HADMÉRNÖK
VÉDELEMINFORMATIKA

15. évfolyam (2020) 3. szám 157–178.
DOI: 10.32567/hm.2020.3.9

Deák Veronika[1]

A közszolgálati kiberbiztonsági képzés lehetősége Magyarországon

The Opportunities of Developing a Cyber Security Training Programme for Public Service in Hungary

A közszolgálat kiemelt célpontja a kibertámadásoknak, így ezek megelőzése és eredményes elhárítása érdekében különösen nagy hangsúlyt kell fektetni a különféle szervezetek védelmi képességeinek kialakítására és folyamatos fejlesztésére. Ennek részeként értelmezhető a lehetséges támadási alternatívák megismerését és alkalmazhatóságát célzó közszolgálati kiberbiztonsági képzés megalkotása.
A képzési program megalkotása során fel kell tárni a program megvalósíthatóságának lehetőségeit, illetve a hasonló hazai képzéseket a képzés szükségességének igazolása és az esetleges „jó gyakorlatok" átvétele érdekében.
Jelen tanulmány a hazai kiberbiztonsági, kibervédelmi képzéseket, ezen belül azok tartalmát, elemeit, az esetleges hiányosságait vizsgálja, valamint definiálja a közszolgálati kiberbiztonsági képzés fogalmát és meghatározza annak elemeit, követelményeit.

Kulcsszavak: **közszolgálat, kiberbiztonság, kibervédelem, információbiztonság, adatvédelem, képzési program, közszolgálati kiberbiztonsági képzés, hazai képzések, hazai kiberbiztonsági képzések, NICE-keretrendszer, oktatás**

The public service is a key target of cyber attacks. In order to prevent and effectively tackle such attacks, organisations should continuously develop their defense capabilities. As part of this development, a public service cyber security training programme is needed, that aims at learning about and applying possible cyber attack alternatives. During the specification of the programme, domestic cyber security programmes should be explored in order to prove the need for the training and to adopt possible 'good practices'. In this paper, I evaluate the Hungarian cyber security and cyber defence programmes including their content, key elements and possible

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

shortcomings. Finally, I define the purpose of public service cyber security training programme and identify its elements and requirements.

Keywords: **public service, cyber security, cyber defence, information security, data protection, training programme, domestic training programmes, domestic cyber security training programmes, NICE Framework, education**

Bevezetés

Az egyre újabb és újabb számítástechnikai, illetve elektronikai eszközök a mindennapjaink részeivé váltak. A különböző infokommunikációs eszközök, illetve az információs rendszerek megjelenése és fejlődése nemcsak előnyökkel járnak, hanem számos veszélyt is rejthetnek magukban. Naponta követnek el kibertámadásokat a különféle bizalmas információk megszerzése érdekében, állami és nem állami szerveket egyaránt célozva. Éppen ezért szükségszerű, hogy ezek megelőzése és eredményes elhárítása érdekében növeljük a különféle szervezetek védelmi képességeit.

A kibertámadások jelentős gazdasági, politikai, nemzetbiztonsági, de a társadalomra is kiterjedő káros következményt idézhetnek elő. Az elmúlt évek tapasztalatai alapján elmondható, hogy a közszolgálat kiemelt célpontja a kibertámadásoknak, így különösen nagy hangsúlyt kell fektetni a lehetséges támadási alternatívák megismerésére és alkalmazhatóságára a hatékony védelem kialakítása érdekében. A közszolgálat fejlesztéséhez a különféle infrastruktúrák védettségének teszteléséhez szükség van a védelmi képesség képzési lehetőségeinek meghatározására, a kockázatok és sebezhetőségek feltárása érdekében. A közszolgálatban dolgozó személyek nap mint nap részt vesznek a döntéshozatalban, amiket döntően befolyásolnak a kibervédelemmel kapcsolatos stratégiai kérdések. Ahhoz, hogy az infrastruktúrák tesztelése és ellenőrzése, valamint az esetleges támadások elhárítása és megelőzése hatékonyan, illetve eredményesen megvalósulhasson, továbbá a döntéshozatalban megfelelő lépéseket hajtsanak végre, elengedhetetlen a szakértők bevonása.

A kiberbiztonsággal, információbiztonsággal foglalkozó szakemberek hiánya indokolttá teszi e terület képzési programjának kidolgozását a közszolgálat fejlesztése érdekében. A jelenlegi hazai helyzet alapján számos olyan, a kibertámadási és védelmi képesség kialakítását szolgáló képzés létezik, amelyek csak informatikai tudást adnak át, vagy csak jogi ismeretek elsajátítását célozzák meg. Azonban a közszolgálatban dolgozók számára olyan képzés, amely e két terület megfelelő részét együttesen fedné le, jelenleg hazánkban nem elérhető.

Mindezek miatt szükséges egy olyan képzési program megalkotása a hazai képzési környezetben, amely lehetőséget nyújt a közszolgálatban dolgozó, nem informatikai végzettségű személyek kibervédelmi képességének kialakítására. E képesség alatt a személyes kibervédelmi ismeretek és képességek összessége érthető. A kiberbiztonsági képzés azoknak a személyeknek szól, akik nem rendelkeznek a szükséges alapismeretekkel, nem mozognak a témában otthonosan.

A képzésnek nemzetközi szinten is elfogadottnak kell lennie. Emiatt érdemes a NICE Cybersecurity Workforce[2] keretrendszer által definiált, a kiberbiztonsághoz kapcsolódó munkaköröket tanulmányozni, illetve megvizsgálni az e munkakörök betöltéséhez szükséges képességeket, készségeket, továbbá elsajátítandó ismeretköröket.

Jelen tanulmány célja a szükséges ismeretek, készségek és képességek azonosítása, kibervédelem, kiberbiztonság hazai képzéseinek feltérképezése és azok összehasonlítása az átadott tudásanyagok alapján, illetve a közszolgálati kiberbiztonsági képzés meghatározása. A képzés kialakításához elengedhetetlen a hasonló képzések felkutatása, az esetleges „jó gyakorlatok" átvétele érdekében, azonban terjedelmi okok miatt jelen tanulmány csak a hazai képzések feltárását tűzte ki célul, a nemzetközi képzések vizsgálata egy további tanulmány tartalmát képezi.

Hipotézisek

A képzés szükségességének igazolására és definiálására az alábbi hipotéziseket állítottam fel:

H1. A közszolgálatban dolgozó személyek számára szükséges a NICE által meghatározott és egyéb a NICE által nem definiált ismerethalmaz elsajátítása.

H2. A hazai felsőoktatási rendszerben jelenleg nem létezik olyan képzés, amely lefedi a közszolgálati kibervédelmi képesség kialakításához szükséges alapismereteket.

H3. Definiálható a magyar közszolgálat számára egy felsőoktatási kiberbiztonsági képzés.

Kutatási módszertan

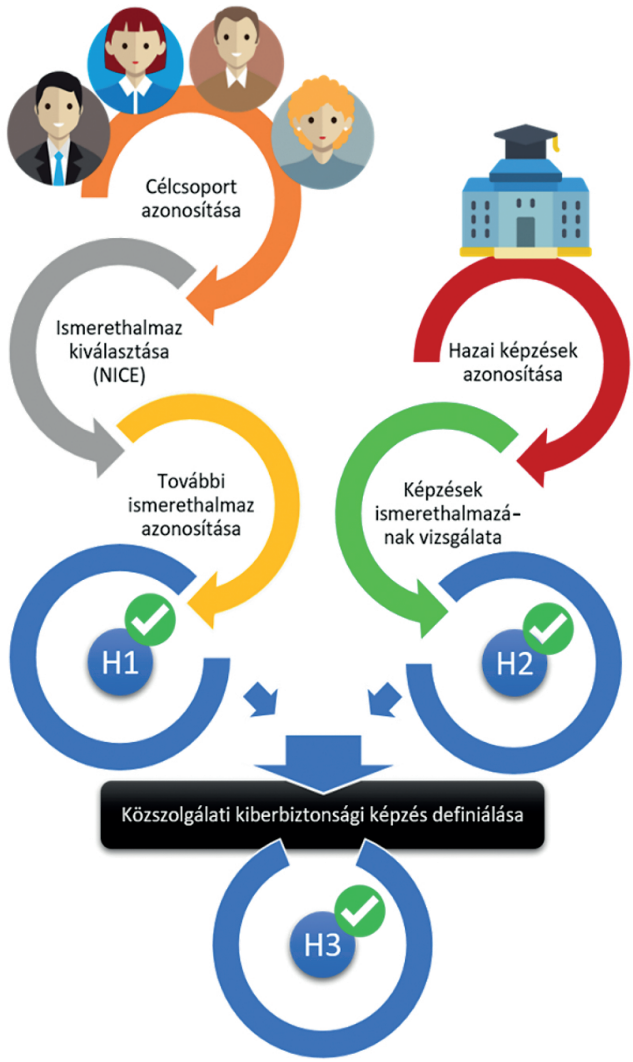
A fentebb említett hipotézisek megválaszolására az 1. ábra segítségével bemutatott módszereket használtam fel, amelyeket az alábbiakban részletezek:

A H1-hipotézis esetén azonosítottam a kiberbiztonsági képzés célcsoportját és a NICE-keretrendszer által rögzített releváns kiberbiztonsági munkakört. Ezt követően definiáltam a képzés során elsajátítandó ismerethalmazt, amely tartalmazza a NICE-ban előírt tudás-, feladat-, készség-, képességhalmazt, valamint egyéb ismeretköröket egyaránt.

A H2-hipotézis esetén azt vizsgáltam, hogy jelenleg a magyarországi felsőoktatási rendszerben milyen kiberbiztonsággal, kibervédelemmel, információbiztonsággal kapcsolatos képzések léteznek, és ezt követően feltérképeztem azok tartalmát, valamint azt, hogy az lefedi-e az első hipotézisben meghatározott szükséges alapismereteket.

A H3-hipotézis igazolására, amennyiben a H2-hipotézis szerint a képzés szükségessége igazolt, a H1-hipotézis alapján meghatározottak szerint definiálom a közszolgálati kiberbiztonsági képzést, valamint annak tartalmát és alapvető elemeit.

[2] A National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework az Egyesült Államok Kereskedelmi Minisztériumának Nemzeti Szabványügyi és Technológiai Intézete által kiadott tanulmány, 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.



1. ábra

Hipotézisek bizonyításának módszerei.

Forrás: a szerző szerkesztése

Kapcsolódó munkák

Ahhoz, hogy a jelen tanulmányban ismertetett közszolgálati kiberbiztonsági képzés minden részletre kiterjedő definiálása megvalósulhasson, nélkülözhetetlen a releváns hazai és nemzetközi szakirodalom mélyebb vizsgálata, továbbá jelen képzés alapjául szolgáló képességek, készségek halmazát a hasonló képzések követelményeinek vizsgálatával határoztam meg.

Hazai kiberbiztonsági oktatással kapcsolatos tanulmányok

Azokat a tanulmányokat vizsgáltam, amelyek a hazai kiberbiztonsági képzésfejlesztésre, a kiberbiztonsági és kibervédelmi képességek fejlesztésére összpontosítanak, illetve a kibervédelmi oktatás kérdéseire keresik a választ.

Az irodalomkutatás során mindenképp ki kell emelni Krasznay Csaba által elkészített *A kiberbiztonság stratégiai vetületeinek oktatási kérdései a közszolgálatban* című publikációt. A szerző rámutat számos olyan, a kibertérben történő eseményre, amelyek kétségkívül hatással vannak a fizikai világra, és rögzíti, hogy ezen eseményekre az ország védelmében részt vevő szervezeteknek reagálniuk kell. Éppen ezért elengedhetetlen olyan közszolgálati szakemberek alkalmazása és képzése, akik érdemben tudnak reagálni a műszaki és nem műszaki természetű kihívásokra egyaránt. A szerző a tanulmányban áttekinti milyen kibervédelmi képességekre van szükség Magyarországon, illetve hogyan lehet ezeket megteremteni. Kibervédelmi képességek közé sorolható a kiberbiztonság általános megértésének képessége, incidensmenedzselési képesség, valamint a stratégiai, vezetői képességek. A szerző javaslatot tesz e képességek fejlesztésének lehetőségeire a hazai felsőoktatási rendszerben megvalósuló alap-, mester- és továbbképzési szintű oktatás keretében.[3]

Nagyné Takács Veronika és Kovács László *Az információbiztonsági vezető szakirányú továbbképzés tapasztalatai* című publikációja rögzíti az információbiztonság jelentőségét és szabályozását, majd bemutatja a Nemzeti Közszolgálati Egyetem Elektronikus Információbiztonsági Vezető (EIV) szakirányú továbbképzésének tartalmát és értékelését, amelyet a szerzők a képzésen végzett hallgatók szakdolgozatának elemzésével végeztek el. Ezek alapján számos következtetést levonnak az EIV fejlesztését célozva, így például javaslatot fogalmaznak meg a képzés céljára és tartalmára, az egyénre szabottabb tanári támogatás biztosítására, illetve a heterogén oktatási csoportok létrehozására vonatkozóan.[4]

Som Zoltán *Az információbiztonság fejlesztési lehetőségei az EIV képzésen keresztül* című cikkében az EIV szakirányú továbbképzésének tapasztalatait és mérési eredményeit mutatja be, amelynek segítségével rávilágít a rendszerben rejlő fejlesztési lehetőségekre is. Ennek keretében személyes megfigyeléseket végzett, és szabadszavas kérdőíveket töltetett ki az EIV-ben részt vevőkkel, majd megvizsgálta, hogy milyen kockázatok merülhetnek fel a képzéssel kapcsolatban, illetve hogy milyen intézkedéseket, ellenintézkedéseket kell megtenni a kockázatok csökkentése érdekében. Végül javaslatokat határozott meg a képzés fejlesztésére, így például szakkollégium létrehozását, illetve egyéni kommunikációs képességek fejlesztését ajánlja.[5]

Simon Béla *Kiberbűnözés elleni képzésfejlesztés* című publikációjában áttekinti, hogy a jelenlegi hazai képzési, oktatási rendszerben mikor és milyen jellegű állami

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

[4] Nagyné Takács Veronika – Kovács László: Az információbiztonsági vezető szakirányú továbbképzés tapasztalatai. *Pro Publico Bono – Magyar Közigazgatás,* 3. (2015), 4. 85–99.

[5] Som Zoltán: Az információbiztonság fejlesztési lehetőségei az EIV képzésen keresztül. *Társadalom és Honvédelem,* 20. (2016), 2. 167–175.

teendők jelentkeznek. A szerző azonosítja a kiberbűnözés elleni fellépés két fő oldalát, a megelőzési oldalát, valamint a már megvalósított bűncselekmények felderítésének, nyomozásának, bizonyításának és az elkövetők büntető igazságszolgáltatás általi felelősségre vonásának megvalósítását. Bemutatja a rendőri/rendészeti felsőoktatás lehetséges, illetve tervezett fejlesztési irányainak lehetőségeit, a megrendelői igények összevetésével.[6]

NICE Framework

A NICE vagy másnéven a Kiberbiztonsági Oktatás Nemzeti Kezdeményezését az Egyesült Államok Kereskedelmi Minisztériumának Nemzeti Szabványügyi és Technológiai Intézete vezeti, amely egyfajta partnerségként értelmezhető a kormány, az akadémiai szféra és a magánszektor között. Az együttműködés középpontjában a kiberbiztonsági oktatás, képzés, valamint a munkaerő hálózatának folyamatos fejlesztése áll. A NICE ennek keretében tudományos és ipari partnerekkel egyeztetve kordinálja a már meglévő sikeres kiberbiztonsági programokat, valamint elősegíti az innovációt és a kiberbiztonsági szakemberek jövőképének kialakítását. A NICE olyan országos és nemzetközi kezdeményezéseket támogat, amelyek segítségével növelhető a kiberbiztonsággal kapcsolatos munkák elvégzéséhez szükséges ismeretekkel, készségekkel és képességekkel rendelkező szakértők száma.

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, ahogyan azt a 2. ábra is szemlélteti. E keretrendszer kiváló alapként szolgálhat az általunk átadni kívánt tudás, készségek, képességek meghatározására, a kiberbiztonsági tantervek, tantárgyi adatlapok kidolgozására.

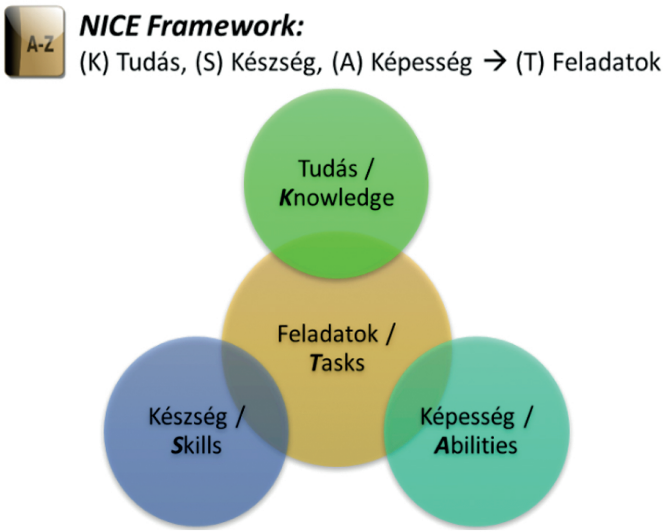
A NICE-keretrendszerről és a kiberbiztonsági oktatás fontosságáról számos nemzetközi tanulmány tartalmaz megállapításokat, következtetéseket.

Alsmadi tanulmánya rámutat a jelenlegi kiberbiztonsági munkaerőhiány jelenségére, valamint arra, hogy folyamatos növekedés figyelhető meg a kiberbiztonsági szakemberek és készségek iránti igények tekintetében. Továbbá rávilágít az elméleti és gyakorlati képességek közötti egyensúly hiányára, illetve az akadémia és az ipar közötti szakadékra, amelyeket a NICE-keretrendszer segítségével meg lehetne oldani.[8]

[6] Simon Béla: Kiberbűnözés elleni képzésfejlesztés. *Magyar Rendészet,* 18. (2018), 3. 193–207.

[7] William Newhouse et alii: *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*. National Institute of Standards and Technology, 2017.

[8] Izzat Alsmadi: Cybersecurity Education Based on the NICE Framework: Issues and Challenges. *ISACA Journal,* 4. (2018), 1–6.



2. ábra
NICE-keretrendszer KSA elemeinek kapcsolata.
Forrás: a szerző szerkesztése

Armstrong és szerzőtársai szintén kihangsúlyozza a növekvő kiberbiztonsági munkaerőhiányt, ezáltal pedig a kiberbiztonsági munkaerő iránti kereslet és versengés megjelenését. A cikk rögzíti az egyetemek szerepét, amely szerint hozzájárulnak a növekvő kiberbiztonsági igények kielégítéséhez azáltal, hogy megfelelő kiberbiztonsági képesítést biztosítanak a következő generáció számára, továbbá döntő fontosságú, hogy az ilyen képzések tanterveit úgy alakítsák ki, hogy az adott munkakör típusához is illeszkedjenek, továbbá gyakorlati ismereteket is tartalmazzanak.[9]

Adriane C. Estes és szerzőtársai tanulmányukban feltárják, hogy a NICE kiberbiztonsági munkaerőrendszere hogyan igazítja és hangolja össze a kiberbiztonsági 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 ezen képességek hiányára, valamint folyamatos fejlesztésére, nemcsak szervezeti, hanem globális szinten is.[10]

McDuffie és Piotrowski rávilágítanak arra, hogy a kiberbiztonsági oktatás és a munkaerő fejlesztése jelentősen hozzájárul a közös kiberbiztonsági nyelv kialakításához, amely nagyban javítja a problémamegoldást is.[11]

[9] Miriam E. Armstrong et alii: Framework for Developing a Brief Interview to Understand Cyber Defense Work: An Experience Report. *Proceedings of the Human Factors and Ergonomics Society 2017 Annual Meeting,* 61. (2017), 1. 1318–1322.

[10] Adriane C. Estes – 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.

[11] Ernest L. McDuffie – Victor P. Piotrowski: The Future of Cybersecurity Education. *Computer,* 47. (2014) 8. 67–69.

A közszolgálati kiberbiztonság megvalósításához szükséges képességek, készségek, ismeretek

Jelen fejezet célja meghatározni, hogy a közszolgálat mely része tekinthető relevánsnak a közszolgálati kiberbiztonsági képzés szempontjából. A meghatározott célcsoporthoz azonosítani kell a kibervédelmi, adatvédelmi és információbiztonsági feladatköröket, végül az ezek végrehajtásához szükséges ismerethalmazt szükséges definiálni.

A célcsoport és a feladataik meghatározása

A közszolgálati kiberbiztonság megteremtéséhez elengedhetetlen a különféle kibervédelmi képességek elsajátítása és folyamatos fejlesztése. Azonban vannak olyan területei a közszolgálatnak, amelyek sokkal részletesebben és több aspektusból is vizsgálják a kiberbiztonságot (például honvédség, nemzetbiztonsági szolgálatok stb.), ezért fontos meghatározni, hogy a közszolgálat mely részeivel szeretnék foglalkozni jelen kutatás fő kontextusában.

Célcsoport meghatározása

Ahhoz, hogy a célcsoport definiálható legyen, mindenképp szükséges meghatározni a közszolgálat fogalmát. A nemzetközi és hazai szakirodalom alapján megállapítható, hogy nagyon nehéz egy egységes definíciót alkotni a közszolgálatra, hiszen országonként eltérő, hogy mely szervek és alkalmazotti körök társíthatók e fogalomhoz. Antal Zsolt a közszolgálat definícióját többféle megközelítésből (jogi, funkcionális, szervezeti) vezeti le, amelyek alapján a közszolgálat olyan nem piaci mechanizmusok által vezérelt tevékenységek összessége, amelyet az állam által többségében tulajdonolt szervezetek valósítanak meg a közjó fenntartása vagy növelése érdekében.[12]

Hazafi Zoltán doktori értekezésében két definíciót rögzít, az egyik az úgynevezett funkcionális fogalom, amelynek értelmében mindenki, aki közfeladatot lát el közszolgálati alkalmazottnak minősül, függetlenül az őt alkalmazó szervezet jogállásától, személyes státuszától, kiválasztásától, illetve díjazásától. A másik, úgynevezett szűkebb meghatározás szerint közszolgálati alkalmazott az, akit a jogállására vonatkozó szabályok ilyen minőséggel ruháznak fel.[13] E definíciókból következik, hogy a közszolgálati alkalmazotti csoport rendkívül széles spektrumú, mind az idetartozó munkaköröknek, mind az alkalmazottak képességeinek, készségeinek köszönhetően. Éppen ezért fontos jelen kutatás szempontjából releváns közszolgálati alkalmazotti kör szűkítése olyan területekre, amelyek kiberbiztonsági kockázatot jelenthetnek, részt vesznek a döntéshozatalban, és képzésük során nem részesülnek részletes, átfogó kiberbiztonsági oktatásban.

[12] Antal Zsolt: A közszolgálati kommunikáció eredményességére ható tényezők – A közszféra és a versenyszféra kommunikációs gyakorlatát befolyásoló különbségek. *Vezetéstudomány*, 49. (2018), 4. 68–76.

[13] Hazafi Zoltán: *Közszolgálati jogunk a változó nemzetközi és hazai térben*. Doktori értekezés. Pécsi Tudományegyetem, ÁJK Állam- és Jogtudományi Kar Doktori Iskola, 2009.

Idetartoznak például az alábbi közszolgálati munkakörök a teljesség igénye nélkül:
a) a közigazgatásban foglalkoztatott közszolgálati tisztviselők,
b) az állami főhatalom szerveinek hivatalaiban dolgozó személyek,
c) az egyes speciális jogállású központi szervekben dolgozó személyek,
d) a rendvédelmi feladatokat ellátó szervek igazgatási feladatot végző tagjai,
e) bírák, ügyészek, illetve a munkájukat segítő alkalmazottak,
f) kiberbiztonsági kockázatot jelentő közalkalmazottak.

Összességében megállapítható, hogy a közszolgálati alkalmazottak ilyen típusú szűkítése elengedhetetlen a közszolgálati kiberbiztonság megvalósításához, hiszen ahhoz, hogy meghatározzuk milyen ismerethalmaz elsajátítása a cél, tudnunk kell, hogy milyen területen zajlik a mindennapos munkavégzés, illetve milyen típusú döntéshozatalban vesznek részt az alkalmazottak.

Feladatok azonosítása

A célcsoport meghatározása után fontos meghatározni azokat az általános kiberbiztonsági feladatokat, amelyeket a közszolgálati dolgozóknak szükséges végrehajtani akár a mindennapi munkájuk során, akár egy esetleges kibertámadás esetén. A NICE-keretrendszer segítségével azonosított feladatokat az 1. táblázat tartalmazza.[14]

1. táblázat

A kiválasztott célcsoport általános kibervédelmi feladatai.

Forrás: a szerző szerkesztése

Feladat
T1. Tanácsadás a felsővezetésnek a kockázatértékelési folyamatról, kockázati szintekről, az információbiztonsági programokról, rendszerekről, irányelvekről, folyamatokról és eljárási szabályokról.
T2. Üzletmenet-folytonossági tervek elkészítése, tesztek elvégzése.
T3. Adatvédelmi, adatbiztonsági érdekek képviselése a szervezeten belül.
T4. Stratégiai tervek kidolgozása és fenntartása.
T5. Szerződések értékelése az adatvédelmi követelmények betartása érdekében.
T6. A különféle döntéshozatali folyamatok során megjelenő kockázatelemzés elkészítése.
T7. Releváns jogszabályok, szabványok, eljárások, technológiai változások figyelemmel kísérése, értelmezése, alkalmazása.
T8. Hazai és külföldi „jó gyakorlatok" alkalmazása.
T9. Belső audit végrehajtása, auditjelentések elkészítése.
T10. Közvetítés a műszaki és nem műszaki szakemberek között.
T11. A kiberbiztonsági politika, stratégia meghatározása a felsővezetéssel együtt, a kiberbiztonsági, adatvédelmi alapelvek a szervezet küldetésében, jövőképében és céljaiban történő megjelenítése.
T12. Kapcsolattartás az adatvédelemért és adatbiztonságért felelős hatóságokkal, testületekkel, kormányzati szervekkel, szereplőkkel.

[14] Newhouse et alii i. m. (7. lj.) 24–58.

T13. Iránymutatás átadása a vezetőség, az alkalmazottak és az ügyfelek számára, a releváns jogszabályokról, politikákról, szabványokról és eljárásokról.
T14. Együttműködés az informatikai, információbiztonsági szakemberekkel.
T15. Közreműködés az információs infrastruktúra kialakításában, fejlesztésében.
T16. Incidenskezelési folyamat kialakítása, incidensek kezelése.
T17. Figyelemmel kísérni a szervezet folyamatait a biztonsági és az adatvédelmi szabályok betartásának ellenőrzése céljából.
T18. A szervezet adatvédelmi kérdésekkel foglalkozó munkatársainak felügyelete.
T19. Kibervédelmi kérdések megválaszolása a szervezeten belül és kívül.
T20. Kiberbiztonsági fenyegetések, támadások felismerése és szegregálása.
T21. A humán fenyegetettségből eredő kockázatok azonosítása.
T22. Kiberbiztonsággal, adatvédelemmel kapcsolatos képzések, oktatások megtartása, lebonyolítása.

Szükséges ismerethalmaz definiálása

Ahhoz, hogy az előző pontban ismertetett feladatokat a közszolgálati alkalmazottak maradéktalanul el tudják látni a munkájuk során fontos követelmény, hogy azonosítsuk milyen tudáshalmaz szükséges számukra.

A NICE által definiált ismerethalmaz

A T1–T18 kibervédelmi feladatok ellátásához szükséges ismerethalmaz definiálása során a NICE Framework keretrendszer kiberbiztonsági pozíciói közül az adatvédelmi tisztviselő munkakört választottam ki, amely a leginkább illeszkedik a célcsoport előképzettségéhez, valamint az általuk megszerezhető képességekhez. Ezt követően megvizsgáltam a keretrendszer által előírt tudás, képesség és készség halmazát, és kiválasztottam azokat, amelyek feltétlenül szükségesek az említett feladatok teljesítéséhez. Ezek alapján a 2. táblázat tartalmazza e feladatokat, tudást, képességeket és készségeket:

2. táblázat

T1–T18 feladatokhoz szükséges KSA-elemek.

Forrás: a szerző szerkesztése

Tudás (K)
K1. Számítógép-hálózatokhoz kapcsolódó alapfogalmak ismerete.
K2. Kockázatkezelési folyamatok ismerete.
K3. Kiberbiztonsági, adatvédelmi jogszabályok, irányelvek, alapelvek ismerete.
K4. Kibertérből érkező fenyegetések ismerete.
K5. Vezeték nélküli technológiák ismerete.
Készség (S)
S1. Adatvédelmi szabályok, irányelvek készítésének készsége.
S2. A beszállítókkal és partnerekkel való tárgyalókészség, valamint ezek adatvédelmi gyakorlataival kapcsolatos értékelésének készsége.
S3. Különböző szintű kommunikációs készség a szervezet különböző területeinek megfelelően.

Képesség (A)
A1. Egyértelmű, világos, átlátható stratégia, iránymutatások, szabályok, eljárások, folyamatok és képzési anyagok, dokumentációk kidolgozásának képessége.
A2. Szabványos működési eljárások, folyamatok kidolgozásának és folyamatos fejlesztésének és a jogszabályoknak való megfeleltetésének képessége.
A3. A releváns adatvédelmi, kiberbiztonsági jogszabályok, technológiák változásának nyomon követésének képessége.
A4. Operatív célok eléréséhez szükséges megfelelő intézkedések, eljárások kiválasztásának képessége.
A5. Műszaki, tervezési információk az ügyfél megértési szintjéhez igazított átalakításának képessége.
A6. Adatvédelmi és információbiztonsági célok összehangolásának képessége.
A7. Annak meghatározásának képessége, hogy egy biztonsági esemény, incidens megsérti-e a magánélet tiszteletben tartásának elvét vagy a jogi előírásokat.
A8. Képzési tervek kidolgozásának képessége.
A9. Adatvédelmi szabályzatok, dokumentumok kidolgozásának képessége.

Egyéb a NICE által nem definiált ismerethalmaz

A további feladatok végrehajtásához azonban további tudást, képességeket és készségeket is kell azonosítani. A T19–T22-es feladatokhoz kapcsolódóan a 3. táblázat foglalja össze a további ismerethalmazt.

3. táblázat

T19–T22 feladatokhoz szükséges KSA-elemek.

Forrás: a szerző szerkesztése

Tudás (K)
K1* Az állami kibervédelmi rendszer ismerete.
K2* A szervezeten belüli kiberbiztonsági és adatvédelmi felelős pozíciók ismerete.
K3* A kibertámadások esetén alkalmazható technikák, eljárások ismerete.
K4* Az emberi tényezők és a kiberbiztonság kapcsolódási pontjainak ismerete.
K5* A kibertámadások mögött rejlő motivációk és pszichológiai tényezők ismerete.
Készség (S)
S1* Emberi tényezők kockázatán alapuló támadások felismerésének készsége.
S2* Adatbiztonsági és kiberbiztonsági magatartás készsége.
Képesség (A)
A1* A belső munkavállalók jelentette kiberbiztonsági kockázatok felismerésének képessége.
A2* A humán fenyegetettségből eredő kockázatok csökkentésének képessége a szervezeten belül.
A3* A szervezetben betöltött pozíciójának megfelelő támogatás nyújtásának képessége egy kibertámadás kezelése során.
A4* Kiberbiztonsággal, adatvédelemmel kapcsolatos képzések, oktatások megtartásának, lebonyolításának képessége.

Hazai kiberbiztonsággal kapcsolatos képzések

Jelen pontban azokat a kiberbiztonsággal kapcsolatos képzéseket mutatom be, amelyekre Magyarországon jelenleg (2020 szeptemberétől) jelentkezni lehet. Összesen

tíz ilyen képzést azonosítottam *A hazai képzések bemutatása* című alfejezetben, amelyek alapadatait az *Alapképzési szakok* című alfejezetben taglalom. Ezt követően megvizsgáltam, hogy a képzés tantervében szerepelnek-e az előzőekben bemutatott NICE-keretrendszer által, valamint az általam meghatározott szükséges alapismeretek, amelyeket a *Mesterképzési szakok* című alfejezetben részletezek.

A hazai képzések bemutatása

A bolognai folyamat részeként átalakult felsőoktatási képzési rendszer az alábbi fázisokból épül fel: *alapképzésből és mesterképzésből,* illetve az alap vagy mesterképzés után is elvégezhető *szakirányú továbbképzésből.* A hazai kiberbiztonsági képzéseket e három csoport alapján mutatom be a következőkben. Ezenkívül számos további képzés (tudatossági programok, továbbképzések, kurzusok stb.) biztosítja a kiberbiztonsági ismeretek átadását a közszolgálatban dolgozó személyek számára, azonban jelen tanulmány és az alábbi alfejezetek célja kizárólag a magyar felsőoktatási rendszerben megtalálható képzések összegyűjtése és bemutatása.

Alapképzési szakok

Az alapképzés általában 3-4 éves időtartamot felölelő képzési forma, amelyen tudományterülettől függően BA (Bachelor of Arts), illetve BSc (Bachelor of Science) fokozat szerezhető. E képzés során tulajdonképpen széles körű alapszintű ismeretek elsajátítása a cél, amely a munkaerőpiacon hasznosítható szakmai ismereteket és megfelelő elméleti alapozást nyújt az adott szakterületen a tanulmányok mesterképzésben történő folytatásához.

Kiberbiztonsághoz kapcsolódó hazai alapképzések: a) Nemzeti Közszolgálati Egyetem – Bűnügyi alapképzési szak – Kiber nyomozó szakirány (NKE KNY);[15] b) Óbudai Egyetem – Biztonságtechnikai mérnök alapképzési szak – Információbiztonsági specializáció (ÓE BM).[16]

Mesterképzési szakok

A mesterképzés, amelyen MA (Master of Arts), illetve MSc (Master of Sciences) fokozat és szakképzettség szerezhető. Mesterképzésre az jelentkezhet, aki legalább egy alapképzési diplomával vagy a korábbi képzési rendszer szerinti főiskolai/egyetemi diplomával rendelkezik, de a felvétel pontos követelményeit és feltételeit

[15] *Nemzeti Közszolgálati Egyetem – Bűnügyi alapképzési szak – Kiber nyomozó szakirány.* Elérhető: www.felvi.hu/felveteli/egyetemek_foiskolak/!IntezmenyiOldalak/meghirdetes.php?meg_id=20905&elj=20a (A letöltés dátuma: 2020. 03. 14.)

[16] *Óbudai Egyetem – Biztonságtechnikai mérnök alapképzési szak – Információbiztonsági specializáció.* Elérhető: www.felvi.hu/felveteli/szakok_kepzesek/szakleirasok/!Szakleirasok/index.php/szak/36/szakleiras (A letöltés dátuma: 2020. 03. 14.)

a felsőoktatási intézmények maguk határozzák meg. A mesterképzés általában 2-4 féléves időtartamot ölel fel. Összességében megállapítható, hogy a mesterképzés során szakterület-specifikus és mélyebb elméleti és gyakorlati ismeretek átadása a cél, amelynek elvégzését követően lehetőség van kilépni a munkaerőpiacra, illetve jelentkezni lehet a képzési rendszer harmadik lépcsőfokát jelentő doktori képzésre, amely a tudományos fokozat megszerzésére készít fel.[17]

Kiberbiztonsághoz kapcsolódó hazai mesterképzések: a) Nemzeti Közszolgálati Egyetem – Kiberbiztonsági mesterképzés (NKE KB);[18] b) Nemzeti Közszolgálati Egyetem – Védelmi infokommunikációs rendszertervező – Információbiztonsági szakirány (NKE VIKR).[19]

Szakirányú továbbképzések

Fontos megemlíteni a szakirányú továbbképzés szintjét is, amely a már korábban megszerzett alap- és mesterfokozatra, főiskolai vagy egyetemi szintű végzettségre épülő oklevelet adó, 2-4 félév időtartamú képzési forma. A mesterképzéstől eltérő képzési forma, amely speciális feladatok ellátására ad felkészítést, valamint lehetővé teszi a korábban szerzett ismeretek meghatározott irányú elmélyítését. Azonban az elvégzését követően megszerzett oklevél nem emeli a korábbi végzettség szintjét.[20]

Kiberbiztonsághoz kapcsolódó hazai szakirányú képzések:

a) Nemzeti Közszolgálati Egyetem – Elektronikus információbiztonsági vezető szakirányú továbbképzés (NKE EIB);[21]
b) Nemzeti Közszolgálati Egyetem – Európai uniós adatvédelmi szaktanácsadó szakirányú továbbképzési szak (NKE EUA);[22]
c) Eötvös Loránd Tudományegyetem – Adatbiztonsági és adatvédelmi szakjogász/szakember szakirányú továbbképzés (ELTE ASZ);[23]
d) Óbudai Egyetem – Kiberbiztonsági szakmérnök/szakember szakirányú továbbképzés (ÓE KSZ);[24]

[17] 2011. évi CCIV. törvény a nemzeti felsőoktatásról.

[18] *Nemzeti Közszolgálati Egyetem – Kiberbiztonsági mesterképzés.* Elérhető: www.felvi.hu/felveteli/szakok_kepzesek/szakleirasok/!Szakleirasok/index.php/szak/20554/szakleiras (A letöltés dátuma: 2020. 03. 14.)

[19] *Védelmi infokommunikációs rendszertervező – Információbiztonsági szakirány szakleírás, tematika.* Nemzeti Közszolgálati Egyetem Elérhető: https://hhk.uni-nke.hu/oktatas/mesterkepzes/vedelmi-vezetestechnikai-rendszertervezo (A letöltés dátuma: 2020. 03. 14.)

[20] 87/2015. (IV. 9.) Korm. rendelet a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény egyes rendelkezéseinek végrehajtásáról.

[21] *Elektronikus információbiztonsági vezető szakleírás.* Nemzeti Közszolgálati Egyetem. Elérhető: https://kti.uni-nke.hu/szakiranyu-tovabbkepzesek/szakiranyu-tovabbkepzesi-szakok/elektronikus-informaciobiztonsagi-vezeto/altalanos-informaciok (A letöltés dátuma: 2020. 03. 19.)

[22] *Európai uniós adatvédelmi szaktanácsadó szakleírás.* Nemzeti Közszolgálati Egyetem. Elérhető: https://kti.uni-nke.hu/szakiranyu-tovabbkepzesek/szakiranyu-tovabbkepzesi-szakok/europai-unios-adatvedelmi-szaktanacsado/altalanos-informaciok (A letöltés dátuma: 2020. 03. 14.)

[23] *Adatbiztonsági és adatvédelmi szakjogász szakleírás.* ELTE Jogi Továbbképző Intézet, Elérhető: https://jotoki.elte.hu/content/adatbiztonsagi-es-adatvedelmi-szakjogasz.t.406 (A letöltés dátuma: 2020. 03. 19.)

[24] *Kiberbiztonsági szakmérnök/szakember képzés tartalma.* Óbudai Egyetem. Elérhető: http://bmi.nik.uni-obuda.hu/kiber_kovetelmeny (A letöltés dátuma: 2020. 03. 19.)

e) Óbudai Egyetem – Információbiztonsági szakmérnök/szakember szakirányú továbbképzés (ÓE ISZ);[25]
f) Gábor Dénes Főiskola – Adatvédelmi és információbiztonsági menedzser szakirányú továbbképzés (GDF AIM).[26]

Hazai képzések alapadatainak vizsgálata

Az első összehasonlítás során a képzések alapadatait vizsgáltam meg, amelyet a 4. táblázat szemléltet. A táblázatban látható, hogy az egyes képzések időtartama (I.) félévekben megadva; a munkarend (M), ami lehet *nappali* (n), *levelező* (l), esetleg *mindkettő* (n/l); a finanszírozási forma (Fin.), amely alapján a képzés lehet *állami ösztöndíjjal támogatott* (öszt.), *önköltséges* (önk.) vagy *mindkettő* (öszt/önk.), végül a bemeneti követelmények.

4. táblázat
Vizsgált hazai képzések alapadatai.
Forrás: a szerző szerkesztése

	Képzés	I.	M.	Fin.	Bemeneti követelmény
BSC/BA	NKE KNY	8	n	öszt.	alkalmassági vizsgálatok + informatikai jártassági és készségvizsgálat
	ÓE BM	7	n/l	öszt/önk.	érettségi bizonyítvány, meghatározott érettségi vizsgakövetelmények
MSC/MA	NKE KB	4	n/l	öszt/önk.	alapképzés + informatikai, államtudományi és társadalomtudományi ismeretek
	NKE VIKR	4	n/l	öszt/önk.	alapképzés
Szakirányú továbbképzés	NKE EIB	2	l	önk.	alapképzés
	ELTE ASZ	3	l	önk.	szakjogász: állam- és jogtudomány képzés szakember: meghatározott alapképzések
	ÓE KSZ	4	l	önk.	szakmérnök: mérnöki alapképzés szakember képzés: alapképzés
	ÓE ISZ	4	l	önk.	szakmérnök: mérnöki alapképzés szakember képzés: alapképzés
	GDF AIM	2	l	önk.	informatikai, műszaki, gazdaságtudományi, társadalomtudományi, pedagógusképzés, jogi, közigazgatási, rendészeti vagy katonai alapképzés
	NKE EUA	2	l	önk.	alapképzés

[25] *Információbiztonsági szakmérnök/szakember képzés tartalma.* Óbudai Egyetem. Elérhető: www.bgk.uni-obuda.hu/hu/kepzeseink/tovabbkepzesek/informaciobiztonsagi-szakmernokszakember (A letöltés dátuma: 2020. 03. 21.)
[26] *Adatvédelmi és információbiztonsági menedzser szakirányú továbbképzés tartalma.* Gábor Dénes Főiskola. Elérhető: http://gdf.hu/szakiranyu-tovabbkepzesek/adatvedelmi-es-informaciobiztonsagi-menedzser/ (A letöltés dátuma: 2020. 03. 21.)

A vizsgálatból kiderül, hogy a vizsgált alapképzésekhez bár nincs szükség egyéb végzettségre, azonban megjelennek a jelentkezéshez szükséges további feltételek, mint például az alkalmassági vizsgálat, informatikai jártasság. Ezenkívül az egyes képzések további megszorításokat, követelményeket tartalmaznak azzal kapcsolatban, hogy milyen típusú előképzettségre van szükség ahhoz, hogy a képzésen részt lehessen venni. Három képzés esetében (NKE VIKR, NKE EIB, NKE EUA) bármely képzési terület alapképzéses diplomáját elfogadják, míg a többi képzés esetében külön rögzítették a bemeneti követelmények konkrét képzési területeit, így például informatikai, műszaki, közigazgatási, jogi és számos további területi alapképzésen szerzett oklevél szükséges.

Az előképzettség a képzés abszolválásának körülményeit is jelentősen befolyásolja, így például más bemeneti tudással rendelkeznek a műszaki és más a humán területről érkező hallgatók, hiszen míg az utóbbi esetében az informatikai oktatás, addig az előbbi esetében a jogi, társadalomtudományi ismeretek elsajátítása okozhat nehézséget.

Összességében megállapítható, hogy a jelenlegi felsőoktatási képzési rendszer minden szintjén elérhető kiberbiztonsággal, információbiztonsággal foglalkozó képzés. 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.

Hazai képzések ismerethalmazának vizsgálata

Miután bemutattam a hazai felsőoktatásban elérhető kiberbiztonsággal foglalkozó képzéseket, szeretném megvizsgálni, hogy létezik-e olyan képzés, amely fedi a *Feladatok azonosítása* című alfejezetben 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 az 5. 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.

A vizsgált képzések közül a Nemzeti Közszolgálati Egyetem védelmi infokommunikációs rendszertervező mesterképzés információbiztonsági szakiránya fedi le a legtöbb korábban meghatározott tudáskört.

Összességében megállapítható, hogy az általam meghatározott új tudáselemek mindegyike megjelenik valamely vizsgált képzés képzési tervében, amely azt mutatja, hogy ezen ismeretkörök a közszolgálati kiberbiztonsági képzés szempontjából relevánsnak tekinthetők. A táblázat alapján egyébként az is látható, hogy kivétel nélkül, minden vizsgált képzés tantárgyi programjában szerepel a számítógép-hálózatokhoz kapcsolódó alapfogalmak oktatása.

5. táblázat

Hazai 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	-	✓	✓	-	-	✓	✓	-	-	-

Azonban egyértelműen kijelenthető, hogy a hazai felsőoktatási rendszerben jelenleg nem létezik olyan képzés, amely teljeskörűen lefedi az előzőekben definiált közszolgálati kibervédelmi képesség kialakításához szükséges alapismereteket, vagyis nincs olyan képzés, amely kellő mértékben és összhangban tartalmazná a szükséges közigazgatási, jogi és informatikai, műszaki ismeretanyagot. A közszolgálati kiberbiztonsági képzés elhatárolódik az állami és önkormányzati szervezetek információbiztonságáról szóló 2013. évi L. törvényben (Ibtv.) meghatározott, az elektronikus információs rendszer védelméért felelős személyek feladatellátáshoz szükséges felsőfokú végzettségtől, mivel nem egy konkrét pozícióra ad képesítést, hanem sokkal általánosabb tudást ad át minden közszolgálatban dolgozó személy számára.

A közszolgálati kiberbiztonsági képzés meghatározása

Az eddigi fejezetekben meghatároztam a közszolgálat számára szükséges tudáshalmazt és megvizsgáltam, hogy létezik-e olyan, a felsőoktatási rendszerben elérhető képzés, amely a felvázolt szükséges ismeretköröket tartalmazza. Mivel egyértelműen kiderült, hogy nem található ilyen képzés hazánkban, ezért elengedhetetlen egy olyan képzés definiálása, amely lefedi ezen ismereteket.

A következőkben meghatározom a közszolgálati kiberbiztonsági képzés alapvető fogalmainak, elemeinek definícióját, értelmezését, a bemeneti, képzési és kimeneti követelményeit.

A kiberbiztonsági képzés definiálása

Ahhoz, hogy definiálhassuk magát a képzést, elengedhetetlen a kibervédelmi képesség pontos meghatározása. A képzés szempontjából fontos, hogy ebben

az esetben a személyes kibervédelmi képességről beszélünk. Természetesen a végső cél a közszolgálat szervezeti szintű kibervédelmi képességének kialakítása, ezáltal a kiberbiztonság fejlesztése, amelynek első lépése a szervezet alkalmazottai körében e képesség elsajátítása. A szervezeti és a személyi kibervédelmi képesség tehát elkülönül egymástól, de egymásra épül. A kibervédelmi képesség magában foglalja az információbiztonság-tudatosságot is, alapvető részeként értelmezhető, amely elengedhetetlen feltétele e képesség kialakításának.

Ezek alapján 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.

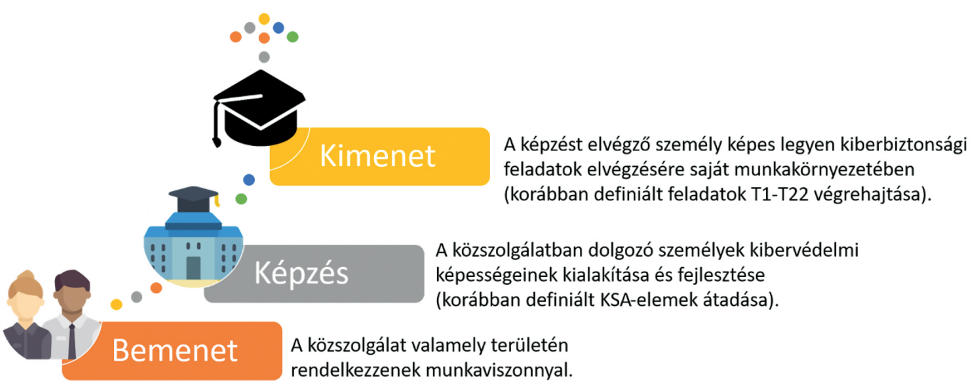
E képesség kialakítását célozza a *közszolgálati kiberbiztonsági képzés*, amely a közszolgálatban dolgozó személyek kibervédelmi képességének kialakítására irányul a közszolgálati kiberbiztonság fejlesztése érdekében.

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.

A 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.

A képzési forma alapvető elemeinek, követelményeinek meghatározása

A képzés alapvető be- és kimeneti követelményeit és a képzés célját tekinti át a 3. ábra. Az alfejezet további részében ezen elemeket részletezem.



3. ábra

A közszolgálati kiberbiztonsági képzés definíciója és alapvetői követelményei.

Forrás: a szerző szerkesztése

A képzés bemeneti követelménye, hogy a képzésben részt vevő személy a közszolgálat valamely területén rendelkezzen munkaviszonnyal és hazai alapképzési, illetve mesterképzési szakkal vagy ezzel egyenértékű külföldi felsőoktatási végzettséggel.

A képzés során a közszolgálatban dolgozó személyek a kibervédelem elméleti és gyakorlati oldalát is egyaránt megismerhetik, hiszen a képzés egy elméleti és egy gyakorlati részből áll. Az elméleti részben a résztvevők elsajátíthatják többek között – a teljesség igénye nélkül – a munkájukhoz szorosan kapcsolódó államtudományi, jogi és közigazgatás-szervezési ismereteket, biztonságpolitikai, diplomáciai ismereteket, rendészeti, katonai és védelmi ismereteket, kommunikációs ismereteket, informatikai alapismereteket, információ- és informatikai biztonsági ismereteket, valamint adatvédelmi ismereteket. Ahhoz, hogy a képzés résztvevői a megszerzett elméleti tudást éles helyzetbe is át tudják ültetni, a képzés gyakorlati része nyújt segítséget, amely során konkrét támadásokkal szembesülhetnek, amelyeket önállóan vagy csapatban kell megoldaniuk. Ennek szerepe, hogy az alkalmazottakat ne érje váratlanul egy valós támadás és meg tudják hozni a megfelelő, sok esetben stratégiai döntéseket. A képzés gyakorlati része a hazai és nemzetközi oktatásban is megjelenő kibergyakorlatokra épül, amelyek során konkrét támadások szimulálásával a már meglévő tudásra alapozva, összekapcsolható az elméleti és a gyakorlati tudás. Ennek következtében a résztvevők képesek lesznek felismerni a kibertérből érkező fenyegetéseket és esetleges kockázatokat. A képzés gyakorlati része során a mindennapos üzemeltetési feladatokkal és az információs rendszer, valamint az ehhez kapcsolódó folyamatok, eljárások megfelelőségének ellenőrzésével is meg kell birkózniuk a hallgatóknak.

A képzés kimeneti követelménye, hogy a képzést elvégző személy képes legyen a korábban definiált és azonosított feladatok elvégzésére saját munkakörnyezetében. A képzés abszolválását követően a korábban említett területeken szerezhetnek széles körű szakmai ismereteket, valamint a mindennapi munkájuk során előforduló aktuális és lehetséges kihívások megoldására szolgáló szakmai kompetenciákat.

Összegezve a közszolgálati kiberbiztonsági képzés egy gyakorlatban is alkalmazható szakmai tudást, valamint problémafelismerő és -megoldó készséget nyújt résztvevőinek, amelynek elsajátításával képesek felismerni, feltérképezni a kibertámadások támadási felületeit és megelőző lépéseket tenni a környezetében jelentkező kibertámadási pontokon. Továbbá a résztvevők képesek lesznek azonosítani egy-egy konkrét támadást, illetve beavatkozni szükség esetén.

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.

Az első hipotézisben azt vizsgáltam, hogy a közszolgálatban dolgozó személyek számára szükséges-e a NICE által és más egyéb nem a NICE által meghatározott ismeretkörök elsajátítása. Ennek érdekében először azonosítottam a célcsoportot, majd az e csoporthoz tartozó feladatokat. Az így definiált feladatokat a NICE-ban

található ismerethalmazzal próbáltam meg lefedni. A lefedetlen pontokat új, általam meghatározott ismeretkörökkel bővítettem.

A második hipotézis esetén azzal a feltételezéssel éltem, hogy a hazai felsőoktatási rendszerben jelenleg nem létezik olyan képzés, amely lefedi a közszolgálati kibervédelmi képesség kialakításához szükséges alapismereteket. Ennek érdekében a többek között hazai felsőoktatási képzésekről tájékoztatást nyújtó felvi.hu portál segítségével feltártam a 2020 szeptemberében induló kiberbiztonsággal kapcsolatos képzéseket. Az egyes képzések képzési, illetve tantárgyi programjai segítségével bemutattam azok alapvető jellemzőit, a képzéseket csoportosítottam a többciklusú bolognai rendszer fázisai alapján, és megvizsgáltam, hogy az egyes képzések tartalmazzák-e az első hipotézisben meghatározott tudáselemeket. Ez alapján megállapítható, hogy a második hipotézis igaznak bizonyul, hiszen egyik képzés sem fedte le maradéktalanul a szükséges alapismereteket.

A harmadik hipotézisben azt feltételeztem, hogy a magyar közszolgálat számára definiálható egy felsőoktatási kiberbiztonsági képzés. A feltételezés igazolására definiáltam a képzést, annak be- és kimeneti követelményeit, valamint főbb elemeit, az első hipotézisben meghatározott ismerethalmaz segítségével.

Összegzés és jövőbeli tervek

A kiberbiztonság egy gyorsan változó, folyamatosan fejlődő és bővülő terület, amely egyre újabb és újabb kihívásokat, illetve fenyegetéseket tartogathat számunkra. A közszolgálat hatékony és eredményes működéséhez elengedhetetlen a kibertér használata, azonban számos előnye mellett a hátrányaival és az esetleges kockázatokkal is számolnunk kell.

Jelen tanulmányban bizonyítottam, hogy szükséges egy olyan eddig még nem létező képzési program megalkotása a hazai képzési környezetben, amely lehetőséget nyújt a közszolgálatban dolgozó, nem informatikai végzettségű személyek kibervédelmi képességének kialakítására. E képesség alatt a személyes kibervédelmi ismeretek és képességek összessége érthető. A kiberbiztonsági képzés azoknak a személyeknek szól, akik nem rendelkeznek a szükséges alapismeretekkel, nem mozognak a témában otthonosan.

A bizonyítás során a következő lépéseket hajtottam végre:

1. Definiáltam a képzés tényleges célcsoportját és azonosítottam azokat az általános kibervédelmi feladatokat, amelyekkel a közszolgálatban dolgozók a mindennapi munkájuk során szembekerülhetnek.
2. Meghatároztam azokat a tudás-, képesség- és készségelemeket, amelyeket szükséges átadni a közszolgálatban dolgozó személyeknek, hogy a kiberbiztonsági feladataikat maradéktalanul elláthassák.
3. Megvizsgáltam azokat a kiberbiztonsággal kapcsolatos képzéseket, amelyekre Magyarországon jelenleg (2020 szeptemberétől) jelentkezni lehet. Összesen tíz ilyen képzést azonosítottam (alapképzések, mesterképzések és szakirányú továbbképzések felbontásában), bemutattam a képzések célját és alapvető

jellemzőit. Majd ezt követően megvizsgáltam, hogy a képzések tantervei lefedik-e a szükséges ismereteket.

4. Végül definiáltam a közszolgálati kiberbiztonsági képzés programját, amelyhez meghatároztam a képzés be- és kimeneti követelményeit és a képzés konkrét célját.

A kutatás folytatásaként elengedhetetlen a nemzetközi képzések vizsgálata az esetleges „jó gyakorlatok" átvétele érdekében, a képzés konkrét tematikájának kidolgozása, a számonkérések típusának meghatározása az egyes témakörökhöz, végül a képzési célok támogatásához szükséges műszaki környezet definiálása.

Felhasznált irodalom

Adatbiztonsági és adatvédelmi szakjogász szakleírás. ELTE Jogi Továbbképző Intézet. Elérhető: https://jotoki.elte.hu/content/adatbiztonsagi-es-adatvedelmi-szakjogasz.t.406 (A letöltés dátuma: 2020. 03. 19.)

Adatvédelmi és információbiztonsági menedzser szakirányú továbbképzés tartalma. Gábor Dénes Főiskola. Elérhető: http://gdf.hu/szakiranyu-tovabbkepzesek/adatvedelmi-es-informaciobiztonsagi-menedzser/ (A letöltés dátuma: 2020. 03. 21.)

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

Antal Zsolt: A közszolgálati kommunikáció eredményességére ható tényezők – A közszféra és a versenyszféra kommunikációs gyakorlatát befolyásoló különbségek. *Vezetéstudomány,* 49. (2018), 4. 68–76. DOI: https://doi.org/10.14267/VEZTUD.2018.04.07

Armstrong, Miriam E. – Keith S. Jones – Akbar Siami Namin: Framework for Developing a Brief Interview to Understand Cyber Defense Work: An Experience Report. *Proceedings of the Human Factors and Ergonomics Society 2017 Annual Meeting,* 61. (2017), 1. 1318–1322. DOI: https://doi.org/10.1177/1541931213601812

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.

Hazafi Zoltán: *Közszolgálati jogunk a változó nemzetközi és hazai térben*. Doktori értekezés. Pécsi Tudományegyetem, ÁJK Állam- és Jogtudományi Kar Doktori Iskola, 2009.

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

McDuffie, Ernest L. – Victor P. Piotrowski: The Future of Cybersecurity Education. *Computer,* 47. (2014), 8. 67–69. DOI: https://doi.org/10.1109/mc.2014.224

Nagyné Takács Veronika – Kovács László: Az információbiztonsági vezető szakirányú továbbképzés tapasztalatai. *Pro Publico Bono – Magyar Közigazgatás*, 3. (2015), 4. 85–99.

Elektronikus információbiztonsági vezető szakleírás. Nemzeti Közszolgálati Egyetem. Elérhető: https://kti.uni-nke.hu/szakiranyu-tovabbkepzesek/szakiranyu-tovabbkepzesi-szakok/elektronikus-informaciobiztonsagi-vezeto/altalanos-informaciok (A letöltés dátuma: 2020. 03. 19.)

Európai uniós adatvédelmi szaktanácsadó szakleírás. Nemzeti Közszolgálati Egyetem. Elérhető: https://kti.uni-nke.hu/szakiranyu-tovabbkepzesek/szakiranyu-tovabbkepzesi-szakok/europai-unios-adatvedelmi-szaktanacsado/altalanos-informaciok (A letöltés dátuma: 2020. 03. 14.)

Információbiztonsági szakmérnök/szakember képzés tartalma. Óbudai Egyetem. Elérhető: www.bgk.uni-obuda.hu/hu/kepzeseink/tovabbkepzesek/informaciobiztonsagi-szakmernokszakember (A letöltés dátuma: 2020. 03. 21.)

Kiberbiztonsági szakmérnök/szakember képzés tartalma. Óbudai Egyetem. Elérhető: http://bmi.nik.uni-obuda.hu/kiber_kovetelmeny (A letöltés dátuma: 2020. 03. 19.)

Nemzeti Közszolgálati Egyetem – Bűnügyi alapképzési szak – Kiber nyomozó szakirány. Elérhető: www.felvi.hu/felveteli/egyetemek_foiskolak/!IntezmenyiOldalak/meghirdetes.php?meg_id=20905&elj=20a (A letöltés dátuma: 2020. 03. 14.)

Nemzeti Közszolgálati Egyetem – Kiberbiztonsági mesterképzés. Elérhető: www.felvi.hu/felveteli/szakok_kepzesek/szakleirasok/!Szakleirasok/index.php/szak/20554/szakleiras (A letöltés dátuma: 2020. 03. 14.)

Newhouse, William – Stephanie Keith – Benjamin Scribner – Greg Witte: *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.* National Institute of Standards and Technology, 2017. DOI: https://doi.org/10.6028/NIST.SP.800-181

Óbudai Egyetem – Biztonságtechnikai mérnök alapképzési szak – Információbiztonsági specializáció. Elérhető: www.felvi.hu/felveteli/szakok_kepzesek/szakleirasok/!Szakleirasok/index.php/szak/36/szakleiras (A letöltés dátuma: 2020. 03. 14.)

Simon Béla: Kiberbűnözés elleni képzésfejlesztés. *Magyar Rendészet,* 18. (2018), 3. 193–207.

Som Zoltán: Az információbiztonság fejlesztési lehetőségei az EIV képzésen keresztül. *Társadalom és Honvédelem,* 20. (2016), 2. 167–175.

Védelmi infokommunikációs rendszertervező – Információbiztonsági szakirány szakleírás, tematika. Nemzeti Közszolgálati Egyetem. Elérhető: https://hhk.uni-nke.hu/oktatas/mesterkepzes/vedelmi-vezetestechnikai-rendszertervezo (A letöltés dátuma: 2020. 03. 14.)

Jogi források

2011. évi CCIV. törvény a nemzeti felsőoktatásról

2013. évi L. törvény az állami és önkormányzati szervezetek információbiztonságáról

87/2015. (IV. 9.) Korm. rendelet a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény egyes rendelkezéseinek végrehajtásáról