HADMÉRNÖK
VÉDELEMINFORMATIKA

15. évfolyam (2020) 4. szám 159–178.
DOI: 10.32567/hm.2020.4.11

Deák Veronika[1]

# A közszolgálati kiberbiztonsági képzés helye nemzetközi viszonylatban

## The Place of Public Service Cyber Security Training in International Context

**Naponta követnek el kibertámadásokat a különféle bizalmas információk megszerzése érdekében, állami és nem állami szerveket egyaránt célozva. Az elmúlt évek tapasztalatai alapján elmondható, hogy a közszolgálat kiemelt célpontja a kibertámadásoknak, így különösen nagy hangsúlyt kell fektetni a szervezeti és személyi kiberbiztonság folyamatos fejlesztésére. Ennek részeként értelmezhető a lehetséges támadási alternatívák megismerését és alkalmazhatóságát célzó közszolgálati kiberbiztonsági képzés megalkotása.**
**A képzési program meghatározása során fel kell tárni a jelenleg elérhető nemzetközi kibervédelemmel és kiberbiztonsággal kapcsolatos felsőoktatási képzéseket a hasonlóságok feltérképezése és az esetleges „jó gyakorlatok" átvétele érdekében. Jelen tanulmány a nemzetközi kiberbiztonsági, kibervédelmi képzéseket, ezen belül azok tartalmát, összetevőit, valamint a NICE Keretrendszer elemeinek nemzetközi képzésekben való megjelenését vizsgálja annak érdekében, hogy a nemzetközi tapasztalatok elemzése során feltárt gyakorlatok átültetése megvalósulhasson a hazai oktatásban.**

***Kulcsszavak:*** **közszolgálat, kiberbiztonság, mesterképzés, nemzetközi, jó gyakorlatok, NICE, oktatás**

**Cyber attacks are executed on a daily basis against private companies and goverment bodies; they aim at accessing to confidential data. Based on the events that happened in the past few years, public service has been a key target of cyber attacks. Hence organisations should continuously develop their defence capabilities. As part**

[1] Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola, doktoranda, e-mail: deak.veronika@uni-nke.hu, ORCID: https://orcid.org/0000-0001-9220-2002

**of this development, the public service cyber security training programme aims at learning about possible cyber attack alternatives.**
**During the specification of the programme, international cyber security programmes should be explored in order to show the relevance of such a training and to adopt possible 'best practices'.**
**In this paper, I proposed a selection and a comparison strategy to evaluate the international cyber security and cyber defence programmes including their content, key elements, relations with the NICE framework and possible shortcomings.**

***Keywords:*** **public service, cyber security, master programme, international, best practices, NICE, education**

## 1. Bevezetés

A különféle infokommunikációs technológiák mai modern társadalmunk nélkülözhetetlen alkotóelemét képezik. Ennek következményeként a közszolgálatban is megfigyelhető ezen eszközök, technológiák alkalmazásának térhódítása. Azonban ezek használata és az egyre növekvő függőség számos kockázatot rejthet magában.

A kibertámadások gyakran célozzák a közszolgálatot, azok hálózatait, illetve infokommunikációs eszközeit annak érdekében, hogy hozzáférjenek például az állampolgárok, az alkalmazottak bizalmas, személyes adataihoz, védett szoftverekhez, alkalmazásokhoz, stratégiai tervekhez vagy bármilyen más egyéb, a támadó szempontjából fontos információhoz. Éppen ezért különösen nagy hangsúlyt kell fektetni a lehetséges támadási alternatívák megismerésére és alkalmazhatóságára a hatékony védelem kialakítása érdekében.

A megfelelő szintű kiberbiztonság megteremtése komoly kihívásként jelentkezik napjainkban, a kibertámadások számának folyamatos növekedésének és a támadások egyre újabb eszközeinek, alternatíváinak köszönhetően. A támadások folyamatosan változnak, fejlődnek és a támadók egyre kifinomultabban használják ki a különféle információs rendszerek, valamint az emberi tényező sebezhetőségeit, illetve egyre komplexebb támadások jelennek meg. Ezen okokból kifolyólag létfontosságú a kibervédelem folyamatos fejlesztése, a kibervédelmi képesség, valamint a kiberbiztonság erősítése.

A közszolgálat kiemelt kibertámadási célpontnak tekinthető, ezért a szervezet egészét – a rendszer legkisebb elemétől kezdve, az információs rendszereken át, egészen az ott dolgozókig – fel kell készíteni egy esetleg támadás megelőzésére, illetve a már bekövetkezett eseményekre való reagálásra. A támadások jelentős része a felhasználók felkészületlenségét és biztonságtudatosságának hiányát célozza, éppen ezért az elsődleges cél a közszolgálatban dolgozók tudatosságának, kibervédelmi képességének kialakítása és folyamatos fejlesztése, amely eléréséhez elengedhetetlen egy olyan képzési forma megalkotása, aminek segítségével ezek a célok megvalósíthatók. Ezt szolgálja a közszolgálati kiberbiztonsági képzés megalkotása, amely a közszolgálatban dolgozó személyek kibervédelmi képességének kialakítására irányul, a közszolgálati kiberbiztonság fejlesztése érdekében. Krasznay Csaba cikke is rávilágít a kiberbiztonsági szakember képzésének szükségességére,

és rámutat számos olyan, a kibertérben történő eseményre, amelyek kétségkívül hatással vannak a fizikai világra.[2]

Korábbi tanulmányomban[3] azonosítottam a közszolgálati kiberbiztonsági képzés célcsoportját, valamint az e képzés során elsajátítandó ismerethalmazt, amely tartalmazza a NICE[4] Keretrendszerben előírt tudás-, feladat-, készség- és képességhalmazt, valamint egyéb ismeretköröket egyaránt. Ezt követően megvizsgáltam a hazai kiberbiztonsággal, információbiztonsággal kapcsolatos képzéseket, végül pedig definiáltam a közszolgálati kiberbiztonsági képzést, annak elemeit, követelményeit.

Ennek folytatásaként, jelen tanulmány célja a képzés meghatározásának nélkülözhetetlen elemeként értelmezhető hasonló nemzetközi képzések feltérképezése, e képzések kiválasztására és összehasonlítására alkalmazott módszer definiálása, valamint annak elemzése, hogy a feltárt nemzetközi képzésekben hogyan és milyen szinten jelennek meg a korábban a NICE Keretrendszer segítségével meghatározott ismeretek, az esetleges jó gyakorlatok átvétele érdekében.

### *1.1. Hipotézisek*

A nemzetközi képzések feltárása és a jó gyakorlatok hazai képzésbe való átültetése érdekében az alábbi hipotéziseket állítottam fel:

H1. Definiálható egy kiválasztási módszer és összehasonlítási stratégia, amely alapján azonosíthatók a közszolgálathoz kapcsolódó nemzetközi kiberbiztonsági képzések, és vizsgálható a hazai közszolgálati kiberbiztonsági képzés relevanciája nemzetközi szinten.

H2. A hazai közszolgálati kiberbiztonsági képzés releváns felsőoktatási képzés lehet nemzetközi szinten is.

H3. Fellelhetők olyan nemzetközi jó gyakorlatok, amelyeket érdemes átültetni a hazai képzésbe.

### *1.2. Kutatási módszertan*

A fentebb említett hipotézisek megválaszolására a következőkben bemutatott módszereket használtam fel, amelyeket az alábbiakban részletezek.

A H1 hipotézis esetén arra a kérdésre kerestem a választ, hogyan, milyen technikák segítségével célszerű azonosítani a nemzetközi képzéseket. E kiválasztási módszer meghatározását követően azt vizsgáltam, hogy milyen szempontok, elvárások, követelmények alapján érdemes összehasonlítani a feltárt nemzetközi képzéseket.

[2] Krasznay Csaba: A kiberbiztonság stratégiai vetületeinek oktatási kérdései a közszolgálatban. *Nemzet és Biztonság,* 10. (2017), 3. 38–53.

[3] Deák Veronika: A közszolgálati kiberbiztonsági képzés lehetősége Magyarországon. *Hadmérnök*, 15. (2020), 3.

[4] A NICE Keretrendszer a NIST (*National Institute of Standards and Technology*) egy speciális kiadványa, amely a kiberbiztonsághoz kapcsolódó munkaköröket kategorizálja, valamint többek között kifejti és leírja a kiberbiztonsági munkakörök tartalmát és e munkakörök betöltéséhez szükséges képességeket, készségeket, továbbá elsajátítandó ismeretköröket. Bővebb információ a következő weboldalon található: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

Ennek érdekében definiáltam egy összehasonlítási stratégiát, illetve annak tartalmát, elemeit. Ezen belül megvizsgáltam, hogy jelenleg a nemzetközi színtéren milyen kiberbiztonsággal, kibervédelemmel, illetve információbiztonsággal kapcsolatos képzések léteznek, ezt követően azonosítottam azokat, és feltérképeztem ezek tartalmát, alapvető elemeit, követelményeit, valamint azt, hogy mennyiben fedi le a NICE Keretrendszerben rögzített kiberbiztonsági munkakörhöz kapcsolódó ismerethalmazt, valamint milyen további ismeretköröket tartalmaz.

A H2 hipotézis esetén a H1 hipotézisben meghatározott keresési stratégia alapján kiválasztott képzéseket a H1 hipotézisben meghatározott összehasonlítási szempontok alapján hasonlítom össze. Amennyiben a korábban definiált hazai közszolgálati kiberbiztonsági képzés során átadandó tudáshalmaz legfeljebb az adott országra jellemző tudásanyagban tér el a nemzetközi képzések során átadandó tudáshalmaztól, a képzés nemzetközileg is relevánsnak tekinthető.

A H3 hipotézis esetén meghatároztam a H2 hipotézis során feltárt nemzetközi képzések azon elemeit, amelyek átültethetők a hazai közszolgálati kiberbiztonsági képzésbe.

## 2. Kapcsolódó munkák

Ahhoz, hogy a jelen tanulmányban ismertetett nemzetközi képzések tartalmának és összehasonlítása lehetőségeinek feltárása, továbbá a közszolgálati kiberbiztonsági képzés alapjául szolgáló NICE Keretrendszer elemzése megvalósulhasson, nélkülözhetetlen a releváns szakirodalom mélyebb vizsgálata.

### *2.1. Képzések összehasonlításával kapcsolatos tanulmányok*

K. Cabaj és szerzőtársai tanulmánya összehasonlító elemzést nyújt számos kiberbiztonsági mesterképzésről, azok felvételi követelményeiről, alapadatairól, tartalmáról, valamint a kiberbiztonsági érettség lényegéről. A cikkben összesen 21 mesterképzést vizsgáltak meg, amelyek kiválasztási kritériumai a következők voltak: a mesterképzés elnevezésében szerepel a kiberbiztonság kulcsszó, valamint ezek a képzések a 2017-es QS Egyetemi Világranglista első 700 egyetemén elérhetők. A kiválasztás fontos további szempontja volt a földrajzi elhelyezkedés, amely alapján különböző országok képzéseit is összehasonlították, így tíz képzést az Egyesült Államokból, ötöt az Egyesült Királyságból, valamint egyet-egyet Ausztráliából, Új-Zélandról, Észtországból, Hollandiából, Izraelből és Spanyolországból elemeztek. Az összehasonlítás során megvizsgálták a képzések felvételi követelményeit, időtartamát, illetve struktúráját. Ez utóbbi során elemezték a képzések felépítését, a teljesítendő kreditek és kurzusok számát, azok típusait, tehát például azt, hogy van-e a hallgatóknak lehetőségük szabadon választható kurzusok felvételére, vagy kizárólag kötelező tantárgyakat abszolválhatnak-e, továbbá fellelhetők-e specializációk, szakirányok az egyes képzések esetében. Ezt követően a szerzők bemutatták a kurzusok tartalmát,

azokat a témákat, területeket, amelyeket az egyes képzések érintenek. Végezetül a képzések abszolválásához szükséges feltételek elemzését végezték el.[5]

Bogdana Bystrova tanulmányában az Ukrajnában és az Egyesült Államokban elérhető kiberbiztonsági felsőktatási képzések általános összehasonlítását ismerteti, amelynek célja a hasonló oktatási programok szervezésével, megvalósításával, tartalmával és tanulmányi eredményeivel kapcsolatos alapképzések gyakorlati tapasztalatainak felhasználása az ukrán kiberbiztonsági oktatásban. A szerző az Észak-Karolinai Állami Egyetem kiberbiztonsági alapképzését és az ukrán kiberbiztonsági képzéseket általánosságban hasonlította össze. Az amerikai képzés esetében a kiválasztás fő szempontja az volt, hogy a vizsgált egyetem a U.S. News and World Report rangsorában az előkelő 31. helyet foglalta el a 150-ből. Bystrova ezt követően összehasonlította a képzéseket a teljesítendő kreditek száma, a tanulási és oktatásmódszertan, az értékelési folyamat, valamint a finanszírozási forma alapján. A szerző legfőbb célja az volt, hogy javaslatot tegyen az amerikai tapasztalatok alapján az ukrán kiberbiztonsági oktatás fejlesztésére, a hiányosságok és problémák orvoslására, az amerikai jó gyakorlatok átvételével.[6]

## *2.2. NICE Keretrendszer*

A NICE Keretrendszer alapvető referenciaként szolgál olyan munkaerő támogatásához, amely képes kielégíteni a szervezet kiberbiztonsági igényeit egy közös, következetes „lexikon" segítségével, amely leírja a lehetséges kiberbiztonsági munkát kategóriánként, szakterületenként, illetve munkakörönként.[7] Továbbá meghatározza az elsajátítandó kiberbiztonsági tudást, készségeket, képességeket és feladatokat az egyes munkakörökhöz. E keretrendszer kiváló alapként szolgálhat az általunk átadni kívánt tudás, készségek, képességek meghatározására, a kiberbiztonsági tantervek, tantárgyi adatlapok kidolgozására.

Alsmadi tanulmánya rámutat a jelenlegi kiberbiztonsági munkaerőhiány jelenségére, valamint arra, hogy folyamatos növekedés figyelhető meg a kiberbiztonsági szakemberek és készségek iránti igények tekintetében.[8] A cikk kiemelt hangsúlyt fektet a NICE és az ehhez hasonló keretrendszerek alkalmazására, továbbá azonosítja azokat a tényezőket, amelyek bizonyítják ezek szükségességét. Ilyen tényezőnek tekinthetők például az elméleti és gyakorlati képességek közötti egyensúly hiánya, az akadémia és az ipar közötti szakadék.[9]

Adriane C. Estes és szerzőtársai tanulmányukban feltárják, hogy a NICE kiberbiztonsági munkaerőrendszere hogyan igazítja és hangolja össze a kiberbiztonsági

[5] Krzysztof Cabaj et alii: Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computers & Security,* 75. (2018), 24–35.

[6] Bogdana Bystrova: Comparative Analysis of Curricula for Bachelor's Degree In Cyber Security in the USA and Ukraine, *Comparative Professional Pedagogy,* 7. (2017) 4. 114–119.

[7] William Newhouse et alii: *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.* U.S. Department of Commerce, 2017.

[8] Steve Morgan: Cybersecurity Jobs Report: A Special Report From the Editors at Cybersecurity Ventures, Cybersecurity Ventures, 31 May 2017.

[9] Izzat Alsmadi: Cybersecurity Education Based on the NICE Framework: Issues and Challenges. *ISACA Journal,* 3. (2018), 1–6.

munkákat a potenciális jelöltekkel. A szerzők bemutatják, milyen előnyei vannak egy szervezet számára a NICE Keretrendszer alkalmazásának, illetve hogyan segít azonosítani a kiberbiztonsági képességeket és megoldást találni e képességek hiányára, valamint folyamatos fejlesztésére nemcsak szervezeti, hanem globális szinten is.[10]

Herman és szerzőtársai arra keresik a választ, hogyan értelmezik a hallgatók a kiberbiztonság egyes fogalmait, illetve hogy a kiválasztott egyetemeken tanuló hallgatók milyen kiberbiztonsági ismeretekkel rendelkeznek. A tanulmány célja továbbá az esetleges hiányok feltérképezése interjúk segítségével. Az interjú elkészítésével a szerzők célja a hallgatók tudásának mérése, a hiányosságok feltárása, azok okainak azonosítása, valamint hosszú távon az oktatás fejlesztése.[11]

## 3. A közszolgálati kiberbiztonsági képzés és a NICE Keretrendszer

Korábbi tanulmányomban[12] már definiáltam a közszolgálati kibervédelmi képesség fejlesztését célzó közszolgálati kiberbiztonsági képzés fogalmát, illetve meghatároztam a képzés definiálásához elengedhetetlen kibervédelmi képességet, amelyeket jelen tanulmány teljes megértéséhez szükséges megismételni:

a) *kibervédelmi képesség:* azon személyes kibervédelmi képességek összességét jelenti, amely a kibertérből érkező jelenleg ismert vagy ismeretlen fenyegetések és támadások megelőzésére, felismerésére és megakadályozására irányul;
b) *közszolgálati kiberbiztonsági képzés:* a közszolgálatban dolgozó személyek kibervédelmi képességének kialakítására irányul a közszolgálati kiberbiztonság fejlesztése érdekében. A képzés jelen esetben egyfajta tudásátadás a közszolgálatban dolgozó személyek, döntéshozók számára, hogy a kibertérből érkező jelenleg ismert vagy ismeretlen fenyegetéseket és támadásokat képesek legyenek megelőzni, felismerni és megakadályozni;
c) *közszolgálati kiberbiztonsági képzés célja:* a közszolgálatban dolgozó személyek, döntéshozók ismeretének módszeres kiterjesztése a kibervédelmi képességhez szükséges tudással, amelynek segítségével a kibertérből érkező jelenleg ismert vagy ismeretlen fenyegetések és támadások kockázatát azonosíthatják, esetlegesen a végrehajtás során kisebb mértékben beavatkozhatnak.

Fontos volt meghatározni azokat az általános kiberbiztonsági feladatokat is, amelyeket a közszolgálati dolgozóknak szükséges végrehajtani akár a mindennapi munkájuk során, akár egy esetleges kibertámadás esetén. E feladatokat a korábban említett NICE Keretrendszer segítségével azonosítottam korábbi tanulmányomban,[13] és ezeket az alábbiakban ismertetem újra. E feladatok meghatározása elengedhetetlen volt

[10] Adriane C. Estes et alii: *Exploring How the NICE Cybersecurity Workforce Framework Aligns Cybersecurity Jobs with Potential Candidates*, Proceedings of the 14th International Conference on Frontiers in Education: Computer Science & Computer Engineering, Las Vegas, Nevada, CSREA, 2018.
[11] Travis Scheponik et alii: How Students Reason about Cybersecurity Concepts. *IEEE Frontiers in Education Conference (FIE)*, 1. (2016), 1–5.
[12] Deák Veronika: A közszolgálati kiberbiztonsági képzés lehetősége Magyarországon. *Hadmérnök*, 15. (2020), 3.
[13] Uo.

a képzés tartalmának kialakításához, így a nemzetközi jó gyakorlatok feltárásához is szükséges, amely már jelen tanulmány célja.

1. táblázat

*A közszolgálati kiberbiztonsági képzés során elsajátítandó tudáshalmaz*

Forrás: a szerző szerkesztése

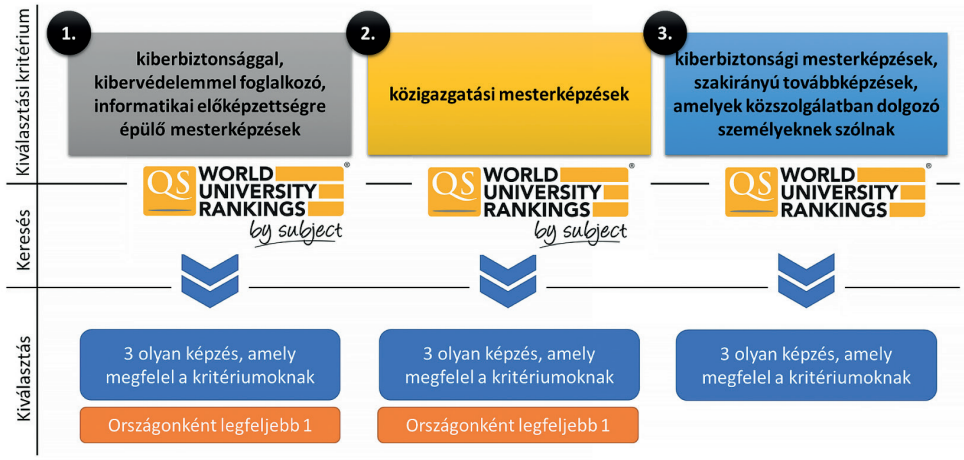
| **NICE által meghatározott tudáshalmaz (K)** |
|---|
| • számítógéphálózatokhoz kapcsolódó alapfogalmak ismerete<br>• kockázatkezelési folyamatok ismerete<br>• kiberbiztonsági, adatvédelmi jogszabályok, irányelvek, alapelvek ismerete<br>• kibertérből érkező fenyegetések ismerete<br>• vezeték nélküli technológiák ismerete |
| **NICE által nem definiált, de szükséges tudáshalmaz (K*)** |
| • az állami kibervédelmi rendszer ismerete<br>• a szervezeten belüli kiberbiztonsági és adatvédelmi felelős pozíciók ismerete<br>• a kibertámadások esetén alkalmazható technikák, eljárások ismerete<br>• az emberi tényező és a kiberbiztonság kapcsolódási pontjainak ismerete<br>• A kibertámadások mögött rejlő motivációk és pszichológiai tényezők ismerete. |

## 4. A képzések kiválasztásának módszere és az összehasonlítási stratégia

A közszolgálati kiberbiztonsági képzés hazai megvalósításához mindenképp szükséges feltérképezni és megvizsgálni a nemzetközi oktatásban megjelenő kiberbiztonsággal, információbiztonsággal kapcsolatos képzéseket. Ezen belül e képzések rendszerét, struktúráját, felépítését és tartalmát, annak érdekében, hogy a nemzetközi tapasztalatok vizsgálata során feltárt jó gyakorlatok esetleges átültetése megvalósulhasson a hazai oktatásban. Ennek keretében jelen pontban ismertetek néhány külföldi, a kibervédelmi képesség fejlesztését, illetve közszolgálati ismeretek átadását célzó képzési programot. Ezt követően az előző pontban felvázolt tudáshalmaz alapján összehasonlítom a kiválasztott nemzetközi példákat aszerint, hogy milyen mértékben jelenik meg a képzésben ezen ismeretek átadása.

### *4.1. A képzések kiválasztásának módszere*

Ahhoz, hogy bizonyítsam a közszolgálati kiberbiztonsági képzés fontosságát, szükségességét és relevanciáját hazánkban, a nemzetközi képzések több típusát is megvizsgáltam, majd ezeket összevetettem egy általam kialakított szempontrendszer alapján. A képzések kiválasztásának módszere a következőkben és az 1. ábrán ismertetett lépésekből állt.




1. ábra

*A képzések kiválasztásának módszere*

Forrás: a szerző szerkesztése

A képzések három csoportját különítettem el. Az első csoportba sorolhatók a kiberbiztonsággal, kibervédelemmel foglalkozó, informatikai előképzettségre épülő mesterképzések. A második kategóriát a közigazgatási mesterképzések alkotják. A harmadik csoport esetén olyan képzéseket kívántam megvizsgálni, amely az általam a korábbiakban felvázolt, közszolgálatban dolgozó személyek számára biztosítja a kibervédelmi képesség kialakítását. Olyan egyetemi szintű kiberbiztonsági mesterképzések, szakirányú továbbképzések után kutattam, amelyek konkrétan a közszolgálatban dolgozó személyeknek szólnak. Olyan képzést, amely teljesen megfelelne ezen elvárásoknak nem találtam, ezért olyan képzéseket kerestem, amelyek a kiberbiztonság és a közigazgatás elemeit együttesen tartalmazzák, így e képzések alkotják a harmadik csoportot.

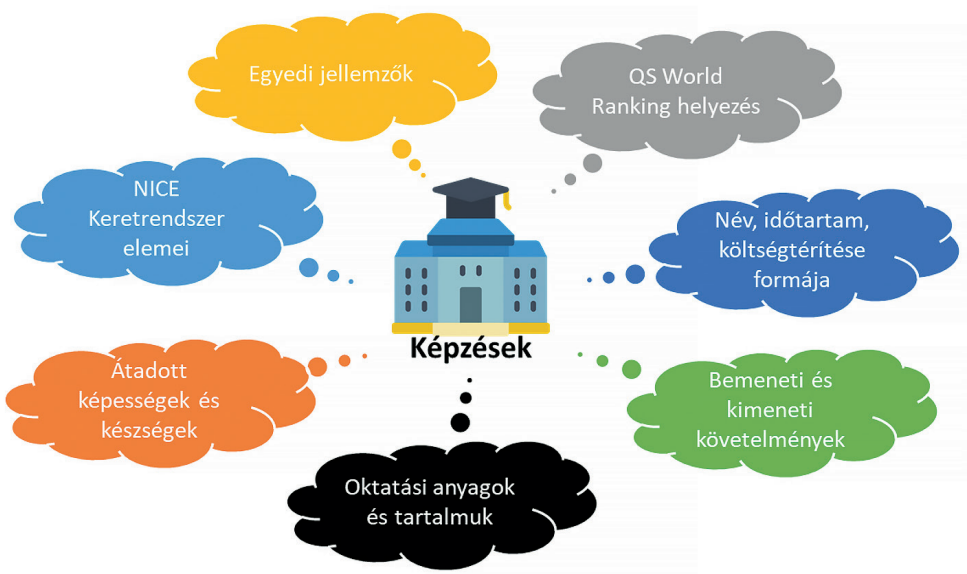
A képzések felkutatására a QS World University Rankings által felállított világszintű egyetemi rangsort használtam. Ez a ranglista a Quacquarelli Symonds (QS) által évente kiadott, a világ egyetemeinek rangsorát tartalmazó kiadványában is fellelhető. Honlapjukon megtalálható a világ egyetemeinek összesített rangsorolása, valamint a témánkénti és régiók szerinti rangsorok egyaránt. Ezenkívül a regisztrált felhasználók további információkhoz, elemzésekhez és közvetlen egyetemi összehasonlításokhoz is hozzáférhetnek.[14] Ezeknek köszönhetően a QS általános és téma szerinti rangsorait használtam a megfelelő képzések kiválasztásához. Ennek keretében bármely csoportot is vizsgáltam, megnéztem az általános és téma szerinti (például informatikatudomány) rangsort, és növekvő sorrendben elemeztem az egyetemeket azzal kapcsolatban, hogy található-e a képzési repertoárjukban az általam éppen vizsgálni kívánt képzés. Ennek célja az volt, hogy mindig az adott ország azon képzését válasszam ki,

[14] Bővebb információ a következő weboldalon található: *University Rankings.*

amely megfelel az általam támasztott elvárásoknak és a ranglistának megfelelően a legjobbnak minősül az adott országban. Ennek érdekében kilistáztam az általános és a téma szerinti rangsort, sorban haladva megvizsgáltam az országok egyetemeit, és minden országból egyet választottam ki, amely megfelel a feltételeknek. Minden csoporthoz három egyetemet társítottam a könnyű áttekintés érdekében, majd pedig egy általam felvázolt szempontrendszer szerint vizsgáltam meg a képzéseiket. Minden egyetem esetében a feltételeknek leginkább megfelelő képzést választottam ki bővebb ismertetés céljából. Az adott képzések konkrét vizsgálatánál az egyetemek honlapjai és az azokon megtalálható tantervek, tájékoztatóanyagok szolgáltak információval.

### *4.2. Összehasonlítási stratégia*

A kiválasztást követően a képzések összehasonlítására, a NICE Keretrendszer segítségével meghatározott tudáselemek képzési programban történő megjelenésére, a jó gyakorlatok azonosítására, valamint következtetések levonására az alábbi összehasonlítási stratégiát alkalmaztam.




2. ábra
*Összehasonlítási stratégia*
Forrás: a szerző szerkesztése

A képzések kiválasztását követően minden egyes képzést ugyanazon szempontrendszer szerint vizsgáltam meg, annak érdekében, hogy áttekinthetőbbek legyenek, illetve a képzések bemutatását követően össze is lehessen hasonlítani sajátosságaikat és meg lehessen határozni előnyeiket, hátrányaikat. Minden képzés esetében

vizsgáltam a képzés rangsorban betöltött helyét, pontos nevét, időtartamát, illetve a költségtérítés formáját. Ezt követően elemeztem a képzés feltételeit, a bemeneti követelményeket. Ez azért rendkívül fontos, mert például az első csoportban szereplő képzésekre kizárólag az informatikai, matematikai tudományok vagy ezekhez szorosan kapcsolódó tudományok képzési területén, alapképzésben szerzett oklevél birtokában lehet jelentkezni. Ezen kívül számos, a nemzetközi képzésekre jellemző egyéb feltételt határoztak meg, mint például az igazolt angol nyelvtudás, GRE/GMAT teszt,[15] a közigazgatási mesterképzések esetében pedig a munkatapasztalat és ajánlólevél. Ezenkívül megvizsgáltam a képzés típusát, az oktatott tantárgyakat, valamint azok tartalmát, elsajátítandó készségeket, képességeket. Ezután összehasonlítottam a képzéseket az alapján, hogy tantárgyi programjuk milyen mértékben tartalmazza a korábban a NICE Keretrendszer segítségével definiált tudáshalmazt. A vizsgálat során a képzés weboldalán található információkat, tematikát és elérhető oktatási anyagokat elemeztem, és egy táblázat segítségével szemléltettem, hogy az egyes képzések melyik tudáselemet tartalmazzák.

## 5. Nemzetközi képzések összehasonlítása

Jelen fejezet bemutatja a kiválasztási módszer segítségével feltárt kiberbiztonsággal kapcsolatos nemzetközi képzéseket, azok csoportosítását, tartalmát, alapvető elemeit és követelményeit. Ezt követően szemléltetem, hogy a korábban definiált tudáshalmaz egyes elemei megjelennek-e az egyes képzésekben.

### *5.1. A nemzetközi képzések feltérképezése*

Három csoportot azonosítottam a nemzetközi képzések feltérképezése során. Az első csoportba az informatikai alapképzettségre épülő, kiberbiztonsággal foglalkozó mesterképzések tartoznak. A második csoportba a klasszikus közigazgatási mesterképzések sorolhatók. A harmadik csoport esetén olyan képzéseket kutattam, amelyek az általam felvázolt közszolgálati kiberbiztonsági képzéssel hasonlóságot mutatnak.

#### 5.1.1. Informatikai alapképzettségre épülő kiberbiztonsággal foglalkozó mesterképzések

A képzések felkutatásához a QS informatikatudományok alapján történő rangsorolását vettem figyelembe. A ranglista 17. helyén a *University College of London* (*UCL*) található, amely a ranglista első, informatikai alapképzettségre épülő kiberbiztonsági képzéssel rendelkező egyeteme. Ezen a képzésen kiberbiztonsági szakértők a tudományosan alátámasztott elméleti ismereteket és a legmodernebb gyakorlati tudás

[15] A nemzetközi egyetemeken felvételi kritériumként alkalmazott szabványosított tesztek, amelyek az alkalmasság felmérésére szolgálnak.

egyensúlyát tanítják az újdonsült szakemberek számára.[16] A rangsorban a 18. helyet elfoglaló *Washingtoni Egyetem* (*University of Washington* – UW) a következő olyan egyetem, amely rendelkezik az informatikai előképzettség meglétéhez kötött kiberbiztonsággal foglalkozó mesterképzéssel. Kétéves kiberbiztonsági mérnök mesterképzésre jelentkezhet az, aki kiberbiztonsági szakemberré szeretne válni, és aki a technológia fejlődésével lépést tartva kívánja kombinálni az informatikai alapismereteket a modern kiberbiztonsági technológiák elméleti ismereteivel és gyakorlati tapasztalataival.[17] A rangsor 51–100. helyei közé sorolt hollandiai *Eindhoveni Műszaki Egyetem* (*Eindhoven University of Technology*) szintén kétéves mesterképzést biztosít az érdeklődők számára. Az információbiztonsági technológiák néven futó mesterképzés partnerintézményen, a Radboud Egyetemen keresztüli együttműködés keretében valósul meg. Ez a program széles körű áttekintést nyújt az információbiztonsági technológiák módszereiről, és magában foglalja a jog, a kiberbiztonság, az etika és az üzleti tevékenységek egyes szempontjait is.[18]

### 5.1.2. Klasszikus közigazgatási mesterképzések

E képzések kutatására a közpolitika és közigazgatás téma szerinti rangsort alkalmaztam. A ranglista 1. helyén álló amerikai *Harvard Egyetem tagintézménye, a Harvard Kennedy School* egy kétéves, szakmai tapasztalatra épülő közigazgatási mesterképzést indít, amely során a hallgatók egyéni tanulmányi terv segítségével fejleszthetik tudásukat, összpontosíthatnak személyes és szakmai törekvéseikre, valamint ismereteket szerezhetnek a különféle tudományágakról. A Harvard kurzusain a kibervédelem számos területével találkozhatnak a hallgatók, többek között a digitális kormányzattal, a kiberbiztonság technológiai, politikai és jogi aspektusával, valamint a kibertér és az információs műveletek kapcsolatának vizsgálatával is.[19] A ranglista 3. helyén található angliai *London School of Economics and Political Science*, rövidebben London School of Economics egy 19 hónapos közigazgatási mesterképzést biztosít az érdeklődők számára. A képzés célja a kormányzati és állami szervek, közintézmények és a magánszektor szakemberei számára olyan tudásfejlesztés megvalósítása, amely ötvözi az egyéni és csoportos munkatapasztalon alapuló problémamegoldást a közszférában és a politikában. A képzés tantervében kibervédelmi vonatkozások is megfigyelhetők, de kizárólag a kiberbiztonság jogi hátterének vizsgálatával kapcsolatban.[20] A rangsor első tíz helyén egy kivétellel angol és amerikai egyetemek váltakoznak. A 7. helyen a *Tokiói Egyetem* áll, amely kizárólag közpolitika témájú angol nyelvű mesterképzéssel rendelkezik. A 11. helyet az *Ausztrál Nemzeti Egyetem* (*The Australian National University*) foglalja el. Kétéves mesterképzés teszi lehetővé a tágan értelmezett közigazgatás megismerését azok számára, akik az állami, kormányzati szervekben szeretnének elhelyezkedni. A képzés kurzusai között kiberbiztonsági vonatkozásúról nem esett

[16] *Information Security MSc.* University College of London.
[17] *Master of Science in Cybersecurity Engineering.* University of Washington.
[18] *Mastertrack Information Security Technology.* Eindhoven University of Technology.
[19] *Master in Public Administration.* Harvard University.
[20] *Executive Master of Public Administration (EMPA).* London School of Economics and Political Science.

szó, de az ANU Kibervédelmi Intézete ilyen lehetőséget biztosít a kiberbiztonsággal mélyebben foglalkozni kívánó hallgatók számára.[21]

#### 5.1.3. Közigazgatási és kiberbiztonsági ismereteket egyaránt tartalmazó képzések

Végül olyan képzéseket kutattam, amelyek az általam felvázolt közszolgálati kiberbiztonsági képzéssel hasonlóságot mutatnak, tehát a közszolgálatban dolgozó szakemberek számára nyújtanak kibervédelmi ismereteket. Összességében megállapítható, hogy az ehhez hasonló képzések száma rendkívül alacsony, konkrét közszolgálati dolgozók számára kiberbiztonsági felsőoktatási képzést nem találtam, ezért olyan képzéseket kerestem, amelyek együttesen ötvözik a közigazgatási és kiberbiztonsági ismeretek elsajátítását. Éppen ezért, az ebbe a csoportba tartozó képzéstípusok alacsony számának köszönhetően nem volt lehetőség eltérő országok képzéseit vizsgálni. Az első ilyen képzés az amerikai *Arizonai Állami Egyetem* (*Arizona State University* – ASU) kiberbiztonsági politika és menedzsment online elvégezhető mesterképzése, amely egyaránt ötvözi a kiberbiztonsági és a közigazgatással, közpolitikával kapcsolatos ismereteket.[22] A következő ilyen a San Bernardinó-i *Kaliforniai Állami Egyetem* (*California State University, San Bernardino* – CSUSB) olyan kétéves közigazgatási mesterképzést nyújt, amelyen kiberbiztonsági szakirány választható, és amelynek célja, hogy a közszolgálatban vezető szerepek betöltésére készítse fel a hallgatókat.[23] Ezt követi a szintén amerikai *Carnegie Mellon Egyetem*, ahol információbiztonsági politika és menedzsment szakirányú továbbképzéssel biztosítják az információbiztonsági és közigazgatási, közpolitikai ismeretek elsajátítását. Jelen képzés célja, hogy olyan szakembereket képezzen, akik képesek lesznek az állami és magánszféra szervezeteit, valamint más személyeket biztonságosabbá, biztonságtudatosabbá tenni. Míg más programok az információbiztonság technikai mérnöki megközelítéseit hangsúlyozzák, addig jelen képzés a technikai készségeket a közpolitikai, szakpolitikai, stratégiai és menedzsmentkurzusok széles körével ötvözi.[24]

### *5.2. Nemzetközi képzések alapadatainak vizsgálata*

Az összehasonlítás során a képzések alapadatait vizsgáltam meg, amelyeket a 2. táblázat szemléltet. A táblázatban látható az egyes képzések időtartama (I.) években megadva; a rangsorban betöltött helyezés (R), amely szám mögött található a rangsor típusa, amely lehet *informatikai tudományok* (I), *közigazgatás és közpolitika* (K), esetleg *általános* (Á); a finanszírozási forma (Fin.), amely alapján a képzés lehet *állami ösztöndíjjal támogatott* (ösz.), *önköltséges* (önk.) vagy *mindkettő* (ösz./önk.); végül a bemeneti követelmények.

[21] *Master of Public Administration.* Australian National University.
[22] *Cybersecurity policy and management (MA).* Arizona State University.
[23] *Master of Public Administration.* California State University, San Bernardino.
[24] *Information Security Policy & Management (MSISPM).* Carnegie Mellon University.

2. táblázat

*A vizsgált nemzetközi képzések alapadatai*

Forrás: a szerző szerkesztése

| | Képzés | I. | R. | Fin. | Bemeneti követelmény |
|---|---|---|---|---|---|
| **Informatikai alapképzettségre épülő kiberbiztonsági képzések** | UCL | 1 | 17 (I) | önk. | Informatikai, elektronikai mérnöki és matematikai területeken alapképzésben szerzett oklevél, angol nyelvtudás (pl. IELTS, TOEFL) |
| | UW | 2 | 18 (I) | önk. | Informatikai területen alapképzésben szerzett oklevél, angol nyelvtudás, 3,0 feletti görgetett átlag |
| | EUT/RU | 2 | 51-100 (I) | önk. | Informatikai, matematikai, információbiztonsági vagy kapcsolódó területeken alapképzésben szerzett oklevél, külföldi hallgatók esetében az alapképzésben szerzett oklevelet egyedileg bírálják el, személyes interjú |
| **Klasszikus közigazgatási mesterképzések** | HU HKS | 1 | 1 (K) | önk. | Alapképzésben szerzett oklevél + 4 mesterképzési szakon indított kurzus teljesítése/ mesterképzésben szerzett oklevél, 3 év szakmai tapasztalat, GRE/GMAT-teszt, angol nyelvtudás |
| | LSE | 1,5 | 3 (K) | önk. | Alapképzésben szerzett oklevél, 2 ajánlólevél, magas szintű angol nyelvtudás, 5 év munkatapasztalat |
| | ANU | 2 | 11 (K) | önk. | Alapképzésben szerzett oklevél, szakmai tapasztalat, 7 pontos GPA, angol nyelvtudás |
| **Közszolgálat + kiberbiztonság** | CMU HC | 2 | 48 (Á) | önk. | Alapképzésben szerzett oklevél, szakmai tapasztalat, angol nyelvtudás (TOEFL, IELTS), GRE-teszt |
| | ASU | 2 | 215 (Á) | önk. | Kriminológia, igazságügyi igazgatás, közigazgatás, közszolgálat, szociológia, közbiztonsági/tűzvédelmi menedzsment, környezetvédelem, közegészségügy, alkalmazott tudományok, földrajz vagy más szorosan kapcsolódó területen alapképzésben szerzett oklevél, 2 éves szakmai tapasztalat, 2 ajánlás, 3,00 GPA, angol nyelvtudás |
| | CSUSB | 2 | – | önk. | Alapképzésben szerzett oklevél, szakmai tapasztalat, statisztikai előképzettség (bevezető statisztikai kurzus) |

Fontos kiemelni, hogy természetesen léteznek egyéb, a közszolgálatban dolgozó személyek számára elérhető továbbképzések, tréningek, különféle oktatások, azonban jelen tanulmány célja e vonatkozásban kizárólag a felsőoktatási képzési rendszerbe illeszkedő képzéstípusok elemzése.

### *5.3. Nemzetközi képzések ismerethalmazának vizsgálata*

Miután bemutattam a nemzetközi felsőoktatásban elérhető kiberbiztonsággal foglalkozó képzéseket, szeretném megvizsgálni, hogy létezik-e olyan képzés, amely fedi a 3. fejezetben azonosított ismeretek körét. Ehhez megvizsgáltam, hogy az egyes képzések oktatási anyaga tartalmaz-e részletes képzési anyagot a K1–K5 és K1*–K5* tudáshalmazzal kapcsolatban.

A vizsgálat során a képzések weboldalán található információkat, tematikákat és elérhető oktatási anyagokat vizsgáltam meg. A vizsgálat eredményét a 3. táblázat tartalmazza, ahol a sorok az egyes képzéseket, az oszlopok az azonosított tudáshalmazt jelölik. Egy cellába akkor került ✓ jel, ha az adott sorban található képzés oktatja az adott oszlopban található ismeretanyagot. Ha egy cellába – jel került, akkor nem található információ azzal kapcsolatban, hogy az adott ismeretkört is oktatják az adott képzésen.

3. táblázat

*A vizsgált nemzetközi kiberbiztonsággal kapcsolatos képzések összehasonlítása tudáselemek szerint*

Forrás: a szerző szerkesztése

| Képzési forma | Képzés rövidítése | K1 | K2 | K3 | K4 | K5 | K1* | K2* | K3* | K4* | K5* |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **BSc/ BA** | NKE KNY | ✓ | – | ✓ | ✓ | ✓ | ✓ | – | ✓ | – | ✓ |
| | ÓE BM | ✓ | ✓ | ✓ | ✓ | – | – | – | ✓ | ✓ | ✓ |
| **MSc/MA** | NKE KB | ✓ | ✓ | ✓ | ✓ | – | – | – | – | ✓ | – |
| | NKE VIKR | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | – |
| **Szakirányú továbbképzés** | NKE EIB | ✓ | ✓ | ✓ | – | – | – | – | – | – | – |
| | ELTE ASZ | ✓ | – | ✓ | ✓ | – | – | ✓ | ✓ | – | – |
| | ÓE KSZ | ✓ | – | ✓ | ✓ | ✓ | – | – | – | – | – |
| | ÓE ISZ | ✓ | ✓ | ✓ | – | – | – | – | – | ✓ | – |
| | GDF AIM | ✓ | – | ✓ | – | – | – | – | ✓ | – | – |
| | NKE EUA | – | ✓ | ✓ | – | – | ✓ | ✓ | – | – | – |

A vizsgált képzések közül egyik képzés tantervében sem jelent meg az állami kibervédelmi rendszer, valamint a szervezeten belüli kiberbiztonsági és adatvédelmi felelős pozíciók ismerete. Ennek oka lehet, hogy ezen ismeretkörök egyediek, országonként változhatnak, ezért olyan általános képzések esetében, mint amelyeket jelen vizsgálat tartalmaz, nem indokolt nemzetspecifikus ismeretek átadása.

A vizsgált képzések közül a University College of London információbiztonsági mesterképzése, az Eindhoven University of Technology információbiztonsági technológiák mesterképzése, a California State University közigazgatási mesterképzés kiberbiztonsági szakiránya, valamint a Carnegie Mellon University Heinz College információbiztonsági politika és menedzsment mesterképzése fedi le a legtöbb korábban meghatározott tudáshalmazt. Több különböző ország képzése is kifejezetten nagy mértékben tartalmazza a vizsgált témaköröket, ami azt jelenti, hogy egy kiberbiztonsági

képzés, amely ezen ismereteket tartalmazza, nemcsak hazánkban, hanem nemzetközi szinten is relevánsnak tekinthető.

A nemzetközi szinten elérhető klasszikus közigazgatással kapcsolatos mesterképzések többségében nem tartalmaznak kiberbiztonsági ismereteket. Ez azt a nemzetközi gyakorlatot szemlélteti, hogy a kiberbiztonsági ismereteket nem a klasszikus közigazgatási mesterképzésekbe kell integrálni, hanem külön kiberbiztonság-specifikus képzéseket kell létrehozni, amely ötvözi a közszolgálati és kiberbiztonsági ismereteket egyaránt.

Összességében megállapítható, hogy a korábban meghatározott tudáselemek jelentős része (két elem kivételével az összes) megjelenik valamely vizsgált képzés képzési tervében, ami azt mutatja, hogy ezen ismeretkörök a közszolgálati kiberbiztonsági képzés szempontjából is relevánsnak tekinthetők. A táblázat alapján egyébként az is látható, hogy nincs olyan tudáselem, amely minden vizsgált képzés tantárgyi programjában szerepelne. Ez mutatja a képzések felépítésének, meghatározott előképzettségeinek, feltételeinek és típusainak különbségét.

Fontos kiemelni, hogy a jelenlegi képzési rendszer fázisaiban átadott ismeretek mennyisége és mélysége eltérő, jelentősen befolyásolja azt a képzési forma struktúrája, követelményei, időtartama, valamint a képzés során elsajátítandó készségek, képességek, ismeretek halmaza. Ezenkívül befolyásoló tényezőnek tekinthető a képzés munkarendje is, tehát hogy a hallgatók nappali, levelező vagy online munkarendben teljesítik az adott képzést.

## 6. Nemzetközi jó gyakorlatok azonosítása

A közszolgálati kiberbiztonsági képzés hazai megvalósításához elengedhetetlen feltérképezni és megvizsgálni a nemzetközi oktatásban megjelenő kiberbiztonsággal, információbiztonsággal kapcsolatos képzéseket, azok struktúráját, tartalmát és tapasztalatait. Az előző pontban bemutatott képzések összehasonlító elemzése során számos jó gyakorlatot azonosítottam, amelyeknek átültetése a hazai képzésbe jelentősen hozzájárulhat a nemzetközi szintű képzés definiálásához. A feltárt jó gyakorlatokat a következőkben ismertetem.

A cél az volt, hogy olyan nemzetközi gyakorlatokat azonosítsak, amelyek bizonyíthatóan hozzájárulnak az adott felsőoktatási intézmény minőségi színvonalának emeléséhez. Éppen ezért olyan eljárásokat, eszközöket, módszereket és egyéb gyakorlatokat kerestem, amelyek pozitívan képesek befolyásolni a hatékony elméleti és gyakorlati tudásátadást. A nemzetközi tapasztalatok implementálásának előnye, hogy ezek már olyan nemzetközi színtéren kipróbált és bevált gyakorlatok, amelyek hatékonyságát az egyetemek eredményei is igazolnak. Fontos azonban megemlíteni, hogy komplex oktatási rendszerek integrálása nem minden esetben valósítható meg egy az egyben, mivel minden országnak, így azok felsőoktatási rendszereinek is más és más sajátosságai, hátterei, követelményei és társadalmi-gazdasági viszonyai vannak. Éppen ezért fontos, hogy a saját körülményeinket, felsőoktatási rendszereink felépítését, működését figyelembe véve szükséges e tapasztalatokat adaptálni. A jó gyakorlatok implementálása során kiemelt figyelmet kell fordítani azok technikai,

szervezési és anyagi feltételeire is, csak ezek tisztázását követően kezdődhet meg ezek alkalmazása. A nemzetközi gyakorlatok átültetését követően kulcsfontosságú ezek hatékonyságának ellenőrzése és értékelése, valamint a tapasztalatok folyamatos rögzítése.

Az azonosított jó gyakorlatok az alábbiak:

a) hallgatók és tanárok, karok, intézetek közötti szoros kapcsolattartás;
b) hallgatók közötti együttműködés;
c) gyakorlati oktatás, labor;
d) gyakorlati projektmunka;
e) esettanulmányok segítségével történő oktatás;
f) állami vagy magánszférában dolgozó, kiberbiztonsággal foglalkozó szakértők meghívott előadóként való részvétele az oktatásban.

A jó gyakorlatok közé tartozik a hallgatók és a tanárok, karok, illetve intézetek, tanszékek közötti szoros kapcsolattartás elősegítése, folyamatos biztosítása. Ennek célja, hogy a hallgatók félévi munkája során felmerülő problémák, nehézségek leküzdésében, valamint a munka folytatásában megfelelő szakmai segítséget kaphassanak.

A következő tapasztalat szorosan kapcsolódik az előbb említetthez, hiszen lényege, hogy a hallgatók megfelelő támogatást kapjanak tanulmányaikhoz. A hallgatók közötti együttműködés erősítésének célja, hogy fejlessze a hallgatók együttműködő-képességét, valamint a saját ötletek csoportban való megosztásával hozzájáruljon a gondolkodás és a megértés elmélyítéséhez.

A gyakorlati oktatás, illetve labormunkák előnye, hogy a hallgatók a magán- és állami szférában felmerülő konkrét problémákkal, feladatokkal találkozhatnak, így valódi és releváns szakmai tapasztalatot szerezhetnek. Ezenkívül a kiberbiztonsággal összefüggő ismeretek elsajátítása során elengedhetetlen a különféle infokommunikációs technológiák, támadási és védelmi alternatívák konkrét műszaki környezetben való szimulálása. Így e gyakorlati feladatok és laborgyakorlatok nélkülözhetetlen részét képezik a kiberbiztonsági oktatásnak.

A gyakorlati projektmunka lényege egy informatikára, kiberbiztonságra specializálódott projekt végrehajtása a képzés végén, amely során egy valós ügyféllel, szervezettel együttműködés keretében egy aktuális problémára, kihívásra keresik a hallgatók a választ.

Az esettanulmányok segítségével végzett oktatás számos egyetemre jellemző sajátosság, amelynek lényege, hogy egy konkrét, gyakorlati példa segítségével szemléltesse az átadni kívánt ismeretanyagot, valamint egy adott kihívás, probléma megoldásának lehetőségeit a hallgatók számára. Ezen oktatási módszer előnye, hogy fejleszti a hallgatók problémamegoldó, analitikus, érvelési és együttműködési képességeit, továbbá hozzájárul valós gyakorlati problémák megismeréséhez.

Az aktuális kiberbiztonsági kihívások szemléltetését számos egyetem állami vagy magánszférában dolgozó kiberbiztonsággal foglalkozó szakértők meghívott előadóként való részvételével biztosítja. E módszer szintén hozzájárul a valós, gyakorlati problémák és azok megoldásainak megismeréséhez, valamint a munkaerőpiacon szerzett tapasztalatok megosztásához.

## 7. Következtetések

Az előző fejezetek egyfajta előkészítései és egyben bizonyításai voltak a hipotézisek megválaszolásának. Jelen fejezet célja, hogy az első fejezetben megadott hipotézisekre egyértelmű választ adhassak.

Ezek alapján a H1 hipotézis helyes, és ennek bizonyítása a 3. fejezetben meghatározott keresési stratégia és összehasonlítási szempontrendszer, amely alapján kiberbiztonsággal kapcsolatos nemzetközi képzések a célnak megfelelően összehasonlítók.

A H2 hipotézis teljesülését bizonyítja az 5. fejezetben található, a vizsgált nemzetközi képzések ismerethalmazának vizsgálatán alapuló összehasonlítás (3. táblázat), amelynek eredményeként megállapítható, hogy egy hazai közszolgálati kiberbiztonsági képzés a nemzetközi szinten is releváns képzésnek minősül, hiszen a korábban meghatározott tudáselemek jelentős része (két elem kivételével az összes) megjelenik valamely vizsgált képzés képzési tervében. Csak azon ismeretkörök nem jelennek meg (K1* és K2*), amelyek országonként eltérőek.

Végül a H3 hipotézis szintén igaznak bizonyult, ennek bizonyítása a 6. fejezetben található meg, vagyis fellelhetők olyan nemzetközi jó gyakorlatok, amelyeket érdemes átültetni a hazai képzésbe.

## 8. Összegzés és jövőbeni tervek

A kiberbiztonság egy gyorsan változó, folyamatosan fejlődő és bővülő terület, amely egyre újabb és újabb kihívásokat, illetve fenyegetéseket tartogathat számunkra. A közszolgálati kiberbiztonsági képzés megvalósítására a közszolgálati kiberbiztonság fejlesztése érdekében van szükség, hiszen a kibertér és ennek következtében a kibertérből érkező fenyegetések a mindennapi élet természetes velejárójává váltak.

Jelen tanulmányban bizonyítottam, hogy a közszolgálati kiberbiztonsági képzés nemzetközi szinten is releváns képzésnek tekinthető. A vizsgált képzések képzési tervében szinte az összes korábban definiált tudáselem megjelenik, amely azt mutatja, hogy ezen ismeretkörök a közszolgálati kiberbiztonsági képzés esetében is helytállók.

A bizonyítás során az alábbi lépéseket hajtottam végre:

- Definiáltam a nemzetközi képzések feltérképezéséhez szükséges kiválasztási módszert, amelynek segítségével azonosíthatók a közszolgálati kiberbiztonsági képzés szempontjából releváns felsőoktatási képzések. A módszer három lépésből áll, az első lépésben határoztam meg a kiválasztási kritériumot, amelynek felkutatása a QS World University Rankings által felállított világszintű általános és téma szerinti egyetemi rangsor segítségével valósult meg. A harmadik lépésben az adott kiválasztási kritériumnak megfelelően három képzést választottam ki.
- Meghatároztam a képzések összehasonlító elemzésére szolgáló összehasonlító stratégiát, amelyet a NICE Keretrendszer segítségével meghatározott tudáselemek képzési programban való megjelenésére, a jó gyakorlatok azonosítására, valamint következtetések levonására alkalmaztam. Ennek keretében a kiválasztott képzéseket ugyanazon szempontrendszer szerint vizsgáltam meg. Minden

képzés esetében azonosítottam a képzés rangsorban betöltött helyét, pontos nevét, időtartamát, illetve a költségtérítés formáját. Ezt követően elemeztem a képzés feltételeit, a bemeneti követelményeket, a képzés típusát, az oktatott tantárgyakat, valamint azok tartalmát, elsajátítandó készségeket, képességeket. Ezután összehasonlítottam a képzéseket az alapján, hogy tantárgyi programjuk milyen mértékben tartalmazza a korábban a NICE Keretrendszer segítségével definiált tudáshalmazt.

- Megvizsgáltam a feltárt nemzetközi képzések tartalmát, elemeit és követelményeit, ez alapján pedig azonosítottam e képzések jó gyakorlatait, amelyeknek átültetése a hazai képzésbe jelentősen hozzájárulhat a nemzetközi szintű képzés definiálásához. A nemzetközi tapasztalatok implementálásának előnye, hogy ezek már olyan nemzetközi színtéren kipróbált és bevált gyakorlatok, amelyek hatékonyságát az egyetemek eredményei is igazolták.

A kutatás folytatásaként szükséges még a képzés konkrét tematikájának kidolgozása, a számonkérések típusának meghatározása az egyes témakörökhöz, végül a képzési célok támogatásához szükséges műszaki környezet definiálása.

## Felhasznált irodalom


Alsmadi, Izzat: Cybersecurity Education Based on the NICE Framework: Issues and Challenges. *ISACA Journal*, 3. (2018), 1–6.

Bystrova, Bogdana: Comparative Analysis of Curricula for Bachelor's Degree In Cyber Security in the USA and Ukraine. *Comparative Professional Pedagogy,* 7. (2017), 4. 114–119. DOI: https://doi.org/10.1515/rpp-2017-0058

Cabaj, Krzysztof – Dulce Domingos – Zbigniew Kotulski – Ana Respício: Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computers & Security,* 75. (2018), 24–35. DOI: https://doi.org/10.1016/j.cose.2018.01.015

*Cybersecurity policy and management (MA).* Arizona State University. Elérhető: https://asuonline.asu.edu/online-degree-programs/graduate/cybersecurity-policy-and-management-ma/ (A letöltés dátuma: 2020. 04. 16.)

Deák Veronika: A közszolgálati kiberbiztonsági képzés lehetősége Magyarországon. *Hadmérnök*, 15. (2020), 3. DOI: https://doi.org/10.32567/hm.2020.3.9

Estes, Adriane C. – Dan J. Kim – Andrew T. Yang: *Exploring How the NICE Cybersecurity Workforce Framework Aligns Cybersecurity Jobs with Potential Candidates.* Proceedings of the 14th International Conference on Frontiers in Education: Computer Science & Computer Engineering, Las Vegas, Nevada, CSREA, 2018.

*Executive Master of Public Administration (EMPA).* London School of Economics and Political Science. Elérhető: www.lse.ac.uk/school-of-public-policy/empa (A letöltés dátuma: 2020. 04. 16.)

*Information Security MSc.* University College of London. Elérhető: www.ucl.ac.uk/prospective-students/graduate/taught-degrees/information-security-msc (A letöltés dátuma: 2020. 04. 13.)

*Information Security Policy & Management (MSISPM).* Carnegie Mellon University. Elérhető: www.heinz.cmu.edu/programs/information-security-policy-management-master/ (A letöltés dátuma: 2020. 04. 16.)
Krasznay Csaba: A kiberbiztonság stratégiai vetületeinek oktatási kérdései a közszolgálatban. *Nemzet és Biztonság,* 10. (2017), 3. 38–53.
*Master in Public Administration.* Harvard University. Elérhető: www.hks.harvard.edu/educational-programs/masters-programs/master-public-administration (A letöltés dátuma: 2020. 04. 16.)
*Master of Public Administration.* Australian National University. Elérhető: https://programsandcourses.anu.edu.au/program/MPUAD (A letöltés dátuma: 2020. 04. 16.)
*Master of Public Administration.* California State University, San Bernardino. Elérhető: https://jhbc.csusb.edu/mpa (A letöltés dátuma: 2020. 04. 16.)
*Master of Science in Cybersecurity Engineering.* University of Washington. Elérhető: www.uwb.edu/cybersecurity (A letöltés dátuma: 2020. 04. 13.)
*Mastertrack Information Security Technology.* Eindhoven University of Technology. Elérhető: www.tue.nl/en/education/graduate-school/mastertrack-information-security-technology/ (A letöltés dátuma: 2020. 04. 13.)
Morgan, Steve: Cybersecurity Jobs Report: A Special Report From the Editors at Cybersecurity Ventures, Cybersecurity Ventures, 31 May 2017.
Newhouse, William – Stephanie Keith – Benjamin Scribner – Greg Witte: *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.* U.S. Department of Commerce, 2017. DOI: https://doi.org/10.6028/NIST.SP.800-181
Scheponik, Travis – Alan T. Sherman – David DeLatte – Dhananjay Phatak – Linda Oliva – Julia Thompson – Geoffrey L. Herman: How Students Reason about Cybersecurity Concepts. *IEEE Frontiers in Education Conference (FIE)*, 1. (2016), 1–5. DOI: https://doi.org/10.1109/FIE.2016.7757363
*University Rankings.* Elérhető: www.topuniversities.com/university-rankings (A letöltés dátuma: 2020. 04. 13.)