Szemelvények a katonai műszaki tudományok eredményeiből II.

Hallgatói kötet

Szerkesztette
Hausner Gábor

LUDOVIKA
EGYETEMI KIADÓ

Szemelvények a katonai műszaki tudományok eredményeiből II.

Szemelvények a katonai műszaki tudományok eredményeiből II.

Hallgatói kötet

Szerkesztette

Hausner Gábor

LUDOVIKA
EGYETEMI KIADÓ

Budapest, 2021

Szerzők

Ambrus Éva
Bodnár László
Csanádi Győző
Deák Veronika
Dévai Dóra
Domán László
Goda Zoltán
Huszár Péter
Huszár Viktor
Katona Gábor
Kralovánszky Kristóf
Kretz András
Kutassy Emese
Lakatos Bence Roland
Matusz Márk Péter
Olajosné Lakatos Boglárka
Priváczkiné Hajdu Zsuzsanna
Salamon Endre
Takács Krisztina
Terék Tamás
Tímár Attila

Szakmai lektorok

Bíró Tibor
Haig Zsolt
Padányi József
Palik Mátyás
Pohl Árpád
Restás Ágoston

Ludovika Egyetemi Kiadó
Székhely: 1089 Budapest, Orczy út 1.
Kapcsolat: info@ludovika.hu
A kiadásért felel: Koltay András rektor
Felelős szerkesztő: Karácsony Fanni
Olvasószerkesztő: Oláh Andrea
Korrektor: Bíró Csilla, Bujdosó Hajnalka
Tördelőszerkesztő: Fehér Angéla

ISBN 978-963-531-441-6 (PDF) | ISBN 978-963-531-442-3 (ePub)

Tartalom

Deák Veronika

A közszolgálati kiberbiztonsági képzés tervezése tudományos alapokon

Bevezetés

A kiberbiztonság gyorsan változó, fejlődő, illetve bővülő terület, amely napról napra újabb kihívásokat, veszélyeket tartogathat számunkra. A megfelelő szintű és minőségű kiberbiztonság megteremtése komplex feladatként jelentkezik, 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 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.

A közszolgálati szervezetek ellen elkövetett kibertámadások mára mindennapossá váltak. A támadások elsősorban belső és bizalmas információk megszerzésére, illetve a különféle szolgálatatások működésének korlátozására irányulnak. Ennek köszönhetően 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 képességének kialakítása és folyamatos fejlesztése, amely eléréséhez elengedhetetlen egy olyan képzési forma megalkotása, amely segítségével ezen célok megvalósíthatók. A Nemzetközi Információs Rendszer Biztonsági Tanúsító Konzorciuma (*The International Information System Security Certification Consortium Inc.* – ISC) felmérése szerint a kiberbiztonsági munkaerőhiány 2022-re eléri az 1,8 milliót.[1] Ez a hiány is azt mutatja, hogy egyre sürgetőbb a kiberbiztonsági munkaerő képzése. 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.

Ahhoz, hogy egy ilyen komplex képzés kidolgozása megvalósulhasson, fontos definiálni, hogy melyek azok a lépések és elemek, amelyek szükségesek egy tudományos

[1] Steve Morgan: Cybersecurity Jobs Report: A special report from the editors at Cybersecurity Ventures. *Cybercrime Magazine,* 2017.

alapokon nyugvó képzés kialakításához. Jelen publikációban azonosítom és rendszerezem ezen sarkalatos pontokat, illetve lépéseket, továbbá bemutatom azon kutatási módszereket, amelyek szükségesek a képzés tudományos alapokon történő meghatározásához. Az így definiált keretrendszer működését a közszolgálati kiberbiztonsági képzés megalkotásának folyamatával szemléltetem.

Jelen publikációban két fő hipotézist azonosítottam, amelyek megválaszolását tűztem ki célul. A hipotézisek a következők:

H1. Definiálható egy folyamatmodell, amely meghatározza a tudományos alapokon nyugvó felsőoktatási képzések tervezésének lépéseit.

H2. Azonosíthatók azon kutatási módszerek, amelyek szükségesek a képzés tudományos alapokon történő meghatározására.

Az első hipotézis célja azonosítani olyan egyértelmű feladatokat, amelyek szükségesek egy képzés definiálásához úgy, hogy a képzés akadémiai szempontból is megalapozott relevanciával bírjon. A második hipotézis során azt kell meghatározni, hogy melyek azok a kutatási módszertanok, amelyeket egy kutatás során alkalmazni kell az egyes feladatok esetén, hogy a feladatok megvalósítása akadémiai szempontból is bizonyítottnak minősüljön.

A fentebb említett hipotézisek megválaszolására a következőkben bemutatott módszereket használtam fel:

A hipotézisek igazolására egy 8 elemű folyamatmodellt definiáltam, amelyek között egyértelmű sorrend állítható fel. Az egyes feladatokhoz egyértelműen azonosítottam a releváns kutatási módszereket. A folyamatmodell helyességét, miszerint a modell segítségével előállított képzés akadémiai szempontból releváns, azzal bizonyítom, hogy az egyes lépések megoldását lehetséges tudományos kutatási módszerek bemutatásával és azok esettanulmányon történő alkalmazásával támasztom alá. A feladatokhoz kapcsolódó kutatási módszerek azonosítását pedig egy esettanulmányon keresztül bizonyítom.

Irodalmi áttekintés

Ahhoz, hogy a jelen tanulmányban célul kitűzött keretrendszer minden elemére kiterjedő definiálása, valamint tartalmának meghatározása során a szükséges kutatási módszerek azonosítása megvalósulhasson, nélkülözhetetlen a releváns hazai és nemzetközi szakirodalom mélyebb vizsgálata.

A kutatásmódszertan alapjai

Számos tudományos mű foglalkozik a tudományos kutatás elméleti, gyakorlati, illetve módszertani kérdéseivel. Hornyacsek Júlia *A tudományos kutatás elmélete és módszertana* című könyvében átfogó képet ad a tudományos kutatás gyakorlati alapjairól, módszereiről. Azonosítja a kvalitatív és kvantitatív módszerek csoportját, ezeken belül

a mérés, a megfigyelés, az elemzés, az esettanulmány, a kísérlet, a kérdezés, a tesztelés, a kérdőíves vizsgálat, illetve a dokumentumok elemzését határozza meg.[2]

Gőcze István *Tudományelmélet és kutatásmódszertan alapjai* című könyve a tudományos módszerek fajtáit és formáit három csoportba sorolja, amely alapján megkülönböztethetünk általános, különös és egyedi módszereket. Az általános módszerek az összes tudományra és annak bármely objektumára vonatkoznak. A különös módszerek valamennyi tudományban használatosak, de csak a kutatás tárgyának egy oldalára, például jelenségre vagy mennyiségre vonatkoznak.[3]

Carrie Williams tanulmányában három gyakori kutatási módszert mutat be: a kvalitatív, a kvantitatív és a vegyes módszereket. A kvantitatív módszerek közé sorolja a leíró módszert, a korrelációs, fejlesztési, megfigyelési, tervezési tanulmányokat és a felmérés egyes típusait, amelyek összehasonlító és okozati vizsgálati kutatásokban hatékonyan alkalmazhatók. A kvalitatív módszerek közé sorolja az esettanulmányt, a megalapozott elméletet, a néprajzi vizsgálatot és a tartalomelemzést.[4]

Képzéstervezéssel kapcsolatos tanulmányok

Az irodalomkutatás során olyan hasonló keretrendszereket, valamint tanulmányokat kerestem, amelyek választ adnak arra a kérdésre, hogy milyen komponensek, lépések szükségesek egy felsőoktatási képzés definiálásához.

Shaaron Pratt és Caroline Adams szerint egy új kurzus, illetve tanterv kidolgozása előtt és közben tíz kérdésre kell választ adni. Ide sorolhatók a képzés céljaira, tartalmára, annak megszervezésére, az oktatási stratégiák meghatározására, oktatói módszerekre és számos további, a képzés konkrét megszervezésére vonatkozó kérdések. A szerzők kifejtik, hogy a kurzus fejlesztésének (vagy egy már meglévő képzés újradefiniálásának) a folyamata egy irányító csoport létrehozásával kezdődik, amely általában a kurzus csapatának tagjaiból áll, és szükség esetén más egyetemek bevonásával történik. Az érvényesítési mechanizmus megköveteli a meglévő tanfolyam felülvizsgálatát. Az eredmények, a hallgatói visszajelzések, a külső vizsgáztatók észrevételei, a szakértői vélemények és az eredmények tükrében figyelembe vett erősségeket és gyengeségeket rögzíteni kell a tanterv tervezése során. Meg kell határozni a képzés kimenetelét, valamint a kívülről érkező igényeket. A kurzusnak tükröznie kell az aktuális iránymutatásokat, ajánlásokat, a kapcsolódó szakirodalmat és kutatásokat. A szerzők a tantervelméleti szakemberekre hivatkozva bemutatják, hogy a tantervben hivatalos tananyag, hivatalos tanterv, tényleges tanterv és rejtett tanterv is létezik, majd ismertetik ezek lényegét.[5]

Ping Wang és Fred Kohun cikkében rávilágít arra, hogy a különféle doktori programok tantervét és kurzusait folyamatosan frissíteni és fejleszteni kell a társadalom gyors

---

[2] Hornyacsek Júlia: *A tudományos kutatás elmélete és módszertana*. Budapest, NKE, 2014.

[3] Gőcze István: *Tudományelmélet és kutatásmódszertan alapjai*. Budapest, ZMNE, 2010.

[4] Carrie Williams: Research methods. *Journal of Business & Economics Research,* 5. (2007), 3. 65–72..

[5] Shaaron Pratt – Caroline Adams: How to create a degree course in radiography: a recipe. *Radiography,* 9. (2003), 4. 317–322.

változásainak kezelése érdekében, különösen az információs rendszerekkel és technológiákkal összefüggő programok esetében. A szerző kiemeli, hogy egy doktori képzés meghatározása során a szakmai és karriercélokat is figyelembe kell venni. Kiemelt figyelmet kell fordítani az úgynevezett moduláris tevékenységekre, amely azokra a képzésspecifikus tevékenységekre utal, amelyek közvetlenül hozzájárulnak a képzés tanulási eredményeihez és támogatják a szakmai és karriercélokat.[6]

Kiberbiztonsági képzések tervezésével kapcsolatos tanulmányok

Régner Sabillón és szerzőtársai olyan kiberbiztonsági képzést definiáltak, amelyen vállalatok alkalmazottai vehetnek részt vállalati szinten. A képzés négy elhatárolt csoportra bontja az alkalmazottakat: IT-szakértők, vezetők, operatív tagok és végfelhasználók. A csoportoknak különböző témaköröket definiálnak aszerint, hogy mi a számukra legszükségesebb továbbképzési pont. A képzés elvégzése után a képzés sikerességét nem személyenként vizsgálják, hanem a csoportokhoz kapcsolódó metrikákat ellenőrzik le később a vállalat mindennapi munkája során. A kiértékelés után a vállalatot érettségi szintjének megfelelő kategóriába sorolják (éretlen, fejlődő, érett, előrehaladott).[7]

Razvan Beuran és szerzőtársai a képzési tevékenységek három fő kategóriáját különítik el a kiberbiztonság témakörében: a támadásorientált képzést, az elemzésorientált képzést, valamint a védelemorientált képzést nevesítik. A szerzők szerint két követelmény megvalósulása szükséges a hatékony kiberbiztonsági képzési rendszer létrehozásához: az egyik a módosítás és az új képzési tartalmak hozzáadásának képessége, a másik a képzési környezet automatikus létrehozásának és kezelésének képessége.[8]

Marc J. Dupuis egy bevezető kiberbiztonsági tanfolyam szükségességét és fejlesztését mutatja be tanulmányában. A cikkben a szerző a kurzus tantervét, felépítését, tartalmát, előnyeit, valamint az esetleges kihívásokat is tárgyalja. Vizsgálja a kurzus kilenc fő célját és az azok alapján meghatározott témaköröket a félév során történő időbeli elhelyezkedésük alapján. A szerző szerint fontos a megfelelő értékelési rendszer kialakítása. A bemutatott képzés során a csoportos vetélkedőkből, projektekből, szakmai előadásokból, laborfeladatokból álló számonkérés a meghatározó.[9]

Patricia Toth és Penny Klein tanulmányukban bemutatják az amerikai szövetségi intézmények, szervezetek, részlegek informatikai, illetve kiberbiztonsági szerepalapú

[6] Ping Wang – Fred Kohun: Designing a doctoral level cybersecurity course. *Issues in Information Systems,* 20. (2018), 1. 88–99.

[7] Régner Sabillón et alii: An effective cybersecurity training model to support an organizational awareness program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada. *Journal of Cases on Information Technology,* 21. (2019), 3. 26–39.

[8] Razvan Beuran et alii: Integrated framework for hands-on cybersecurity training: CyTrONE. *Computers & Security,* (2018), 78. 43–59.

[9] Marc J. Dupuis: Cyber security for everyone: An introductory course for non-technical majors. *Journal of Cybersecurity Education, Research and Practice,* (2017), 1.

képzését. A publikáció relevanciáját a szerzők által bemutatott oktatási tervezési modell öt szakasza adja: az elemzés, a tervezés, a fejlesztés, a megvalósítás és az értékelés.[10]

Közszolgálati kiberbiztonsági képzés tervezése

Jelen publikáció motivációjaként a közszolgálati kiberbiztonsági képzés tervezését és kialakításának lépéseit és a lépések során felhasznált kutatási módszereket szeretném bemutatni, amelyek elengedhetetlenek a képzés kialakítása során.

A közszolgálati kiberbiztonsági képzés megalkotásához az igényt a közszolgálatban világszerte elkövetett számos kibertámadásból fakadó felelősségtudat és bizonytalanság adja. A támadások legfőbb célja a hálózatok, illetve infokommunikációs eszközök támadása annak érdekében, hogy hozzáférjenek például az állampolgárok, az alkalmazottak bizalmas, személyes adataihoz, védett szoftverekhez, alkalmazásokhoz, stratégiai tervekhez vagy bármilyen más egyéb, a támadó szempontjából fontos információhoz.

A támadások jelentős része a felhasználók felkészületlenségét és biztonságtudatosságának hiányát célozza, éppen ezért az elsődleges cél a közszolgálatban dolgozók tudatosságának, kibervédelmi képességének kialakítása és folyamatos fejlesztése, amely eléréséhez elengedhetetlen egy olyan képzési forma megalkotása, amely segítségével ezen célok megvalósíthatók.

A képzés meghatározása során a következő előre definiált követelményeknek kell megfelelni:

a) A képzést el kell határolni a meglévő képzésektől:
Meg kell vizsgálni, hogy a közszolgálatban dolgozók kibervédelmi tudatossága fejleszthető-e meglévő felsőoktatási képzéssel.

b) A képzésnek nemzetközi viszonylatban is elfogadottnak kell lennie:
A képzés során olyan ismereteket kell átadni, amelyek nem csak a hazai közszolgálati szférában alkalmazhatók, hiszen ezáltal a későbbiekben a nemzetközi színtéren definiált fejlesztések könnyebben átültethetők a hazai rendszerbe.

A képzés meghatározása során a következő kihívásokat kell megvizsgálni, ahogyan a 13. ábra is szemlélteti:

a) Mi az egyértelműen definiált célcsoport?
Pontosan meg kell határozni, hogy a közszolgálatban kik azok a személyek, akik számára releváns lehet a képzés. Ha túl általános a célcsoport, akkor a képzés során átadott tudásnak is kellően általánosnak kell lennie, míg túlságosan specifikus célcsoport esetén szakterület-specifikus képzést kell kialakítani.

b) Mi a képzés bemeneti feltétele?

[10] Patricia Toth – Penny Klein: *A role-based model for federal information technology/cyber security training.* NIST special publication, 800-16. 2014. 1–152.

Meg kell határozni, hogy a közszolgálati dolgozók számára milyen előfeltételeket kell megszabni, hogy a képzésen részt vegyenek. Olyan személynek, akinek nem jelent újdonságot a képzés, nem feltétlenül szükséges a képzés elvégzése.

c) Mi a képzés kimeneti feltétele?
A képzés elvégzése után milyen képességeket és készségeket várunk el a végzett hallgatóktól.

d) Hogyan lehet biztosítani a képzés folyamatos fejlesztését?
A kibertámadási és kibervédelmi stratégiák rendkívül gyorsan változnak a világban, ezért egy olyan képzést kell meghatározni, amely képes a bekövetkezett változásokra megfelelően gyorsan reagálni.

1. ábra: *Az esettanulmány kihívásai*
Forrás: a szerző szerkesztése

Kutatási módszertanok

Ahogyan az a 2. fejezetben is látható, a kutatási módszertanokat különbözőféleképpen lehet azonosítani, illetve csoportosítani. Jelen fejezet célja a publikáció kutatásmódszertani fogalmi rendszerének meghatározása.

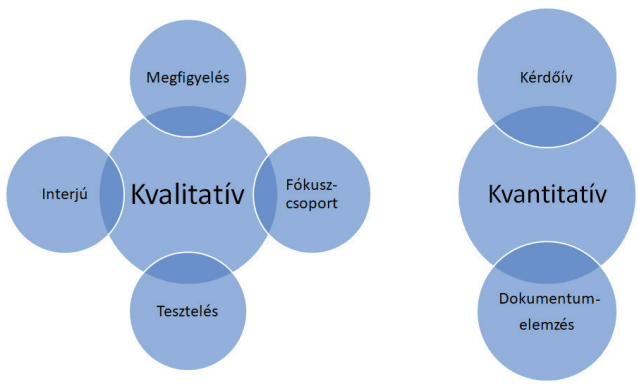
A fogalmi rendszer meghatározása Hornyacsek Júlia *A tudományos kutatás elmélete és módszertana* című művét veszi alapul, azonban csak a publikáció szempontjából releváns módszertanokat tekintem át.[11] Ez alapján az egyes módszereket típusokba sorolhatjuk, amely szerint egy módszer lehet kvalitatív vagy kvantitatív módszer:

- *kvalitatív módszerek:* a tudományterület minőségi mutatóinak vizsgálata;
- *kvantitatív módszerek:* a tudományterület mennyiségi mutatóinak vizsgálata.

Jelen publikáció szempontjából releváns kutatási módszereket a 2. ábra szemlélteti, meghatározásuk pedig az alábbiak:

[11] Hornyacsek (2014) i. m.

– *Interjú:* olyan kvalitatív módszer, amely során az interjúalany előre meghatározott kifejtős kérdésekre válaszol olyan témában, amelynek szakértője. A válaszai azonban nemcsak tárgyilagosak, hanem tartalmazzák a személyes véleményét is.
– *Dokumentumelemzés:* olyan kvantitatív módszer, amely során adott témához kapcsolódó dokumentumok részletes elemzése során juthatunk adatokhoz.
– *Tesztelés:* olyan kvalitatív módszer, amely során egy kontrollcsoport ellenőrzött körülmények között végez el meghatározott feladatokat, amelynek sikeressége alátámasztja a hipotézist.
– *Fókuszcsoport:* olyan kvalitatív módszer, amely során egy csoporttal folytatott beszélgetés alatt gyűjtünk véleményeket, érzéseket egy adott problématerülettel kapcsolatban.
– *Megfigyelés:* olyan kvalitatív módszer, amely során az információgyűjtéshez tapasztalati észrevételeket használunk.
– *Kérdőív:* olyan kvantitatív módszer, amely során a kitöltő eldöntendő vagy feleletválasztós kérdésekre válaszol, ezáltal az eredmény mindig tárgyilagos marad, és statisztikai következtetések vonhatók le belőlük.



2. ábra: *Felhasznált kutatási módszerek csoportosítása*
Forrás: a szerző szerkesztése

Felsőoktatási képzések tervezésének lépései

Egy felsőoktatási képzés tervezése során feltételezhetjük, hogy a tervezés szükségessége már alátámasztott, vagyis akár az iparból, akár a közszférából megjelent az igény egy képzésre, amely a főbb jellemzőket azonosítja (például magas szintű témakörök, irányvonalak). Amennyiben ezen igény nem bizonyított, úgy a tervezés 0. lépése annak igazolása.

A tervezési folyamatnak a 3. ábrán olvasható szakaszait különíthetjük el élesen. Jelen fejezet bemutatja ezen szakaszok tartalmát és ezzel párhuzamosan az alkalmazható kutatási módszereket, illetve a közszolgálati kiberbiztonsági képzés tervezésével szemlélteti az egyes pontok gyakorlati megvalósítását. Fontos kiemelni, hogy a kutatási módszerek alkalmazása során elért eredmények nem kontribúciói jelen publikációnak.

3. ábra: Felsőoktatási képzések tervezésének lépései
Forrás: a szerző szerkesztése

Releváns szereplők meghallgatása

A folyamat első lépése a releváns szereplők meghallgatása, a képzés szükségességének és relevanciájának feltárása. Ezen lépés elengedhetetlen a képzés megfelelő tervezéséhez, hiszen itt kerül sor a gyakorlati tapasztalattal rendelkező szakértők bevonására, meghallgatására. Ennek célja, hogy átfogó képet kaphassunk arról, az adott szakterületen tapasztalattal rendelkező személyek indokoltnak gondolják-e a tervezett képzést, és amennyiben igen, mit tartanak fontosnak, milyen főbb komponensek, tartalmi elemek szükségesek a képzés megvalósításához. A szakértői vélemények bevonása elengedhetetlen a jó gyakorlatok, tapasztalatok képzésbe történő implementálásához, a képzés valós igényeknek megfelelő definiálásához, valamint a képzés tervezésének későbbi szakaszában a képzés folyamatos fejlesztéséhez is. Az ilyen gyakorlati szakemberek segítségével könnyen feltárhatók az esetleges erősségei és gyengeségei a létrehozni kívánt képzésnek, hiszen szakértelmüknek és jártasságuknak köszönhetően valódi tapasztalattal rendelkeznek, ismerik a releváns képzéseket, a tudományterület főbb irányvonalait és az aktuális kihívásokat.

Kapcsolódó kutatási módszerek: dokumentumelemzés, interjú

A releváns szereplők meghallgatásához elengedhetetlen kutatási módszer az interjú, illetve az interjúalanyok által publikált dokumentumok elemzése, továbbá ezen dokumentumokban hivatkozott publikációk elemzése. Az interjú kulcsfontosságú eszköz ahhoz, hogy a képzéshez kapcsolódóan szaktekintélyek véleményét hallgassuk meg, és ne csak egyetlen nézőpontot alkalmazzunk a képzés létrehozása során. Az itt kapcsolódó dokumentumok olyan információkat tartalmazhatnak, amelyek a képzés kialakításának fő irányvonalát befolyásolhatják, kontextusát azonosíthatják.

Kutatási módszerek alkalmazása

A közszolgálati kiberbiztonsági képzés tervezésének első lépéseként olyan szakemberek után kutattam, akik kellő tapasztalattal és jártassággal rendelkeznek a témában, tisztában vannak a lehetőségekkel és az esetlegesen felmerülő problémákkal. Számos szakértő véleményét kikértem a képzés relevanciájával és megvalósításának alternatíváival kapcsolatban, akik számtalan javaslatot fogalmaztak meg, amelyeket felhasználtam a képzés tervezése során. A szakértők bevonását javarészt interjúk lefolytatásával hajtottam végre, amely során feltárt tapasztalatokat, jó gyakorlatokat beépítettem a képzésbe annak definiálása során. Következtetések levonását célozta a Dr. Muha Lajossal és Dr. Otti Csabával készült összehasonlító interjúm, amely során arra kerestem a választ, hogy egyértelműen meghatározható-e különbség a magánszektor és a közszolgálat között kibervédelem szempontjából. Ez magában foglalta a személyek kiberbiztonsági képzését, a technológiai fejlesztések megvalósítását, a kiberbiztonsággal kapcsolatos financiális és stratégiai döntések meghozatalának szerepét és az egyes szervezetek kibervédelmi eszközeit, intézkedéseit. Az interjúkérdésekre adott válaszok és az azonosított limitációk alapján megállapítható, hogy nem határozható meg egyértelmű különbség a magánszektor és a közszolgálat között kibervédelem szempontjából. Mindkét interjúalany kijelentette, hogy bár lehetnek különbségek a fent említett két szektor között, azonban rendkívül nagy az átfedés. Külön kiemelendő, hogy az interjúalanyok inkább a kritikusság szintjei szerint látnak eltéréseket a kibervédelem tekintetében, azonban a feladatok és védelmi stratégiák nagyrészt megegyeznek.

A célcsoport meghatározása

Ahhoz, hogy a képzés minden elemére kiterjedő definiálás megvalósulhasson, elengedhetetlen a célcsoport meghatározása. A célcsoport meghatározása során fontos azonosítani a korcsoportot, az előképzettséget és a szakmai tapasztalatot, hiszen ennek következtében a célcsoportnak megfelelő tartalmú képzés hozható létre. Ennek segítségével az is meghatározható, hogy a képzés általános vagy az adott szakterületre jellemző ismeretekkel, problémákkal és kihívásokkal foglalkozik.

Kapcsolódó kutatási módszerek: dokumentumelemzés, interjú

A dokumentumelemzés jó kiindulópont a célcsoportok meghatározására, ahol a releváns jogszabályok áttekintését és az interjú eszközét is lehetséges használni. Ez utóbbi esetben a témakörspecifikus tudással rendelkező interjúalanyok különböző nézőpontok alapján szűkíthetik vagy tágíthatják azon személyek halmazát, akik számára szükséges lehet egy képzés.

Kutatási módszerek alkalmazása

A közszolgálati kiberbiztonsági képzés tervezése során a célcsoport kiválasztásához megvizsgáltam a közszolgálat definícióját, amelyből következik, hogy annak alkalmazotti csoportja rendkívül széles spektrumú, mind az ide tartozó munkaköröknek, mind az alkalmazottak képességeinek, készségeinek köszönhetően. Éppen ezért fontos a képzés szempontjából releváns közszolgálati alkalmazotti kör szűkítése olyan területekre, amelyek kiberbiztonsági kockázatot jelenthetnek, részt vesznek a döntéshozatalban, és esetlegesen a korábbi képzéseik során nem részesültek részletes, átfogó kiberbiztonsági oktatásban. Ezek alapján az alábbi munkaköröket határoztam meg 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.

Az átadni kívánt képességek és készségek meghatározása

A képzés felépítésének és tartalmának meghatározásához szükséges az átadni kívánt képességek és készségek definiálása. Ennek első lépése, hogy azonosítsuk azokat az általános feladatokat, amelyeket a célcsoport a mindennapi munkája során végrehajt. Ezt követően kerülhet sor a feladatok ellátásához szükséges tudáshalmaz, valamint az ennek elsajátítását követően megszerzett képességek és készségek definiálására. Természetesen a feladatok és az ismerethalmaz meghatározását nagyban befolyásolja, hogy az adott képzés célja általános vagy szakterületspecifikus ismeretek átadása.

Kapcsolódó kutatási módszerek: megfigyelés, dokumentumelemzés

A megfigyelés eszköze elengedhetetlen a képzések definiálása során, így a saját tapasztalatainkra hagyatkozva azonosíthatjuk a szükséges elemeket. A másik fontos kutatási módszer a dokumentumelemzés, amely során azt vizsgáljuk meg, hogy a szakirodalomban milyen igények jelentek meg a témakörben releváns képességekre és készségekre.

Kutatási módszerek alkalmazása

A közszolgálati kiberbiztonsági képzés tervezése során azonosítottam azokat az általános kiberbiztonsági feladatokat, amelyeket a közszolgálati dolgozóknak szükséges végrehajtani akár a mindennapi munkájuk során, akár egy esetleges kibertámadás esetén. Ahhoz, hogy ezen feladatokat a közszolgálatban dolgozó alkalmazottak maradéktalanul el tudják látni, meghatároztam az ahhoz szükséges ismerethalmazt. A feladatokat, a tudás- és készség-, képességhalmazokat a NICE-keretrendszer[12] segítségével definiáltam, úgy, hogy kiválasztottam a képzés célcsoportjához leginkább illeszkedő munkakört, és megvizsgáltam a keretrendszerben rögzített feladatokat, valamint készségek, képességek halmazát.[13] Ezt követően további elemekkel egészítettem ki a listát, mivel saját tapasztalatom alapján vannak olyan területek, amelyeket a NICE-keretrendszer nem fed le (például az emberi tényezőn alapuló sebezhetőség, *social engineering*). A célcsoport számára szükséges tudást az alábbi lista foglalja össze, ahol a K1–5 pontokat a NICE határozza meg, míg a K6–9 az általam hozzáadott pontok:

K1. számítógéphálózatokhoz kapcsolódó alapfogalmak ismerete;
K2. kockázatkezelési folyamatok ismerete;
K3. kiberbiztonsági, adatvédelmi jogszabályok, irányelvek, alapelvek ismerete;
K4. kibertérből érkező fenyegetések ismerete;
K5. vezeték nélküli technológiák ismerete;
K6. az állami kibervédelmi rendszer ismerete;
K7. a szervezeten belüli kiberbiztonsági és adatvédelmi felelős pozíciók ismerete;
K8. a kibertámadások esetén alkalmazható technikák, eljárások ismerete;
K9. az emberi tényezők és a kiberbiztonság kapcsolódási pontjainak ismerete;
K10. a kibertámadások mögött rejlő motivációk és pszichológiai tényezők ismerete.

Hazai képzések vizsgálata

Egy képzés tervezésekor minden esetben meg kell vizsgálni az aktuális, nemzeti képzéseket, azok tartalmát és felépítését a képzésduplikáció elkerülése érdekében, hiszen amennyiben már létezik az általunk létrehozni kívánt képzéssel tartalmában azonos képzés, nem indokolt annak definiálása, megtervezése. Ehhez azokat a képzéseket kell megvizsgálni, amelyeknek célcsoportja azonos vagy annál tágabb és azt, hogy az átadott tudáshalmaz lefedi-e az előző lépésben meghatározott képességeket és készségeket. Ezenkívül a vizsgálat segítségével meghatározhatók az esetleges hiányosságok, jó gyakorlatok, valamint a képzés felhasználási lehetőségei.

---

[12] 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 ezen munkakörök betöltéséhez szükséges képességeket, készségeket, továbbá elsajátítandó ismeretköröket.

[13] William D. Newhouse et alii: *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce.* NIST Special Publication 800-181, 2017.

Kapcsolódó kutatási módszerek: dokumentumelemzés

A hazai képzések vizsgálatához természetesen dokumentumelemzésre van szükség, hiszen át kell tekinteni az összes hazai képzést, amely a témába vág. Erre jó kiindulópont jelenleg a Felvi.hu,[14] amely az összes felsőoktatási képzést tartalmazza. Ezek mellett a hazai akadémiai publikációkat is szükséges megvizsgálni, hiszen ebből kiderülhet, hogy már tervben van-e hasonló képzés kialakítása.

Kutatási módszerek alkalmazása

A közszolgálati kiberbiztonsági képzés tervezésének elengedhetetlen lépése azon kiberbiztonsággal kapcsolatos képzések elemzése, amelyekre a vizsgálat időpontjában jelentkezni lehetett. Összesen tíz ilyen felsőoktatási képzést azonosítottam és megvizsgáltam, hogy a képzés tantervében szerepelnek-e a NICE-keretrendszer által, valamint az általam meghatározott szükséges alapismeretek. Az elemzés alapján megállapítható, hogy a jelenlegi felsőoktatási képzési rendszer minden szintjén elérhető kiberbiztonsággal, információbiztonsággal foglalkozó képzés, azonban olyan képzés nem létezik, amely teljeskörűen lefedné a közszolgálati kibervédelmi képesség kialakításához szükséges alapismereteket.

A képzések összehasonlítása a 10. táblázatban található, ahol a vizsgált képzések a következők voltak:

a) Nemzeti Közszolgálati Egyetem Kiber nyomozó szakirány (NKE KNY);
b) Óbudai Egyetem Biztonságtechnikai mérnök alapképzési szak (ÓE BM);
c) Nemzeti Közszolgálati Egyetem Kiberbiztonsági mesterképzés (NKE KB);
d) Nemzeti Közszolgálati Egyetem Védelmi infokommunikációs rendszertervező mesterképzés (NKE VIKR);
e) Nemzeti Közszolgálati Egyetem Elektronikus információbiztonsági vezető szakirányú továbbképzés (NKE EIB);
f) Nemzeti Közszolgálati Egyetem Európai uniós adatvédelmi szaktanácsadó szakirányú továbbképzési szak (NKE EUA);
g) Eötvös Loránd Tudományegyetem Adatbiztonsági és adatvédelmi szakjogász/ szakember szakirányú továbbképzés (ELTE ASZ);
h) Óbudai Egyetem Kiberbiztonsági szakmérnök/szakember szakirányú továbbképzés (ÓE KSZ);
i) Óbudai Egyetem Információbiztonsági szakmérnök/szakember szakirányú továbbképzés (ÓE ISZ);
j) Gábor Dénes Főiskola Adatvédelmi és információbiztonsági menedzser szakirányú továbbképzés (GDF AIM).

[14] www.felvi.hu/

Az összehasonlító táblázat cellájába 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.

10. táblázat: Hazai kiberbiztonsággal kapcsolatos képzések összehasonlítása tudáselemek szerint

Képzési forma	Képzés rövidítése	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10
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	-	✔	✔	-	-	✔	✔	-	-	–

Forrás: a szerző szerkesztése

Nemzetközi képzések vizsgálata

A képzés kialakításához mindenképpen szükséges feltérképezni és megvizsgálni a nemzetközi oktatásban megjelenő kiberbiztonsággal, információbiztonsággal kapcsolatos képzéseket. Ezen belül is a képzések rendszerét, struktúráját, felépítését és tartalmát annak érdekében, hogy a nemzetközi tapasztalatok vizsgálata során feltárt jó gyakorlatok esetleges átültetése megvalósulhasson a nemzeti oktatásban. A nemzetközi képzések vizsgálata azért is indokolt, hiszen ennek segítségével megállapítható, hogy egy hazai képzés nemzetközi szinten is releváns képzésnek minősül-e, ha a képzés során átadott tudás nemzetközi színtéren is értéket képvisel.

Kapcsolódó kutatási módszerek: dokumentumelemzés

A nemzetközi képzések vizsgálatához, hasonlóan a hazai képzések vizsgálata esetén, dokumentumelemzésre van szükség, hiszen át kell tekinteni a releváns nemzetközi képzéseket, amelyek az adott témához kapcsolódnak. Erre jó kiindulópont lehet

a TopUniversities.com[15] weboldal, amely csoportosítva ad hozzáférést a nemzetközi képzésekhez. Ezek mellett az akadémiai publikációkat is érdemes megvizsgálni, hiszen ebből kiderülhet, milyen kihívásokkal küzdöttek meg mások hasonló képzés megalkotása során.

Kutatási módszerek alkalmazása

A közszolgálati kiberbiztonsági képzés tervezése során a nemzetközi képzések feltárásához egy kiválasztási módszert és egy összehasonlítási stratégiát definiáltam. A kiválasztási módszer lényege, hogy a képzések három csoportját különítettem el, majd azok felkutatására a QS World University Rankings által felállított világszintű egyetemi rangsort használtam. Kilistáztam az általános és a téma szerinti rangsort, és sorban haladva megvizsgáltam az országok egyetemeit, minden országból egyet választottam ki, amely megfelel a feltételeknek. Minden csoporthoz három egyetemet társítottam a könnyű áttekintés érdekében, majd pedig egy általam felvázolt szempontrendszer szerint vizsgáltam meg a képzéseiket. A vizsgálati szempontok közé tartozik a képzés rangsorban betöltött helye, pontos neve, időtartama, a költségtérítés formája, a képzés feltételei, a bemeneti és kimeneti követelmények, a képzés oktatási anyagai, illetve tartalmuk, az adott képzés során átadott képességek és készségek, továbbá a NICE keretrendszer elemeinek az adott képzésben történő megjelenése.

A vizsgált képzéseket összehasonlítottam a korábban definiált tudáshalmaz tartalombeli megjelenése alapján, valamint azonosítottam az elemzés során feltárt jó gyakorlatokat. Ezek alapján bizonyítottam, hogy a közszolgálati kiberbiztonsági képzés nemzetközi szinten is releváns képzésnek tekinthető. A vizsgált képzések képzési tervében szinte az összes korábban definiált tudáselem megjelenik, amely azt mutatja, hogy ezen ismeretkörök a közszolgálati kiberbiztonsági képzés esetében is helytállóak.

A képzés formális specifikálása

A képzés tervezésének következő lépése a formális specifikáció, amely segítségével meghatározhatók a bemeneti és kimeneti követelmények, vagyis hogy mik azok a feltételek és korábbi tanulmányok, amelyek elengedhetetlenek a képzésen való részvételhez, illetve mik azok az elemek, amelyeket a képzés után a hallgató a magáénak tudhat majd.

Kapcsolódó kutatási módszerek: dokumentumelemzés

A képzés formális specifikációjához a releváns jogszabályokat kell áttekinteni, amelyek meghatározzák, hogy mit szükséges a definíció során kötelezően meghatározni. Ezen kívül célszerű a hasonló képzések definícióját, célkitűzéseit is megvizsgálni.

[15] www.topuniversities.com

Kutatási módszerek alkalmazása

A korábbi tanulmányomban[16] rögzített definíció szerint a közszolgálati kiberbiztonsági képzés 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 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 kimeneti követelménye, hogy a képzést elvégző személy képes legyen a korábbi tanulmányban[17] azonosított feladatok elvégzésére saját munkakörnyezetében, így a teljesség igénye nélkül például:

T1. adatvédelmi, adatbiztonsági érdekek képviselése a szervezeten belül;
T2. a különféle döntéshozatali folyamatok során megjelenő kockázatelemzés elkészítése;
T3. releváns jogszabályok ismerete;
T4. hazai és külföldi „jó gyakorlatok” alkalmazása;
T5. kiberbiztonsági fenyegetések, támadások felismerése és szegregálása;
T6. a humán fenyegetettségből eredő kockázatok azonosítása;
T7. kiberbiztonsággal, adatvédelemmel kapcsolatos képzések, oktatások megtartása, lebonyolítása.

A képzési struktúra és a témakörök meghatározása

A képzés struktúrájának és tartalmának meghatározása elengedhetetlen a képzés működése és a korábban meghatározott tudáshalmaz eredményes átadása szempontjából. Ezen lépésben kerül sor a képzés felépítésének és tartalmának definiálására, amely segítségével azonosítható, hogy mely témakörök futhatnak például párhuzamosan, egymással azonos időtartam, félév alatt. A struktúra kialakítása során figyelembe kell venni az egyes témakörök, valamint a gyakorlati részt tartalmazó képzés esetén az elméleti és gyakorlati oktatás sorrendiségét annak érdekében, hogy elkerüljük a témakörök közötti előreutalást, ami által a hallgatók számára olyan tudást adnánk át, amelynek alapjait majd csak későbbi félévben sajátítanák el. Továbbá meg kell határozni a képzés tantárgyainak, valamint azok tantárgyi adatlapjainak alapjául szolgáló témaköröket.

[16] Deák Veronika: A közszolgálati kiberbiztonsági képzés lehetősége Magyarországon. Megjelenés alatt. *Hadmérnök*, 2020.
[17] Deák (2020) i. m.

Kapcsolódó kutatási módszerek: dokumentumelemzés, megfigyelés, fókuszcsoport, interjú

A struktúra és a témakörök meghatározása során lehetőség van több kutatási módszert is használni. A nemzetközi és hazai publikáció elemzése jó támpontot adhat a kiinduláshoz, de fontosak a saját és mások tapasztalatain alapuló megközelítések is.

Kutatási módszerek alkalmazása

Meghatároztam egy elméleti és egy gyakorlati részből álló közszolgálati kiberbiztonsági képzés felépítését, struktúráját. A képzés formája szakirányú továbbképzés, és összesen 4 szemeszteren keresztül tart. Az első két félév tartalmazza az elméleti tudásátadást, ennek során a hallgatók elsajátítják az általános informatikai alapismereteket, a kiberbiztonsággal és adatvédelemmel kapcsolatos jogszabályokat, alapvető fogalmakat, az állami kibervédelmi rendszer felépítését, a szervezeten belüli kiberbiztonsági és adatvédelmi felelős pozíciókat, valamint megismerkednek a kibertámadások típusaival, támadási technikákkal, illetve az ezek megelőzésére és elhárítására irányuló módszerekkel. Ezen kívül elsajátítják a kockázatkezelési ismereteket, valamint az emberi tényező kiberbiztonságban betöltött szerepét. A képzés gyakorlati része során a konkrét támadások szimulálásával, a már meglévő tudásra alapozva, összekapcsolható az elméleti és a gyakorlati tudás. Ennek következtében a hallgatók képesek lesznek felismerni a kibertérből érkező fenyegetéseket és esetleges kockázatokat. A gyakorlati rész további két szakaszra osztható, amelyeket a harmadik és negyedik félévben tartják meg. Ezen kétlépcsős gyakorlati képzés során a hallgatók először a saját infokommunikációs eszközük védelmi mechanizmusaival ismerkednek meg, majd szimulált, szervezeti szintű környezetben a támadások elhárítását hajtják végre. Utóbbi fontossága és relevanciája abban rejlik, hogy a hallgatók képesek legyenek átlátni egy összehangolt támadást és annak részeit. Ezáltal olyan események is gyanússá válhatnak számukra a mindennapi munka során, amelyek önmagukban nem minden esetben jelentenek biztonsági kockázatot, de egy komplex összehangolt támadás részei lehetnek.

A képzés folyamatos fejlesztésének biztosítása

Az utolsó lépés rendkívül fontos minden képzés esetében, hiszen ennek segítségével biztosítható a képzés naprakészsége. Éppen ezért elengedhetetlen a képzés relevanciájának és tartalmának folyamatos monitorozása és felülvizsgálata, valamint a képzés szakterületével, tudományterületével kapcsolatos aktuális és új kutatási eredmények, álláspontok, kihívások nyomon követése. A kialakított képzést fel kell készíteni a módosításokra, fejlesztésekre, amelyhez olyan metrikákat, kiértékelési mechanizmusokat kell definiálni, amivel a képzés minősége mindenkor ellenőrizhető és kiértékelhető. Az eredmények alapján képesnek kell lenni megfogalmazni módosítási javaslatokat, hogy a képzés minőségét és színvonalát javítani lehessen.

Kapcsolódó kutatási módszerek: kérdőív, teszt, dokumentumelemzés

Az elkészült képzés indítására, fejlesztésére és minőségének biztosítására olyan kutatásmódszertani eszközöket lehet használni, mint a tesztelés, amelynek segítségével még a képzés indulása előtt egy kontrollcsoport segítségével kiértékelhetők a tematikák, oktatási stratégiák stb. A kérdőív pedig a már meglévő vagy a képzés indítása után indított kurzusokhoz lehet hasznos. Előbbi esetben segítséget nyújt, hogy egy kurzust milyen irányba kell alakítani, hogy alkalmas legyen a definiált képzéshez, míg utóbbi esetben már a képzés alkalmazása közben futó kurzusok fejlesztésére lehet következtetni a kérdőívek eredményeiből. Természetesen érdemes megnézni az akadémiai világot, hogy milyen megközelítések vannak az adott témakörben a képzések fejlesztésére, amelyeket érdemes lehet még átültetni és átalakítani.

Kutatási módszerek alkalmazása

A közszolgálati kiberbiztonsági képzés folyamatos fejlesztésének biztosítása érdekében kidolgoztam a tudásátadás hatékonyságának mérésére szolgáló módszert. Ennek keretében definiáltuk a hatékonyság fogalmát, amelyet úgy vizsgáltunk, hogy egy oktatott tantárgy esetében minden témakör oktatása előtt és után a hallgatók tesztet töltenek ki, ahol a hallgatóknak az adott témakörrel kapcsolatos kérdésekre kellett felelniük. A hatékonyságot *(h)* pedig úgy definiáltuk az egyes témakörök *(t)* esetén, hogy vettük az oktatás előtt *(e)* és után *(u)* mért összes válasz *(ö)* közül a helyes válaszok *(j)* százalékos arányának különbségét:

$$h_t[\%] = \left\{\frac{j_t^u}{\ddot{o}_t} - \frac{j_t^e}{\ddot{o}_t}\right\} \times 100$$

1. egyenlet: A hatékonyság képlete

Ennek segítségével megállapítható, hogy az egyes témakörök esetében hatékony volt-e a tudástranszfer. Emellett definiáltunk egy szempontrendszert, amely alapján osztályozható, hogy a témakörök során átadott tudás kellően részletes-e, továbbá a témák megfelelően kategorizálhatók és osztályozhatók voltak. A szempontrendszert alkalmazva következtetések vonhatók le az adott témakörre vonatkozóan, továbbá javaslatok fogalmazhatók meg, hogy például melyik témakört szükséges részletesebben oktatni, illetve melyet szükséges módosítani.

Következtetések

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

Az első hipotézis bizonyítására egy folyamatot definiáltam, amely részletezi, miképpen lehet egy képzést tudományos alapokon meghatározni. A második hipotézis bizonyítására pedig meghatároztam a folyamatokhoz kapcsolódó releváns kutatási módszereket. Az első és második hipotézis eredményeit szemlélteti a 4. ábra.

4. ábra: A tervezési lépések során alkalmazható kutatási eredmények
Forrás: a szerző szerkesztése

Ahogy az ábráról is leolvasható, a dokumentumelemzés mindegyik fázisban elengedhetetlen eszköz. Az is látható, hogy a képzés tervezésének korai szakaszában jelentős az interjú eszköze, ahol a szakma releváns személyei irányítják a képzés fókuszát. A képzés végén jelenik meg a lehetőség további módszerek alkalmazására, így a kérdőívek használatára, tesztelésre, megfigyelésre és a fókuszcsoportok használatára.

A bemutatott folyamat és kutatási módszerek csak a szükséges elemeket definiálják, amelyek egy képzés definiáláshoz 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.

Összefoglalás és jövőbeni tervek

Jelen publikációban egy folyamatot definiáltam oktatási képzések tudományos tervezéséhez. A cél, hogy olyan akadémiai kutatásoknak adjon kiindulási pontot, amelyek során tudományos alapokon kell egy megfelelő képzést megtervezni.

A definiált folyamat összesen 8 lépésből áll, amelyek a következők:

1. releváns szereplők meghallgatása;
2. célcsoport meghatározása;
3. az átadni kívánt képességek és készségek meghatározása;

4. hazai képzések vizsgálata;
5. nemzetközi képzések vizsgálata;
6. a képzés formális specifikálása;
7. a képzési struktúra és témakörök meghatározása;
8. a képzés folyamatos fejlesztésének biztosítása.

Minden lépéshez meghatároztam azokat a kutatási módszereket, amelyekkel biztosított, hogy a képzés minden eleme tudományosan bizonyított legyen. A kutatási módszerek közül alapvetően az interjú, a dokumentumelemzés, a megfigyelés, a kérdőív, a tesztelés és a fókuszcsoport technikákat alkalmaztam.

A bemutatott folyamatot és kapcsolódó kutatási módszereket szemléltetésképp a közszolgálati kiberbiztonsági képzés meghatározása során alkalmaztam, ahol egy nemzetközileg is elfogadható képzést kellett definiálni a közszolgálatban dolgozók számára.

A kutatás folytatásaként szükséges lenne a tárgyak tematikájának kialakításához kapcsolódó tudományos folyamat meghatározására, illetve az általános képzéseknél specifikusabb képzések részproblémáinak azonosítására (például doktori képzés, alapképzés, mesterképzés, szakirányú továbbképzés stb.).

Felhasznált irodalom

Babbie, Earl: *A társadalomtudományi kutatás gyakorlata*. Budapest, Balassi, 2008.

Beuran, Razvan et alii: Integrated framework for hands-on cybersecurity training: CyTrONE. *Computers & Security,* (2018), 78. 43–59. Online: 10.1016/j.cose.2018.06.001

Deák Veronika: A közszolgálati kiberbiztonsági képzés lehetősége Magyarországon. Megjelenés alatt. *Hadmérnök,* 2020.

Dupuis, Marc J.: Cyber security for everyone: An introductory course for non-technical majors. *Journal of Cybersecurity Education, Research and Practice,* (2017), 1.

Gőcze István: *Tudományelmélet és kutatásmódszertan alapjai*. Budapest, ZMNE, 2010.

Hornyacsek Júlia: *A tudományos kutatás elmélete és módszertana*. Budapest, NKE, 2014.

Morgan, Steve: Cybersecurity Jobs Report: A special report from the editors at Cybersecurity Ventures. *Cybercrime Magazine,* 2017. Online: https://cybersecurityventures.com/jobs/

Newhouse, William D. et alii: *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce.* NIST Special Publication 800-181, 2017. Online: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=923472

Pratt, Shaaron – Adams, Caroline: How to create a degree course in radiography: a recipe. *Radiography,* 9. (2003), 4. 317–322.

Sabillón, Régner – Ruiz-Serra, Jordi – Cavaller, Victor – Martinez, Jeimy Jose Cano: An effective cybersecurity training model to support an organizational awareness program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada. *Journal of Cases on Information Technology,* 21. (2019), 3. 26–39. Online: 10.4018/JCIT.2019070102

Toth, Patricia – Klein, Penny: *A role-based model for federal information technology/cyber security training.* NIST special publication, 800-16. 2014. 1–152. Online: https://csrc.nist.gov/csrc/media/publications/sp/800-16/rev-1/draft/documents/sp800_16_rev1_3rd-draft.pdf

Wang, Ping – Kohun, Fred: Designing a doctoral level cybersecurity course. *Issues in Information Systems,* 20. (2018), 1. 88–99. Online: https://doi.org/10.48009/1_iis_2019_88-99

Williams, Carrie: Research methods. *Journal of Business & Economics Research,* 5. (2007), 3. Online: https://doi.org/10.19030/jber.v5i3.2532

A Katonai Műszaki Doktori Iskolában folyó képzés és kutatás a műszaki tudományterülethez tartozó tudományágaknak a teljes védelmi szektorban történő alkalmazására irányul. A hallgatók tudományos tevékenységüket gyakran több tudományterület és tudományág határterületén művelik, és a kutatásaik során azok interdiszciplináris kérdéseire, szinergiáira fókuszálnak.

Mindezt az ebben a kötetben található írások is igazolják. A szerzők olyan tudományos problémákat feszegetnek, mint például a blokkláncok és a mesterséges intelligencia alkalmazhatósága a kiberhadviselésben, a Mi–24 helikopterek elektronikai hadviselési képességeinek fejlesztése vagy az állami célú adatátviteli rendszerek integrálhatóságának kérdései. A környezetbiztonság és a vízgazdálkodás, valamint a vízbiztonság területéhez köthetően is több írással találkozhatunk a kötetben.