DOKTORI (PHD) ÉRTEKEZÉS SZERZŐI ISMERTETŐJE

NEMZETI KÖZSZOLGÁLATI EGYETEM
HADTUDOMÁNYI ÉS HONVÉDTISZTKÉPZŐ KAR
KATONAI MŰSZAKI DOKTORI ISKOLA

Dr. Debrecenine Deák Veronika

Közszolgálati kibervédelmi képességek képzésének lehetőségei

Tudományos témavezető:

Dr. Krasznay Csaba, PhD

Budapest, 2023.

Tartalomjegyzék

BEVEZETÉS

A kiberbiztonság egy gyorsan változó, fejlődő, illetve bővülő terület, amely napról napra újabb kihívásokat, veszélyeket tartogat számunkra, köszönhetően annak, hogy rohamosan változó világunkban a technológiai fejlődés soha nem látott méreteket ölt. A különféle infokommunikációs technológiák mai modern társadalmunk nélkülözhetetlen alkotóelemét képezik. Ennek következményeként a közszolgálatban is megfigyelhető ezen eszközök, technológiák alkalmazásának térhódítása.

Azonban ezek mindennapos használata és az egyre növekvő függőség számos kockázatot rejthet magában. A megfelelő szintű és minőségű kiberbiztonság megteremtése komplex feladatként jelentkezik, továbbá kritikus jelentőségűnek tekinthető az állami és a magánszféra működőképességének megteremtésében és folyamatos biztosításában egyaránt. A kibertámadások számának folyamatos növekedése és a támadások újabb eszközeinek, alternatíváinak megjelenése új típusú kihívásokat eredményeznek, valamint további védelmi mechanizmusok kialakítását és folyamatos fejlesztését teszi szükségessé. A kihívásokra és fenyegetésekre történő azonnali reagálás hatalmas terhet ró a szervezetekre. A közszolgálat és a különféle kritikus és kritikus információs infrastruktúrák a társadalom mindennapi működésének nélkülözhetetlen feltételeként értelmezhetők, ezért szükséges az ezek alapját képező információs rendszerek megbízható és biztonságos működésének folyamatos biztosítása.

Az elmúlt évek tapasztalatai alapján elmondható, hogy a közszolgálat kiemelt célpontja a kibertámadásoknak, a közszolgálati szervezetek ellen elkövetett kibertámadások mára mindennapossá váltak. A támadások elsősorban belső és bizalmas információk megszerzésére, illetve a különféle szolgálatatások működésének korlátozására irányulnak. 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 közszolgálatban is létfontosságú a kibervédelem folyamatos fejlesztése, a kibervédelmi képesség és a kiberbiztonság erősítése, amely megvalósításának alapvető elemei a kiberbiztonsági képzések, oktatások és gyakorlatok kidolgozása és lebonyolítása. A támadások jelentős része a felhasználók felkészületlenségét és biztonságtudatosságának hiányát célozza, éppen ezért az elsődleges cél a közszolgálatban dolgozók tudatosságának, kibervédelmi képességeinek kialakítása és folyamatos fejlesztése, amely eléréséhez elengedhetetlen egy olyan képzési forma megalkotása, amely segítségével e célok megvalósíthatók.

A TUDOMÁNYOS PROBLÉMA MEGFOGALMAZÁSA

A tudományos probléma alapjául szolgál, hogy **globális szinten kiberbiztonsági munkaerőhiány jelentkezik**. A Nemzetközi Információs Rendszer Biztonsági Tanúsító Konzorciuma (The International Information System Security Certification Consortium Inc. – ISC) 2021-es felmérése szerint a kiberbiztonsági munkaerőhiány csökkent ugyan (3,12 millióról 2,71 millió kiberbiztonsági szakemberre), azonban még így is komoly hiányosságokat eredményez. Az ISC szerint a globális kiberbiztonsági munkaerőnek 65%-kal kell növekednie ahhoz, hogy képes legyen hatékonyan megvédeni a szervezetek kritikus rendszereit, eszközeit. A kutatás rámutat arra, hogy a munkaerőhiány leküzdésének egyik legfontosabb eszköze a munkatársak szakmai képzése.[1] A munkaerőhiány kezelését és a közszolgálatban dolgozók kiberbiztonsággal kapcsolatos tudatosságát, képességeinek fejlesztését célozza egy olyan képzés kialakítása a közszolgálat számára, amely lehetővé teszi a szervezeti és személyi kiberbiztonság kialakítását és fejlesztését. Ennek megvalósítása elengedhetetlen, ugyanis **a megfelelő képzettségű szakemberek hiánya a közszolgálat, így az állam működésében jelentős korlátot, akadályokat eredményezhet.**

A kiberbiztonsági ismeretekkel felruházott munkaerő hiánya és ennek következtében a rendelkezésre álló emberi erőforrásra nehezedett többletfeladatok, illetve a nyomás számos negatív következményt generálhat. Ilyen valós káros hatások lehetnek többek között – a teljesség igénye nélkül - a kibertámadások felismerésének hiánya, figyelmen kívül hagyása, belső szabályozók be nem tartása, figyelmetlenségből és túlterheltségből fakadó rosszul konfigurált információs rendszerek, a lassabb javításokkal, frissítésekkel összefüggő feladatellátás, hiányos kockázatértékelés, az ellenőrzési vagy akár a felügyeleti szerepkör nem szakszerű ellátása. **A nem megfelelő feladatvégrehajtás számos kiberbiztonsági és működésbeli kockázatot eredményez.**

A tudományos probléma további elemeként értelmezhető, hogy a jelenlegi hazai helyzet alapján számos olyan a kibertámadási és -védelmi képesség kialakítását szolgáló képzés létezik, amelyek alapfeltétele, bemeneti követelménye valamilyen informatikai alapképzettség megléte, viszont **azok számára, akik nem rendelkeznek sem matematikai, sem pedig informatikai képzettséggel, nem biztosított a jelenleg rendelkezésre álló képzések abszolválása.** Éppen ezért szükséges egy olyan képzési program megalkotása, amely lehetőséget nyújt a közszolgálatban dolgozó, nem informatikai végzettségű személyek kibervédelmi képességének kialakítására. Ezen

[1] (ISC)², „Cybersecurity Workforce Study," 2021. [Online]. url: https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx.

képesség alatt a személyes kibertámadási és kibervédelmi jártasságok, készségek, képességek összessége érthető, amely képesség elsajátításának célja, hogy azok, akik nem rendelkeznek a szükséges alapismeretekkel, nem mozognak a témában otthonosan, megfelelő felkészítést kapjanak a hatékony és eredményes védelem kialakítása, a különféle kiberfenyegetések megelőzése, illetve a már bekövetkezett események eredményes elhárítása érdekében. Ezen személyek a közszolgálatban dolgoznak, nap mint nap részt vesznek a döntéshozatalban, így elengedhetetlen a kibervédelmi képességük kialakítása, mert ennek köszönhetően nem csak a komplex védelem kialakítása valósulhat meg, de képesek lesznek a kibervédelemmel kapcsolatos stratégiai döntések megalapozott meghozatalára is.

KUTATÁSI CÉLKITŰZÉSEK

Kutatásom fő célja, hogy egy olyan, a közszolgálati kiberbiztonság fejlesztését célzó képzést definiáljak, amely integrálható a közszolgálati képzési rendszerbe, és amely elméleti, illetve gyakorlati ismeretek elsajátításával teszi lehetővé a kibertérből érkező fenyegetések elleni védekezés hatékony és eredményes megvalósítását, így az állami működés akadálytalan, korlátozástól mentes biztosítását.

Figyelemmel az előzőekben ismertetett tudományos problémára és fő célkitűzésre, kutatásom céljai és az azokhoz tartozó részcélok az alábbiakban kerülnek bemutatásra.

Jelen értekezés alapjául szolgáló kutatás célja egy **tudományos alapokon nyugvó felsőoktatási képzések tervezésének lépéseit tartalmazó folyamatmodell definiálása**. Célom azonosítani az olyan egyértelmű feladatokat, lépéseket, amelyek szükségesek egy képzés definiálásához úgy, hogy a képzés akadémiai szempontból is megalapozott relevanciával bírjon, továbbá bizonyítottnak minősüljön.

A közszolgálati kiberbiztonsági képzés szükségességének vizsgálatához és megalkotásához elengedhetetlen **a megfelelő szintű kiberbiztonság megvalósításához szükséges tudás- és képességhalmaz meghatározása, valamint a képzés célcsoportjának azonosítása**. Ennek keretében szükséges megvizsgálni a közszolgálaton belül a konkrét célcsoportot, valamint azt, hogy melyek azok az általános kiberbiztonsági feladatok, amelyeket a közszolgálati dolgozóknak szükséges végrehajtaniuk akár a mindennapi munkájuk során, akár egy esetleges kibertámadás esetén. Ezt követően határozható csak meg a szükséges és elégséges tudás-, illetve ismerethalmaz, amelyet a célcsoportnak szükséges elsajátítania.

A kutatás további célja **annak feltárása, hogy jelenleg hazánkban, illetve nemzetközi szinten rendelkezésre áll-e a közszolgálat fejlesztését célzó, kibervédelmi képesség kialakítására és fejlesztésére irányuló gyakorlati képzési program. Ennek keretében célom a kibervédelmi képesség nemzetközi és hazai képzéseinek feltérképezése, összehasonlítása, a hazai és nemzetközi „jó gyakorlatok" azonosítása**. Ennek oka, hogy a kapcsolódó képzések és az esetleges hiányosságok feltárásával igazolható a közszolgálati kiberbiztonsági képzés szükségessége. Emellett az összehasonlító elemzés segítségével számos „jó gyakorlat" azonosítható, amelyeknek hazai képzésbe történő átültetése jelentősen hozzájárulhat a nemzetközi szinten is elismert képzés definiálásához.

Kutatásom célja a definiált tudás- és ismerethalmaz felhasználásával **a közszolgálati kibervédelmi képesség képzési programjának definiálása**. Ennek keretében szükséges a képzés formális specifikálása, alapvető elemeinek, céljának, valamint bemeneti és kimeneti követelményeinek meghatározása. Mindemellett jelen kutatás további célja feltárni, hogy a védelmi szektor egy speciális területén, az Önkéntes Tartalékos Rendszerben felhasználható-e a közszolgálati kiberbiztonsági képzés. Ennek érdekében szükséges megvizsgálni, hogy milyen további, az önkéntes tartalékos állomány szerepéből és jogállásából fakadó speciális jellemzőkön alapuló elemekkel szükséges bővíteni a korábban meghatározott, elsajátítandó tudás- és ismerethalmazt a képzés felhasználásához.

A képzés definiálását követően szükséges **meghatározni a képzési célok támogatásához szükséges műszaki keretrendszert, valamint annak gyakorlati megvalósulásának lehetőségeit**. E cél során arra a kérdésre keresem a választ, hogyan lehet elsajátítani a kibervédelmi képességeket, illetve hogyan lehet átadni a szükséges tudást, a különféle védelmi stratégiákat, technikákat olyan személyek részére, akik nem rendelkeznek informatikai előképzettséggel. A cél az, hogy olyan szakembereket képezzünk, akik gyakorlati ismeretekkel rendelkeznek. Ennek köszönhetően a kutatás részcélja egy olyan környezet kialakítása, amelyen keresztül a képzés résztvevői ismert kibertámadási technikákkal szembesülhetnek és egy szimulált, valós környezetben kipróbálhatják a képzés során megismert védelmi mechanizmusokat.

HIPOTÉZISEK

Kutatómunkám kezdetén a tudományos probléma megfogalmazását követően a következő hipotéziseket állítottam fel.

H1. Egy felsőoktatási kiberbiztonsági képzés definiálható tudományos alapokon.

H2. Azonosítható a közszolgálati kiberbiztonság megvalósításához szükséges célcsoport és az általuk elsajátítandó tudáshalmaz.

H3. Azzal a feltételezéssel élek, hogy korábban még nem született a közszolgálat fejlesztését célzó, kibervédelmi képesség kialakítására és fejlesztésére irányuló gyakorlati képzési program.

H4. Definiálható egy olyan, a közszolgálati kiberbiztonság fejlesztését célzó képzési program, amelynek teljesítése nem igényel informatikai előképzettséget.

H5. Definiálható egy olyan kiberbiztonsági tudatosság növelését célzó műszaki keretrendszer, amely lehetőséget biztosít a kibertámadások elleni védelmi mechanizmusok gyakorlatban történő alkalmazására.

KUTATÁSMÓDSZERTAN

A fentebb említett hipotézisek bizonyítására felhasznált kutatási módszereket a következőkben ismertetem.

Kutatásom során kvantitatív és kvalitatív kutatási módszereket is igénybe vettem. A kutatási téma inter- és multidiszciplináris jellegéből fakadóan megköveteli a kapcsolódó tudományterületek teljeskörű vizsgálatát. A kitűzött célok megvalósításához részt vettem a kiberbiztonsággal, információ- és informatikai biztonsággal, valamint az adatvédelemmel kapcsolatos tudományos rendezvényeken, konferenciákon, gyakorlatokon, majd ezt követően feldolgoztam, elemeztem és értékeltem az ott szerzett tapasztalatokat, ismereteket. Emellett folyamatosan nyomon követtem a kiberbiztonsággal, információ- és informatikai biztonsággal, valamint adatvédelemmel kapcsolatos aktualitásokat, fejleményeket a releváns szakfolyóiratok tanulmányozásával, valamint a hírközlési célú médiumokon keresztül, továbbá elemeztem, feldolgoztam és értékeltem a közelmúlt jelentős kibertámadások elleni védekezési eseményeit, tapasztalatait. Megvizsgáltam és elemeztem a jelenleg már elkészített, felhalmozott releváns oktatási anyagokat, segédanyagokat, elkészült doktori (PhD) disszertációkat, valamint a kiberbiztonsági szabályozás tárgyában kiadott nemzetközi, európai uniós és hazai szabályzókat, jogi szervezetszabályozó eszközöket, szabványokat, ajánlásokat és módszertani útmutatókat. Az összegyűjtött hazai és nemzetközi szakirodalmat analitikus módszerrel, majd a rendszerezést követően szintetizálással dolgoztam fel. A szakirodalom feldolgozása során az indukció és a dedukció módszerét is alkalmaztam.

Tudományos munkám során az általános és a különös kutatási módszereket egyaránt alkalmaztam. Az általános módszerek közül a megfigyelést és az összehasonlító módszert használtam fel a nemzetközi tapasztalatok vizsgálata során a külföldi példák hazai alkalmazásának vizsgálata, az esetleges hiányosságok feltárása és a „jó gyakorlatok" azonosítása érdekében. A megfigyelési módszerek közül a közvetlen és közvetett megfigyelést is alkalmaztam a különböző támadási alternatívák alkalmazási lehetőségeinek és korlátainak vizsgálatakor.

Kutatásom során konzultációt folytattam hazai és nemzetközi gyakorlati tapasztalattal rendelkező szakértőkkel, valamint interjút készítettem a „jó gyakorlatok", tapasztalatok képzésbe történő implementálásához, a képzés valós igényeknek megfelelő definiálásához. Mindemellett a kutatás alapjául szolgáló képzés résztvevőihez hasonló érintetti kör vonatkozásában fókuszcsoportos beszélgetés során gyűjtöttem véleményeket, tapasztalatokat és érzéseket a gyakorlati oktatás szerepéről.

Kutatásom részeredményeit folyamatosan publikáltam, illetve számos tudományos és szakmai konferencián, rendezvényen, fórumon ismertettem a tájékoztatás, a szakmai, gondolkodás elősegítése és a kapcsolódó reakciók feltárása céljából.

AZ ELVÉGZETT VIZSGÁLAT TÖMÖR LEÍRÁSA FEJEZETENKÉNT

Az 1. fejezetben megvizsgáltam, hogy azonosíthatóak-e olyan egyértelmű feladatok, amelyek szükségesek egy kiberbiztonsági képzés definiálásához úgy, hogy a képzés akadémiai szempontból is megalapozott relevanciával bírjon. Emellett e fejezetben elemeztem, hogy melyek azok a kutatási módszertanok, amelyeket egy tudományos kutatás során alkalmazni kell az egyes feladatok teljesítése esetén, hogy e feladatok megvalósítása tudományos szempontból is bizonyítottnak minősüljön. Ennek keretében azonosítottam és rendszereztem a képzés definiálásához szükséges sarkalatos pontokat, illetve lépéseket egy nyolcelemű folyamatmodell definiálásával, továbbá bemutattam azon kutatási módszereket, amelyek szükségesek egy képzés megalkotásához.

A 2. fejezetben egy interjún keresztül mutattam be a köz-és magánszférában megvalósuló kiberbiztonság közötti különbségeket, majd ez alapján azonosítottam a kibertér aktuális kihívásait. E fejezetben az interjúból levont következtetések, valamint dokumentumelemzés útján a releváns szakirodalom feldolgozásával, a közszolgálat fogalmának és komponenseinek vizsgálatával, definiáltam a közszolgálati kiberbiztonsági képzés célcsoportjának egyes elemeit és kivételi körét. Mindemellett a képzés célcsoportjának és az aktuális kiberbiztonsági kihívások meghatározását követően azonosítottam azokat az általános kiberbiztonsági feladatokat, amelyeket a

közszolgálatban dolgozóknak szükséges végrehajtani akár a mindennapi munkájuk során, akár egy esetleges kibertámadás esetén. Emellett e fejezetben meghatároztam azokat a tudás-, képesség- és készségelemeket, amelyeket szükséges átadni a közszolgálatban dolgozó személyeknek, hogy az azonosított kiberbiztonsági feladataikat maradéktalanul elláthassák.

Ezt követően a 3. fejezetben kerül sor a hazai és nemzetközi kiberbiztonsággal összefüggő felsőoktatási képzések azonosítására és összehasonlító elemzésére. A képzési program megalkotása során fel kell tárni a program megvalósíthatóságának lehetőségeit, valamint a hasonló hazai és nemzetközi képzéseket, ezen belül azok tartalmát, elemeit annak érdekében, hogy igazolható legyen a képzés létjogosultsága, továbbá, hogy feltárhassam az esetleges hiányosságokat, azok orvoslása, valamint az alkalmazott „jó gyakorlatokat", azok hazai képzési rendszerbe történő átültetése érdekében. Jelen fejezetben definiáltam egy kiválasztási módszert és összehasonlítási stratégiát, amelynek segítségével azonosítottam és összehasonlítottam a releváns hazai és nemzetközi kiberbiztonsággal kapcsolatos képzéseket, valamint e képzések azon elemeit és gyakorlatait, amelyek átültethetők a hazai közszolgálati kiberbiztonsági képzésbe.

Az 4. fejezetben megvizsgáltam az informatikai előképzettség szükségességét a kibervédelmi ismeretek hatékony megszerzésének függvényében. Emellett ismertettem a közszolgálati kiberbiztonsági képzés alapvető fogalmainak, elemeinek definícióját, értelmezését, valamint a képzés Magyar Képesítési Keretrendszer szerinti definícióját. E fejezetben bemutattam az önkéntes tartalékos állomány jogállását, valamint a kibervédelmi feladatok ellátásában betöltött jelenlegi és jövőbeli szerepét. Ezenkívül javaslatot tettem egy kibervédelmi alegység kialakítására az Önkéntes Tartalékos Rendszerben, és ismertettem a közszolgálati kiberbiztonsági képzés lehetséges felhasználását a képzésük során. A fejezetben bemutatásra kerül a képzés folyamatos fejlesztésének biztosítása céljából a tudásátadás hatékonyságának mérésére szolgáló szempontrendszer és mérési módszer, amely segítségével megvalósítható a képzés egyes tárgyainak iteratív fejlesztése.

Az 5. fejezetben bemutattam a kétlépcsős gyakorlati képzés működési környezetét, ahol a képzés résztvevői egy fiktív szervezeti infrastruktúra általános architektúráját, komponenseit, illetve azok védelmi mechanizmusait azonosítják, majd szimulált kibertámadások során védelmi stratégiákat alkalmaznak. Ennek megvalósítása érdekében azonosítottam a gyakorlati képzés alapját képező szimulációs környezetet leíró keretrendszert, amely a közszolgálatban dolgozó személyek kibertámadások felismerésére és elhárítására irányuló felkészítését szolgálja. Emellett ismertettem egy egyszerűsített szimulációs környezetet, amelyet a közszolgálati kiberbiztonsági képzés kapcsolódó saját infokommunikációs eszközök védelmére vonatkozó gyakorlati oktatásra

készítettem, ahol olyan kibertámadásokat mutattam be a gyakorlatban a hallgatóknak, amelyek elhárításához nem szükséges mély informatikai tudás.

ÖSSZEGZETT KÖVETKEZTETÉSEK

A kibertámadások száma exponenciális növekedést mutat, amelyek jelentős hatással vannak a gazdaságra, a társadalomra, valamint a szervezetek alapvető működésére nézve egyaránt. Egyre komplexebb és kifinomultabb kibertámadásokkal kell szembenéznünk nap mint nap, amelynek következtében új típusú kihívások jelennek meg a szervezetek életében. Ezzel összefüggésben szükséges kiemelni a szervezet és az abban dolgozó alkalmazottak kibervédelmi képességeinek kialakítását és fejlesztését, hiszen a megfelelő szintű felhasználói biztonságtudatosság jelentősen hozzájárulhat a kibertámadások bekövetkezési valószínűségének csökkentéséhez, valamint a támadások káros következményeinek mérsékléséhez.

A releváns kiberbiztonsági képességekkel rendelkező szakemberek felkutatása és foglalkoztatása során számos nehézséggel találkozhatunk, tekintettel a jelenleg fennálló kiberbiztonsági munkaerőhiányra, valamint ezen munkaerő iránti kereslet folyamatos növekedésére. A kibertámadások eredményes megelőzése és elhárítása érdekében elengedhetetlen a kibervédelmi képességek kialakítása és folyamatos fejlesztése. E képességek elsajátítására számtalan lehetőség áll rendelkezésünkre, a felsőoktatási képzésektől kezdve, a tudatosító kampányokon át, egészen a kibergyakorlatok megvalósításáig rendkívül széles skálán mozognak az elérhető kiberbiztonsági képzési programok. A megfelelő típusú képzés kiválasztásánál számos szempontot érdemes figyelembe venni, így például – a teljesség igénye nélkül - azok megvalósulási formáját, időtartamát, bemeneti követelményeit, a korábbi résztvevők gyakorlati tapasztalatait, tartalmát, valamint az elmélet és gyakorlat arányát.

A kibertámadások észlelése és előrejelzése komoly kihívásként jelentkezik, amelyek kezelésének alapvető eleme a felhasználók elméleti és gyakorlati kibervédelmi képességeinek kialakítása, fejlesztése. E célt hivatott szolgálni jelen értekezésben bemutatott közszolgálati kiberbiztonsági képzés definiálása, tekintettel arra, hogy a kiberbiztonsági oktatás rendkívül fontos szerepet tölt be a jelenlegi és a jövőbeli szakemberek kiberbiztonsági felkészítésében.

Értekezésem azon tudományos problémán alapul, hogy világszinten kiberbiztonsági munkaerőhiány jelentkezik, amely a közszolgálat alapvető működésének vonatkozásában is jelentős korlátot, akadályokat eredményezhet. Így például a megfelelő kompetenciákkal rendelkező szakemberek hiánya egy kibertámadás bekövetkezése esetén a szervezet üzletmenetfolytonosságát

is jelentősen befolyásolhatja. E káros hatások mérséklését és megelőzését szolgálja disszertációm legfőbb célkitűzéseként definiált közszolgálati kibervédelmi képesség kialakítását célzó képzési program tudományos alapokon történő definiálása.

Kutatásom kezdetekor abból a feltételezésből indultam ki, hogy egy felsőoktatási képzés definiálható tudományos alapokon. Annak érdekében, hogy e hipotézist bizonyítsam, **definiáltam egy nyolcelemű folyamatmodellt, amely meghatározza a tudományos alapokon nyugvó felsőoktatási képzések tervezésének lépéseit, valamint azonosítottam azon kutatási módszereket, amelyek szükségesek a képzés tudományos alapokon történő meghatározására**. A bemutatott folyamat és kutatási módszerek csak azon elemeket definiálják, amelyek egy képzés definiálásához szükségesek. Minél specifikusabb a célterület az egyes folyamatrészeket érdemes tovább bontani és további kutatási módszertanokat is lehet használni, hogy elégséges alapot képezzen a képzés helyességének bizonyítására. A definiált folyamatmodell és a kapcsolódó kutatási módszerek alkalmazhatóságát a közszolgálati kiberbiztonsági képzés teljeskörű definiálásával igazoltam.

Kutatásom célkitűzéseinek megfelelően vélelmeztem, hogy azonosítható a közszolgálati kiberbiztonság megvalósításához szükséges célcsoport és az általuk elsajátítandó tudáshalmaz. Ennek igazolására a képzési program megalkotásának kritériumfeltételeként **azonosítottam a közszolgálati kiberbiztonság megvalósításához szükséges célcsoportot, valamint az általuk elsajátítandó tudás-, képesség-, készséghalmazt,** amely segítségével a közszolgálatban megjelenő kiberbiztonsági feladatok az aktuális kiberbiztonsági kihívásokhoz igazodva végrehajthatók. Ennek oka, hogy a célcsoport és az elsajátítandó ismerethalmaz meghatározása elengedhetetlen a képzés szükségességének igazolásához, a hasonló típusú képzések feltárásához, valamint a kapcsolódó gyakorlati tapasztalatok azonosításához. Ahhoz, hogy e célcsoport és ismerethalmaz minél teljesebb körű definiálása megvalósulhasson, mélyinterjú és dokumentumelemzés segítségével azonosítottam a kibertér aktuális kihívásait, amelyhez szorosan igazodik a képzés során elsajátítandó tudáshalmaz.

Jelen értekezés azon a feltételezésen alapszik, hogy korábban még nem született konkrétan a közszolgálat fejlesztését célzó, kibervédelmi képesség kialakítására és fejlesztésére irányuló gyakorlati képzési program. Ennek bizonyítására egy általam definiált összehasonlítási szempontrendszer alapján összehasonlítottam és elemeztem a hazai, valamint nemzetközi kiberbiztonsággal összefüggő felsőoktatási képzéseket. Az összehasonlítással célom volt a képzési program megvalósíthatósági lehetőségeinek feltárása, tekintettel a képzésduplikáció elkerülésére,

hiszen amennyiben már létezik a jelen értekezésben célul kitűzött képzéssel tartalmában azonos képzés, nem indokolt annak megtervezése. Mindemellett az összehasonlítás segítségével feltártam a vizsgált képzések hiányosságait, valamint az alkalmazott „jó gyakorlatokat". A hazai és nemzetközi tapasztalatok implementálásának előnye, hogy ezek már olyan hazai és nemzetközi színtéren kipróbált és bevált gyakorlatok, amelyek hatékonyságát a felsőoktatási intézmények eredményei már korábban igazolták, így azok hazai képzési rendszerbe történő átültetése jelentősen hozzájárulhat a képzés színvonalának növeléséhez, továbbá minőségének megteremtéséhez. A fentiek segítségével **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.** Mindemellett igazoltam, 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.

Kutatási célkitűzéseim meghatározásakor vélelmeztem, hogy definiálható egy olyan, a közszolgálat fejlesztését célzó képzési program, amelynek teljesítése nem igényel informatikai előképzettséget. E hipotézis bizonyítása érdekében **definiáltam a közszolgálati kiberbiztonsági képzés programját, a képzés Magyar Képesítési Keretrendszer szerinti definícióját, a képzés alapjait, valamint a kapcsolódó alapfogalmakat, bemeneti és kimeneti követelményeit**. Ennek keretében azonosítottam a képzés struktúráját, elemeit és egy tantervi háló segítségével definiáltam a képzés elméleti és gyakorlati része során elsajátítandó ismerethalmaz egyes témaköreit, illetve azok tartalmát, amely többek között magában foglalja az elsajátítandó kibervédelmi mechanizmusokat, ismeretköröket. Ezt követően a közszolgálati kiberbiztonsági képzés Önkéntes Tartalékos Rendszerben történő alkalmazásának lehetőségére tettem javaslatot a korábban definiált képzés kibővítésével, átstrukturálásával. Emellett meghatároztam a képzés során megvalósuló tudásátadás hatékonyságának mérésére szolgáló szempontrendszert és mérési módszert, amely alapján megvizsgáltuk egy, a közszolgálati kiberbiztonsági képzés profiljába illeszkedő tantárgy tartalmának megfelelőségét, valamint az egyetemi oktatás során megvalósuló tudásátadás hatékonyságát. A tudásátadás hatékonyságát mérő koncepció segítségével a képzés tárgyainak fejlesztése folyamatosan biztosítható.

Kutatásom során azzal a feltételezéssel éltem, hogy definiálható egy olyan műszaki keretrendszer, amely lehetőséget biztosít kibertámadások elleni védelmi stratégiák gyakorlatban történő

alkalmazására. E hipotézis igazolására **meghatároztam a kétlépcsős gyakorlati képzés működési környezetét. Azonosítottam a gyakorlati képzés alapját képező szimulációs környezetet leíró keretrendszert, valamint definiáltam egy automatizált értékelési rendszert**, amely alkalmas a gyakorlati képzési rész során átadott tudásanyag számonkérésére. A szimulációs környezetet leíró keretrendszer szükségességét jelzi, hogy segítségével a közszolgálatban dolgozó személyeket fel lehet készíteni a kibertámadások észlelésére és esetleges bekövetkezése esetén azok következményeinek elhárítására, mérséklésére. A keretrendszer gyakorlati tapasztalatokra épül, amely egyéni és csoportos tanulási környezetet biztosít a hatékony és eredményes kibervédelmi technikák elsajátítására. A keretrendszer segítségével előre definiált specifikációk alapján automatizmusok útján hajtható végre a kibertámadások szimulálása és az azokkal szemben alkalmazható védelmi mechanizmusok gyakorlati alkalmazása.

ÚJ TUDOMÁNYOS EREDMÉNYEK

E1. Definiáltam egy nyolc elemből álló folyamatmodellt, amely meghatározza a tudományos alapokon nyugvó felsőoktatási képzések tervezésének lépéseit és a kapcsolódó kutatási módszereket.

E tudományos eredmény vonatkozásában egy 8 lépcsős folyamatmodellt definiáltam. A folyamatmodell helyességét, alkalmazhatóságát és akadémiai relevanciáját azzal bizonyítottam, hogy az egyes lépések megoldását lehetséges tudományos kutatási módszerek bemutatásával és azok egy esettanulmányon történő alkalmazásával támasztottam alá.

E2. Azonosítottam a közszolgálati kiberbiztonsági képzés célcsoportját és az általuk elsajátítandó tudáshalmaz-, képesség- és készséghalmazt.

Egy célzott mélyinterjú keretében vizsgáltam a köz- és magánszférában megvalósuló kibervédelem különbségeit. Az interjú lefolytatásának segítségével számos következtetést vontam le (pl. a kibervédelmi kockázatok mérséklése céljából a felhasználók tudatosítása és a technológiai fejlesztések szerepe), amelyek beépíthetők a közszolgálati kiberbiztonsági képzés tartalmába. Azonosítottam a képzés célcsoportját, valamint az e csoporthoz tartozó feladatokat. Emellett meghatároztam a feladatok végrehajtásához szükséges ismeret-, tudás-, képesség-, és készséghalmazt, amelyek segítségével a szervezet kibervédelemmel összefüggő tevékenysége elvégezhető.

E3. Bebizonyítottam, 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, amely nemzetközi szinten is releváns.

E tudományos eredmény keretében 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. Mindemellett igazoltam, 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.

E4. Definiáltam az informatikai előképzettséget nem igénylő közszolgálati kiberbiztonsági képzés struktúráját, képzési programját, egyes komponenseit, valamint általános értékelési rendszerét.

Meghatároztam a közszolgálati kiberbiztonsági képzés struktúráját, elemeit, valamint a kétlépcsős gyakorlati képzés keretében megvalósuló elméleti és gyakorlati rész általános tartalmát, amely magában foglalja az elsajátítandó kiberédelmi mechanizmusokat, ismeretköröket. Továbbá definiáltam a közszolgálati kiberbiztonsági képzést, annak be- és kimeneti követelményeit, valamint főbb elemeit a korábban meghatározott ismerethalmaz segítségével. Meghatároztam a tudásátadás hatékonyságát mérő koncepciót, amely alapján megvizsgáltuk egy, a közszolgálati kiberbiztonsági képzés profiljába illeszkedő tantárgy tartalmának megfelelőségét, valamint az egyetemi oktatás során megvalósuló tudásátadás hatékonyságát.

E5. Definiáltam egy olyan műszaki keretrendszert, amely lehetőséget biztosít kibertámadások elleni védelmi stratégiák gyakorlatban történő alkalmazására.

E tudományos eredmény vonatkozásában egy szimulációs környezetet leíró keretrendszert definiáltam, valamint felvázoltam a keretrendszer hardverarchitektúráját és bemutattam annak komponenseit, a kibertámadások szimulációját hardver és alkalmazás szintre lebontva. Emellett meghatároztam a szimulációs környezetben megvalósuló gyakorlati oktatás automatizált értékelési rendszerét. A kialakított rendszer hatékonyságát és alkalmazhatóságát a közszolgálati kiberbiztonsági képzés célcsoportjához illeszkedő résztvevők segítségével teszteltem le.

AJÁNLÁSOK ÉS GYAKORLATI FELHASZNÁLHATÓSÁG

Kutatásom során részletesen definiáltam egy, a közszolgálati kiberbiztonság fejlesztését célzó képzési programot, amely lehetőséget biztosít a nem informatikai előképzettséggel rendelkező, közszolgálatban dolgozó szakemberek releváns kibervédelmi képességeinek elsajátítására. Ebből következik, hogy értekezésem gyakorlati felhasználását ajánlom:

a) a közszolgálati képzési rendszer fejlesztéséért felelős szakemberek számára, a közszolgálati kiberbiztonsági képzés vagy annak egyes elemeinek implementálása érdekében;
b) a közszolgálatban dolgozó szakemberek számára az elsajátítandó ismerethalmaz alapján képességeik fejlesztése, ismereteik bővítése céljából;
c) közszolgálati szervezetek vezetőinek a szervezet foglalkoztatottjainak kibervédelmi felkészítése érdekében;
d) felsőoktatási intézmények részére a kapcsolódó felsőoktatási képzések felülvizsgálatának, kialakításának tervezésekor a jelen értekezésben bemutatott képzési program elemeinek implementálásához;
e) az Önkéntes Tartalékos Rendszer döntéshozóinak az önkéntes tartalékos állomány kibervédelmi képességeinek fejlesztését szóló képzés kialakításában.

Annak érdekében, hogy a kutatásomban elért eredmények gyakorlatban történő alkalmazása, hasznosíthatósága hosszútávon biztosítható legyen, célszerű meghatározni jelen értekezésben bemutatott kutatásom lehetséges folytatásának lehetőségeit.

A kutatás egyik legfőbb célja egy olyan gyakorlati képzés kialakítása volt, amely a közszolgálatban dolgozó személyek kibervédelmi képességeinek kialakítását és fejlesztését célozza. Ahhoz, hogy e képzési program gyakorlati felhasználása eredményesen megvalósulhasson, továbbá nemzetközi szinten is megfelelő értéket képviseljen elengedhetetlen a kutatás továbbfejlesztése. Ennek legfőbb alkotóelemét képezi egy olyan **közös platform, illetve fórum létrehozása, amely lehetőséget biztosít a kiberbiztonsági képzéseket szolgáltató hazai és nemzetközi egyetemek számára, hogy megoszthassák tapasztalataikat és alkalmazott „jó gyakorlataikat**”. A tudás- és tapasztalatmegosztás célja a kapcsolódó képzések folyamatos fejlesztése, a hiányosságok feltárása, valamint a releváns „jó gyakorlatok” saját képzésbe történő adaptálása. E platform segítségével a felsőoktatási intézmények a tudásátadás hatékonyságának mérésére szolgáló módszer alkalmazásával, valamint folyamatos vizsgálatok lefolytatásával, elemzések elkészítésével

feltárhatják hogyan fejleszthető a saját képzésük, továbbá milyen módosításokat, változtatásokat szükséges eszközölni a képzés minőségének javítása érdekében.

A DOKTORJELÖLT TÉMAKÖRBŐL KÉSZÜLT PUBLIKÁCIÓS JEGYZÉKE

Magyar nyelvű könyvfejezet

[1] Angyal I, Arató Gy, Bakos B, Baranya Zs, Bocsok V, Bogáncs T, Bonnyai T, Buttyán L, Csatár J, Danyek M, **Deák Veronika**, Görgey P, Gyebnár G, Illés G, Krasznay Cs, Molnár F, Pongrácz P, Szabó-Nyakas Zs, Szádeczky T, Szent-Királyi B, Winter G: Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyve – www.seconsys.eu (2021).

[2] **Deák Veronika**: *A közszolgálati kiberbiztonsági képzés tervezése tudományos alapokon* – Hausner Gábor (szerk): Szemelvények a katonai műszaki tudományok eredményeiből II., Ludovika Egyetemi Kiadó, 2021. Budapest, 63-82.

[3] **Deák Veronika**: Hírszerzés a kibertérben – Krasznay Csaba (szerk): Taktikák és stratégiák a kiberhadviselésben Ludovika Egyetemi Kiadó, 2023. Budapest, 87-114.

Lektorált nemzetközi idegen nyelvű folyóiratcikkek

[4] **Deák Veronika**: *Simulation Framework for Practical Cyber Security Training in the Public Service* – Security and Defense Quarterly: Non-military aspects of security in the changing international order, 33. évfolyam, 1. szám (2021), 87-104.

Lektorált hazai idegen nyelvű folyóiratcikkek

[5] **Deák Veronika**: *Finding differences on cyber security between public and private sectors* – National Security Review, 1. szám (2021), 169-180.

Lektorált magyar nyelvű folyóiratcikkek

[6] Krasznay Csaba, **Deák Veronika**: *Adatbiztonsági informatikai alapismeretek átadásának vizsgálata egy szakirányú továbbképzés keretében* – Hadmérnök, XVI. évfolyam 4. szám (2021), 112-132

[7] **Deák Veronika**: *A közszolgálati kiberbiztonsági képzés helye nemzetközi viszonylatban* – Hadmérnök, XV. évfolyam 4. szám (2020), 157-178

[8] **Deák Veronika**: *A közszolgálati kiberbiztonsági képzés lehetősége Magyarországon* – Hadmérnök, XV. évfolyam 3. szám (2020), 157-178.

[9] **Deák Veronika**: *A nyílt forrású információszerzés szerepe a kibertámadások végrehajtása során* – Hadmérnök, XIII. évfolyam 3. szám (2018), 391-402

[10] **Deák Veronika**: *Biztonságtudatosság az információs környezetben* – Szakmai Szemle, XV. évfolyam, 3. szám, 2017. november, 59-77.

[11] **Deák Veronika**: *Kártékony programok terjedése social engineering technikákon keresztül* – Hadmérnök, XIV. Évfolyam 2. szám (2019), 256-271

[12] **Deák Veronika**: *Prototípus implementáció kibervédelmi technikák gyakorlati oktatására* – (Elbírálás alatt)

[13] **Deák Veronika**: *Social engineering alapú információszerzés a kibertérben megvalósuló lélektani műveletek során* – Hadmérnök, XIV. Évfolyam 12. szám (2019), 95-111

[14] **Debreceniné Deák Veronika**, Hegyi Henrietta, Koczka Ferenc: *Felhőszolgáltatások műszaki és jogi szempontú attitűdvizsgálata* – Felderítő Szemle, XXI. évfolyam 1. szám (2022), 67-89.

Hazai szakmai konferencia kiadványában megjelent saját nyelvű absztrakt/poszter

[15] Beláz Annamária, **Deák Veronika***: Kiber gyakorlatok és szerepük (poszter),* A biztonság sokszínű arca konferencia, 2018. november 1. DOI:10.13140/RG.2.2.26756.37767

[16] **Deák Veronika**: *Social engineering és biztonságtudatosság*, XXIII. Tavaszi Szél konferencia Absztraktkötet, 2018., 140., ISBN: 978-615-5586-26-2

[17] **Deák Veronika**: *Social engineering felhasználása a lélektani műveletek során*, XXII. Tavaszi Szél konferencia Absztraktkötet, 2019., 240., ISBN: 978-615-5586-42-2

[18] **Deák Veronika**: *A közszolgálati kibervédelmi képesség gyakorlati képzésének technikai és technológiai alapjai*, XXIII. Tavaszi Szél konferencia Absztraktkötet, 2020., 188., ISBN:978-615-5586-70-5

A DOKTORJELÖLT SZAKMAI-TUDOMÁNYOS ÉLETRAJZA

Név: Dr. Debrecenine Deák Veronika

Tanulmányok:

2011-2015 Nemzeti Közszolgálati Egyetem, Közigazgatás-Tudományi Kar - igazgatásszervező alapképzési szak

2015-2017 Nemzeti Közszolgálati Egyetem, Államtudományi és Közigazgatási Kar - Közigazgatási mesterképzési szak – közigazgatási vezető szakirány

2016-2018 Eötvös Loránd Tudományegyetem, Jogi Továbbképző Intézet - Adatvédelmi és adatbiztonsági jogi szakokleveles szakember képzés

2017- Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola - PhD képzés

2021-2022 Nemzeti Közszolgálati Egyetem – Közigazgatási Továbbképzési Intézet - Elektronikus információbiztonsági vezető képzés

Szakmai pályafutás:

2019-től másfél éven keresztül a Login Autonom Kft. biztonságtechnikai tanácsadója volt. Ugyanettől az évtől a Probono közszolgálati továbbképzésért felelős portál felületén elérhető "IT Biztonság angyalai" informatikai biztonsági tudatosítást célzó csatorna adatvédelmi és adatbiztonsági szakértője. 2020. szeptember elsejétől a Nemzeti Közszolgálati Egyetem adatvédelmi tisztviselőjeként folytatta munkáját, majd 2022-től pedig e pozíció mellett az Adatvédelmi Iroda irodavezetőjeként látja el feladatait. Mindemellett 2017-től számos hazai és nemzetközi kutatási, valamint tananyagfejlesztési projektben vett részt.

Nyelvismeret:

Angol és német nyelvből középfokú komplex nyelvvizsgával rendelkezik.

Tagságok:

2018 és 2022 között tagként vett részt az NKE Egyetemi Doktori Tanácsának munkájában, 2018 óta pedig a Magyar Hadtudományi Társaság Elektronikai, Informatikai és Robotikai Szakosztályának tagja.

Díjak, elismerések:

2017-ben a XXXIII. OTDK, Had- és Rendészettudományi Szekció, Kiberbiztonság Tagozatában I. helyezést ért el pályamunkájával.