiberbiztonsági mesterképzési szak elindítása

A Nemzeti Közszolgálati Egyetem kiberbiztonsági mesterképzési szaka végül 2020 szeptemberében indult el, nappali és levelező képzésben. A szakalapítást az államtudományi képzési területen szerezhető képesítések jegyzékéről és a képzések képzési és kimeneti követelményeiről szóló 222/2019. (IX. 25.) Korm. rendelet és a Magyar Akkreditációs Bizottság 2019/5/VI/7. határozata tette lehetővé. A szakfelelős kezdetben Szádeczky Tamás, majd a későbbiekben Krasznay lett. A képzési és kimeneti követelmények világosan meghatározták a szak helyét a magyar és az európai kiberbiztonsági programok között. Képzési területként az államtudományi, ezen belül az államtudományi és a közigazgatási terület lett megnevezve, így jelezve a felvételizők számára, hogy határozottan nem műszaki képzésre jelentkeznek, hanem a belső szakzsargonban *soft cybersecurity*nak nevezett, az állami kibervédelemre fókuszáló képzési programban fognak részt venni. A mesterképzés lezárásával okleveles kiberbiztonsági szakértő végzettséget kapnak a hallgatók, amely a magyar felsőoktatásban egyedi képzettséget jelent.

A szakmai kompetenciák megfogalmazásánál is figyelembe kellett venni, hogy a képzés az államtudományok területén indul. Ki kellett emelni a közszolgálati szempontokat, a műszaki területeknél pedig a „szükséges és elégséges" elvét kellett követni. A kompetenciák kialakításánál az európai példákat sem lehetett egy az egyben figyelembe venni, mivel, mint azt korábban említettük, ebben az időszakban elsősorban a műszaki szakterületen indultak hasonló mesterképzések. A belső szakmai munka eredményeképp így a következő kompetenciák fogalmazódtak meg.

1. Tudás:
   – 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 kibertámadások 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 állása tekintetében;
   – tisztában van a nyomozó hatóság feladataival az egyes állami szervezeteket, vállalatokat 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.
2. Képességek:
   – 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 nyomozó hatósággal 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.

3. Attitűd:
   – munkája során figyelembe veszi és alkalmazza a kiberbiztonsággal kapcsolatos jogszabályokat;
   – megérti és elfogadja a nemzetközi kiberjog komplexitását, ennek köszönhetően a munkája során törekszik annak 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.
4. Autonómia és felelősség:
   – 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 alapján 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 az operatív teendők stratégiai célokká való konvertálásában;
– gyakorlatába beépíti és alkalmazza az e szakterületen folyó kutatások eredményeit.

A Kiberbiztonsági Akadémia Szakmai Irányító Testületének résztvevőitől kapott visszajelzések alapján ezek a kompetenciák szükségesek a közszolgálati igények teljesítéséhez tekintettel arra, hogy a képzési programban elsősorban a közszolgálati információbiztonsági felelős, a kritikus információs infrastruktúra védelméért felelős szakember és a nemzetközi kiberkapcsolati munkatárs („kiberdiplomata") szerepkörök betöltésére van szükség, illetve ezek mellett a rendvédelemben („kibernyomozó", hírszerző/elhárító) és a honvédelemben („kiberkatona") dolgozó munkatársak kompetenciájának bővítése szükséges. A képzési program emellett lehetővé teszi egyes piaci hiányszakmák utánpótlásképzését is, például információbiztonsági auditorét vagy kockázatkezelési szakemberét, amelyek a műszaki területen végzettek számára kevésbé vonzók, illetve a szerepkörök betöltéséhez olyan interperszonális készségek szükségek, amelyek egy mérnöknél nem feltétlenül állnak rendelkezésre.

A tanterv ennek megfelelően teljes mértékben multidiszciplináris, számos tudományterületből merít:

– államtudományi, jogi és közigazgatás-szervezési ismeretek (10–15 kredit);
– információbiztonsági és biztonságszervezési ismeretek (25–30 kredit);
– nemzetközi tanulmányok és biztonságpolitikai ismeretek (10–15 kredit);
– rendészeti szakismeretek (10–15 kredit);

– alkalmazott infokommunikációs szakismeretek (10–15 kredit);
– katonai és védelmi szakismeretek (10–15 kredit);
– vezetési és kommunikációs szakismeretek (10–15 kredit).

Ez a felosztás lehetővé tette azt, hogy a képzésbe integrálhatóvá váljanak az Európában megszokott alaptantárgyak, építeni lehessen az elektronikus információbiztonsági vezető szakirányú továbbképzés tantárgyaira, de megjelenhessenek az NKE karainak specialitásai is.

A négy féléves képzés 120 kreditjének megszerzéséhez a hallgatóknak nappali tagozaton összesen 3600 munkaórát kell eltölteni az ismeretek megszerzésével, ami félévenként átlagosan 30 kreditet és 385 tanórát jelent. Hetente átlagosan 28 tanóra kerül az órarendbe, ezek összeállításánál viszont az NKE figyelembe veszi a hallgatók igényét arra, hogy a második évtől 20 órás munkaviszonyban munkát tudjanak vállalni. Levelező tagozaton pénteki és szombati napokon van a képzés, félévente átlagosan 110 óra hosszban. A képzés kötelező része a 10 hetes szakmai gyakorlat, amelyet jellemzően a második félév utáni nyáron teljesítenek a hallgatók. A törzsanyag a következőképp alakul:

– jogi és közigazgatási ismeretek;
– a magyar közigazgatás szervezeteinek és szakigazgatási rendszereinek működése;
– kiberbiztonsági szabályozások és szabványok;
– bevezetés a kiberbiztonság szakterületi ismereteibe;
– biztonságpolitika;
– kiberhadviselés;
– létfontosságú rendszerek és létesítmények védelme;
– biztonsági technológiák alkalmazása;
– vezetéselmélet;
– adatvédelem;
– kockázatértékelés, kockázatmenedzsment;
– kritikus információs infrastruktúra védelem;
– kiberdiplomácia;
– kiberbűnözés;
– kiberbiztonsági stratégia és vezetés;
– válságmenedzsment és kommunikáció;
– információs rendszerek és hálózatok biztonsága;
– a hazai és nemzetközi szervezetek feladatai a kibervédelemmel összefüggésben;
– digitális nyomrögzítés;
– közmenedzsment;
– közszolgálati információs rendszerek védelme;

– a kiberbiztonság humán tényezői;
– incidensmenedzsment;
– hírszerzés a kibertérben;
– biztonságtechnika;
– kriptográfia a közszolgálatban;
– biztonsági tesztelés;
– kiberbiztonság pszichológiai aspektusai.

A hallgatók szabadon választhatóként bármit választhatnak az ÁNTK tantárgyai közül, de néhány tárgyat dedikáltan a kiberbiztonsági mesterszakhoz hirdettek, például az adatbányászat, az adatvédelem a gyakorlatban, a kiberbiztonsági akkreditáció és tanúsítás, a kiberbiztonsági innováció, a pénzintézeti információs rendszerek védelme és a villamosenergia-rendszerek kibervédelme. 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. Mivel a felvételizők többsége vagy informatikai, vagy államtudományi és társadalomtudományi előképzettséggel rendelkezik, a képzés része a kreditpótló tantárgyak meghirdetése. Ezeket a képzés első évében szükséges teljesíteni.

A képzés diplomamunka megírásával és záróvizsgával zárul. A diplomamunka a szakképzettségnek megfelelő alkotó jellegű, témavezető vagy konzulens irányításával két félév alatt elvégezhető, önálló munkával megoldható feladatról készült dolgozat, amely tanúsítja, hogy a hallgató jártasságot szerzett a tanult ismeretanyag gyakorlati alkalmazásában, az elvégzett munka és az eredmények szakszerű összefoglalásában, a témakörébe tartozó feladatok kreatív megoldásában, a szakképzettségnek megfelelő önálló munka végzésében. A záróvizsga a tantervben meghatározottak szerint több részből áll. Elsőként a gyakorlati vizsgát végzik el a hallgatók, amelynek során egy kiberbiztonsági esemény komplex kezelését kell megoldaniuk. A diplomamunka megvédése után szóbeli vizsga

következik a kockázatértékelés, kockázatmenedzsment és az információs rendszerek és hálózatok biztonsága tárgyak anyagából.

A kiberbiztonsági mesterképzési szak első tapasztalatai

A képzés indítását egy nem várt, globális kihívás tette igazán izgalmassá, tekintettel arra, hogy a Covid–19-pandémia első hulláma pontosan a felvételi időszakában ért csúcsra, míg az első képzési évet a második és a harmadik hullám tette kiszámíthatatlanná. Bár a szakindítás során felmerült a hibrid képzés megvalósításának lehetősége – összhangban az európai trendekkel –, mind az oktatóknak, mind a hallgatóknak különösebb felkészülés nélkül kellett alkalmazkodniuk a megváltozott körülményekhez. Két év tapasztalata alapján elmondható, hogy a hibrid oktatásnak van létjogosultsága, de elsősorban a levelező képzésen és leginkább az elméleti foglalkozásokon. A kiberbiztonság ugyanis nem magányos foglalkozás, muszáj hangsúlyt helyezni a csoportdinamikára, a közösségépítésre, ami online formában nem valósítható meg. Az elméleti órák és egyes technológiai gyakorlatok esetében viszont akár ki is lehetne váltani az óralátogatási kötelezettségeket, mivel már rendelkezésre állnak azok a videórögzítési megoldások, *e-learning* környezetek és felhőből elérhető laborok, amelyek felhasználásával még rugalmasabbá tehető a képzés. A pandémia utáni felsőoktatásnak, ebbe beleértve az NKE-t is, célszerű ezt a rugalmasságot biztosítani a hallgatói számára, hiszen ez a nemzetközi versenyképesség kulcsa.

A hallgatók összetétele, a tőlük és a munkaadóktól származó visszaigazolások azt mutatják, hogy a mesterképzésnek van helye a magyar felsőoktatási rendszerben. Nappali tagozaton elsősorban az NKE-n alapszakot végzett hallgatókkal lehet találkozni – az első két évben felvettek között ritka a műszaki informatikát vagy gazdaságinformatikát végzett hallgató. A nappalisok esetében ezért nagyobb hangsúlyt kell fektetni az informatikai alapozásra, mert a „szükséges és elégséges" informatikai tudással még a végzéskor sem feltétlenül rendelkeznek. Ezt öntanulás formájában kell megoldani, hozzáférést engedve nekik olyan *e-learning* anyagokhoz, amelyekkel az NKE jelenleg nem rendelkezik. A levelező tagozatosok között eközben jelentős túlsúlyban vannak azok a hallgatók, akik már évek, évtizedek óta a szakterületen dolgoznak, nem egy esetben egyszerre hallgatói és meghívott oktatói is a szaknak. Azok a hallgatók viszont, akik nem ebbe a körbe tartoznak, azzal a csapdahelyzettel küzdenek, hogy a „hangos többség" miatt nem feltétlenül szerzik meg a kompetenciákat, mivel az oktatóknak az a benyomása támadhat, hogy már számos ismerettel rendelkeznek. Ezért nehezen megoldható a szakértők és a nem szakértők igényeinek való egyszerre megfelelés, aránylag kis óraszám mellett. Az öntanulás így itt is megoldást jelenthet.

Fontos kérdés a végzettek karrierútja. A szak létrehozásának eredeti szándéka az volt, hogy a közszolgálat szakemberképzési igényeit elégítse ki. Az első évek tapasztalata azonban azt mutatja, hogy a korábbi munkatapasztalat nélküli hallgatókat inkább piaci környezetbe veszik fel, először gyakornokként, majd juniorként. Ez egyfelől igen pozitív szakmai visszajelzés, hiszen a legfőbb elhelyezkedési lehetőséget a pénzintézeti és a tanácsadó szektor jelenti, de egyben aggasztó is, hogy a közszolgálat nem tud valós alternatívát nyújtani a munkaerőpiacon. Ennek oka pedig nem feltétlenül a fizetésekben keresendő, sokkal inkább abban, hogy a gyakornoki kiírások, felvételi eljárások túlságosan bürokratikusak, nem tudnak versenyre kelni a piaci szereplők agilitásával, professzionális HR-eljárásaival. Szintén pozitív, hogy az egyébként is közszolgálatban dolgozó, jellemzően levelező szakos hallgatók maradnak a saját pozícióikban, illetve lehetőséget kapnak az előrelépésre.

Végül, de nem utolsósorban, meg kell emlékezni az eredeti fejlesztési célkitűzések utolsó lépéséről, a nemzetköziesítésről. Ami 2017 környékén még ambiciózus elképzelés volt, az 2022-ben már realitás. A világ biztonsági környezetének változása miatt minden adott ahhoz, hogy az NKE kiberbiztonsági mesterszaka a külföldi hallgatók előtt is megnyíljon. A teljesség igénye nélkül, a Digital Europe program ösztönzi és támogatja a közös kiberbiztonsági mesterképzések indítását, az európai kiberbiztonsági ügynökség (ENISA) ki fogja adni a European Cybersecurity Skills Framework keretrendszert, amely leírja, hogy milyen készségek oktatása szükséges a szakterületen, az Európán kívüli országokból pedig hatalmas igény mutatkozik a képességfejlesztésre. Az ENISA kiberbiztonsági felsőoktatási programjait gyűjtő adatbázisában eközben a 133 listázott képzés közül csak 13 van Közép-Európában, ezek között pedig hasonló sincs ahhoz, amilyet az NKE nyújt.[7] A szak organikus fejlődésének következő lépése lehet tehát egy angol nyelvű képzés – pont úgy, ahogy azt Kis Norbert évekkel ezelőtt célul tűzte ki a szakmai stáb elé.

[7] ENISA: CYBERHEAD – Cybersecurity Higher Education Database, www.enisa.europa.eu/topics/cybersecurity-education/education-map/education-courses

Kiadja a Nemzeti Közszolgálati Egyetem
Ludovika Egyetemi Kiadó
A kiadásért felel: Deli Gergely rektor
Székhely: 1083 Budapest, Ludovika tér 2.
Kapcsolat: kiadvanyok@uni-nke.hu

Felelős szerkesztő: Inzsöl Kata
Olvasószerkesztők: Biró Csilla, Bujdosó Hajnalka, György László, Kalcsics Ildikó, Kutas Éva,
Resofszki Ágnes, Szabó Ilse, Tomka Eszter
Tördelőszerkesztő: Fehér Angéla
Korrektorok: Biró Csilla, Bujdosó Hajnalka, György László,
Kalcsics Ildikó, Kutas Éva, Tomka Eszter

Nyomdai kivitelezés: Pátria Nyomda Zrt.
Felelős vezető: Orgován Katalin vezérigazgató

ISBN 978-963-531-757-8 (nyomtatott)
ISBN 978-963-531-758-5 (ePDF)
ISBN 978-963-531-759-2 (ePub)

Kis Norbert jogász, egyetemi tanár oktatóként és vezetőként is szolgálta, szolgálja a felsőoktatást. Az ELTE, a Széchenyi István Egyetem, majd a Corvinus tanára volt, és a kezdetektől részt vett a Nemzeti Közszolgálati Egyetem építésében, dékánként, illetve rektorhelyettesként is. Kormányzati pozíciókat töltött be felsőoktatási területen, és az ügyvédvilágban szintén megmérettette magát. Nemzetközi kapcsolatait kutatóként, oktatóként és vezetőként sikerrel fordította intézményei javára.

Egykori és jelenlegi egyetemi kollégái úgy döntöttek, hogy 50. születésnapjára egy ünnepi kötettel kedveskednek neki. A kötet szerzői és szerkesztői azt remélik, hogy az ünnepelt szakmai érdeklődéséhez közel álló tárgyú tanulmányokat egybegyűjtő kötet a közigazgatás, az állambölcselet, a kormányzástan és a büntetőjog iránt érdeklődőknek is élvezetes olvasmány lesz.

A szakmai eredményein túl Kis Norbert ugyanakkor férj, családapa, futballrajongó, magyar patrióta, az igazságot kereső, sorskérdéseken töprengő és nemzetközi perspektívákban gondolkodó ember. A kötet tanulmányain keresztül kollégái segítségével talán személyiségének egy-egy vonása is kirajzolódhat az olvasó előtt.