HADMÉRNÖK
VÉDELEMINFORMATIKA

16. évfolyam (2021) 4. szám 113–132.
DOI: 10.32567/hm.2021.4.9

Krasznay Csaba,[1] Deák Veronika[2]

Adatbiztonsági informatikai alapismeretek átadásának vizsgálata egy szakirányú továbbképzés keretében

Evaluating the Basic Knowledge Transfer of Data Security in a Postgraduate Specialist Training Course

A közszolgálati kiberbiztonság fejlesztését célzó felsőoktatási képzés során elengedhetetlen az informatikai alapismeretek átadása a hallgatók számára.

Az ilyen típusú képzésekre jelentkező hallgatók jelentős része nem képzett informatikus, így esetükben nem feltételezhető a mélyebb műszaki, technikai, informatikai alapismeretek megléte. Egy ilyen típusú képzés kialakítása során figyelni kell arra, hogy a hallgatóság megértse és képes legyen feldolgozni, elsajátítani az átadott ismereteket.

Jelen tanulmány az informatikai alapismeretek átadásához egy már meglévő tantárgy tematikáját, az általa átadott ismeretanyag hatékonyságát, helyességét, az esetleges hiányosságait vizsgálja, és javaslatot fogalmaz meg, hogyan lehet azt a közszolgálati kiberbiztonsági képzésbe beilleszteni.

Kulcsszavak: **közszolgálat, kiberbiztonság, képzés, informatika, alapismeretek, készségek, képességek, tudásátadás, hatékonyság**

In case of a training programme which aims to improve cyber security in the public service it is required to transfer basic knowledge of information technologies to the attendees.

[1] Nemzeti Közszolgálati Egyetem Eötvös József Kutatóközpont Kiberbiztonsági Kutatóintézet, intézetvezető, egyetemi docens, e-mail: krasznay.csaba@uni-nke.hu

[2] Nemzeti Közszolgálati Egyetem adatvédelmi tisztviselő; Katonai Műszaki Doktori Iskola, doktori hallgató, e-mail: deak.veronika@uni-nke.hu

Generally, only a small part of the attendees on such training programmes are qualified computer science experts. Hence, we can assume that the rest of the students lack a deeper engineering and technical knowledge on this field. However, it is a challenging task to educate such students in a way they can understand and use the transferred knowledge.

In this paper, we evaluate the results of an existing course in the field of information technologies that can be a basis for a similar course in the cybersecurity training programme for public service. We investigate the effectiveness, correctness and insufficiency of the knowledge transfer. Finally, we propose improvements and changes to be able to integrate such courses into a cybersecurity training programme for public service.

Keywords: **public service, cybersecurity, training programme, computer science, skills, knowledge transfer, effectiveness**

1. Bevezetés

A közszolgálati kiberbiztonság fejlesztését célzó képzés során elengedhetetlen az informatikai alapismeretek átadása a hallgatók számára. Az elmúlt évek eseményei azt mutatják, hogy a közszolgálat a kibertámadások kedvező célpontjaként értelmezhető, így különösen nagy hangsúlyt kell fektetni a lehetséges támadási alternatívák megismerésére és alkalmazhatóságára a hatékony védelem kialakítása érdekében.

A közszolgálati kiberbiztonság kialakításához és folyamatos fejlesztéséhez elengedhetetlen a közszolgálatban dolgozó személyek kibervédelmi ismereteinek bővítése. Ezt célozza a közszolgálati kiberbiztonsági képzés,[3] amelynek megalkotása tudományos módszerek alapján történik. Ennek egyik fő feladata a képzéshez szükséges főbb alapismeretek feltérképezése és hatékony tudástranszfer bizonyítása.

A jelenlegi IT-szektorban jelentkező szakemberhiány indokolttá teszi a közszolgálat képzési programjának kidolgozását a kiberbiztonság fejlesztése érdekében. A közszolgálati kiberbiztonsági képzés alapvetően azoknak a közszolgálatban dolgozó, nem informatikai végzettségű személyeknek szól, akik nem rendelkeznek a szükséges kibervédelmi alapismeretekkel, nem mozognak a témában otthonosan, a cél, hogy megfelelő felkészítést kapjanak a hatékony és eredményes védelem kialakítása, a különféle kiberfenyegetések megelőzése, illetve a már bekövetkezett események elhárítása érdekében.

A kibervédelmi képesség kialakításához szükséges készségek, képességek meghatározásának részét képezi azon informatikai alapismeretek azonosítása, amelyek nélkülözhetetlenek a hatékony közszolgálati kiberbiztonság elérése érdekében. Az informatikai alapismeretek meghatározása egy, már folyamatban lévő, rokon területen megvalósított képzés keretében oktatott tantárgy hatékonyságának elemzésével

[3] Jelen tanulmánynak nem célja a közszolgálati kiberbiztonsági képzés részletes bemutatása.

történik, amelynek tematikája esetlegesen felhasználható a közszolgálati kiberbiztonsági képzéshez.

Ennek igazolására az alábbi hipotéziseket állítottuk fel:

H1. A tantárgy keretein belül hatékony volt a tudástranszfer.

H2. A tantárgy tematikája megfelelően fedi a szükséges informatikai alapismereteket.

H3. Definiálható egy szempontrendszer, amely alapján osztályozható, hogy a témakörök során átadott tudás kellően részletes-e.

H4. A tantárgy felhasználható a kiberbiztonsági képzés során.

1.1. Kutatási módszertan

A fentebb említett hipotézisek megválaszolására az alábbi módszereket használtuk fel.

A H1 hipotézis esetén minden témakör oktatása előtt és után a hallgatók tesztet töltöttek ki. A hatékonyságot pedig úgy definiáltuk az egyes témakörök esetén, hogy vettük az oktatás előtt és után mért helyes válaszok százalékos arányának különbségét:

$$hatékonyság_{témakör}[\%] = \left\{\frac{helyes\ válaszok_{témakör}^{oktatás\ után}}{összes\ teszt\ kérdés_{témakör}} - \frac{helyes\ válaszok_{témakör}^{oktatás\ előtt}}{összes\ teszt\ kérdés_{témakör}}\right\} \times 100 \quad (1)$$

A H2 hipotézis esetén azt vizsgáltuk, hogy az oktatott ismeretanyag elegendő-e a *NICE Cybersecurity Workforce Framework*[4]-ben meghatározott képességek elsajátítására és a *Certified Information Systems Security Professional* (CISSP) képesítés[5] megszerzésére. A NICE Frameworköt és a CISSP-képesítés tartalmát a 2. pontban részletesen kifejtjük.

A H3 hipotézis során olyan szempontrendszert kell definiálni, amely a H1-ben meghatározott hatékonyság alapján osztályozni tudja az egyes témaköröket az alábbiak tekintetében:

- mélyebb tudás átadása szükséges,
- a témakör kellően részletes,
- a témakör egyszerűsítése szükséges.

A H4 hipotézis igazolására a H1, H2 és H3 hipotézisek eredményét vesszük alapul. Amennyiben a vizsgált tantárgy felhasználható, bemutatjuk, hogy milyen változtatások szükségesek a közszolgálati kiberbiztonsági képzésbe történő integrálásához.

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

[5] A *Certified Information Systems Security Professional* (CISSP, más néven minősített információs rendszer biztonsági szakember) képzése az informatikai rendszerek technikai kérdéseinek biztonsági vonatkozásairól szól. Bővebb információ a következő weboldalon található: www.isc2.org/Certifications/CISSP#

1.2. Struktúra

A második pontban bemutatjuk az előbbiekben említett NICE Framework és CISSP tartalmát, elemeit és a képzéshez fűződő kapcsolatát, valamint a kapcsolódó munkákat. A harmadik pontban a mérések körülményeit és az alkalmazott módszertant fejtjük ki. A negyedik pont tartalmazza a mérések eredményeinek általános és egyes témakörök szerinti áttekintését, valamint kiértékelését. Az ötödik pontban a témakörök osztályozását, az általunk definiált szempontrendszert, majd a hatodik pontban az eredmények alapján levonható következtetéseket ismertetjük, amelyet az utolsó pontban az összegzés, a jövőbeni tervek, a mérések lehetséges folytatása követ.

1.3. Előzetes következtetések

Meggyőződésünk, ha a bemutatott hipotéziseket megfelelően alá tudjuk támasztani, akkor az megfelelő alapot biztosíthat a közszolgálati kiberbiztonsági képzés és más képzések fejlesztéséhez kapcsolódóan.

2. Kapcsolódó munkák

Ahhoz, hogy a jelen tanulmányban ismertetett tudástranszfer hatékonyságmérés minden részletre kiterjedő értékelése megvalósulhasson, nélkülözhetetlen a releváns hazai és nemzetközi szakirodalom mélyebb vizsgálata. A jelen mérés alapjául szolgáló célcsoport részére átadott tudás alapját képező képességek, készségek halmazát a hasonló képzések követelményeinek vizsgálatával határoztuk meg.

2.1. Hazai közigazgatásban végzett kutatások

Elsősorban olyan tanulmányokat elemzünk, amelyekben hasonló kutatást végeztek el, illetve a kiberbiztonsági képzésfejlesztés, a kiberbiztonsági és kibervédelmi képességek fejlesztését vizsgálják. Az irodalomkutatás során feltárt tanulmányok közül mindenképp ki kell emelni az Illésy Miklós, Nemeslaki András, Som Zoltán által elkészített *Elektronikus információbiztonság-tudatosság a magyar közigazgatásban* című publikációt. A szerzők a magyar közigazgatás információbiztonsággal kapcsolatos tudatosságát térképezték fel egy szakértői interjúsorozattal, illetve egy köztisztviselői kérdőíves megkérdezéssel, amelyet leíró statisztikai módszerekkel elemeztek.[6]

A tanulmányban részletezett interjúk megerősítették, hogy a rohamos technológiai fejlődéshez történő alkalmazkodást nagymértékben befolyásolhatja az információbiztonsággal kapcsolatos humánerőforrás-fejlesztés információbiztonsági vezetői és alkalmazotti szinteken egyaránt. A szerzők által elvégzett kérdőív kimutatta azokat

[6] Illésy Miklós – Nemeslaki András – Som Zoltán: Elektronikus információbiztonság-tudatosság a magyar közigazgatásban. *Információs Társadalom,* 14. (2014), 1. 52–73.

a területeket, amelyek alapján láthatóvá váltak az ellentmondások az információbiztonság-tudatosság megítélésében. A tanulmány tapasztalatai azt mutatják, hogy elengedhetetlen az információbiztonság-tudatosság folyamatos fejlesztése a kibertérből érkező fenyegetések megakadályozása, elhárítása érdekében.[7]

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.[8]

2.2. National Initiative for Cybersecurity Education (NICE) Framework

A hatékony és eredményes tudásátadás eléréséhez nem csak a hasonló méréseket szükséges vizsgálni, nélkülözhetetlen azon képességek, készségek meghatározása, amelyeket át szeretnénk adni a célcsoport számára. E halmaz megállapításához a korábbiakban említett National Initiative for Cybersecurity Education (NICE) Frameworkben részletezett ismereteket vettük alapul. A NICE Keretrendszer meghatározza az elsajátítandó kiberbiztonsági tudást, készségeket, képességeket és feladatokat az egyes kiberbiztonsággal kapcsolatos munkakörökhöz.[9] Ez a keretrendszer kiváló alapként szolgálhat az általunk átadni kívánt tudás, készségek, képességek meghatározására, a kiberbiztonsági tantervek, tantárgyi adatlapok kidolgozására.

A NICE kapcsán szükséges megemlíteni az ENISA[10] Európai Kiberbiztonsági Képességek Keretrendszerét,[11] amely definiálására és kidolgozására külön munkacsoportot hoztak létre 2020-ban. A keretrendszer célja a NICE Keretrendszerhez hasonlóan a kiberbiztonsággal összefüggő munkakörök és azok teljesítéséhez szükséges készségek, képességek azonosítása, amely szorosan igazodik az Európai Unió tagállamainak sajátosságaihoz, igényeihez.

2.3. A NICE Framework szerepe a nemzetközi oktatásban

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

[7] Illésy (2014): i. m.

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

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

[10] *European Union Agency for Cybersecurity* (ENISA) – Európai Uniós Kiberbiztonsági Ügynökség.

[11] *European Cybersecurity Skills Framework* (bővebb információ a következő linken elérhető: www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework).

Alsmadi tanulmánya rámutat a jelenlegi kiberbiztonsági munkaerőhiány jelenségére, valamint kiemeli a NICE és az ehhez hasonló keretrendszerek alkalmazásának szerepét, továbbá azonosítja azon tényezőket, amelyek bizonyítják ezek szükségességét.[12] Armstrong és szerzőtársai szintén hangsúlyozzák a növekvő kiberbiztonsági munkaerőhiányt, ezáltal pedig a kiberbiztonsági munkaerő iránti kereslet és versengés megjelenését.[13]

Dodge és szerzőtársai kifejtik, hogy a kiberbiztonsági munkaerő fejlesztése elengedhetetlen, az ezek során felmerülő problémák, kihívások nem csak bizonyos országokban jelentkeznek, így figyelembe kell venni a globális hatásokat, következményeket.[14]

Andrew McGettrick rámutat, hogy már 2013-ban is egyértelmű volt, hogy a kiberbiztonsági oktatás több területet érint, mint például az akadémia, közigazgatás, egészségügy és a magánszféra. Ezért a hallgatókat motiválni kell annak érdekében, hogy felkeltsék az érdeklődésüket a kiberbiztonság iránt.[15]

Estes és szerzőtársai tanulmányukban feltárják, hogy a NICE kiberbiztonsági munkaerőrendszere hogyan igazítja és hangolja össze a kiberbiztonági munkákat a potenciális jelöltekkel. A keretrendszer segítséget nyújt a szervezeti kiberbiztonsági igények, illetve a személyes karriercélok és ezek eléréséhez szükséges eszközök meghatározásához is.[16]

Scheponik és szerzőtársai arra keresik a választ, hogyan értelmezik a hallgatók a kiberbiztonság egyes fogalmait, illetve hogy a kiválasztott egyetemeken tanuló hallgatók milyen kiberbiztonsági ismeretekkel rendelkeznek. A tanulmány célja interjúk elkészítésével a hallgatók tudásának mérése, a hiányosságok feltárása, azok okainak azonosítása, valamint hosszú távon az oktatás fejlesztése.[17]

Bicak és szerzőtársai kifejtik, hogyan változott meg a kiberbiztonsági képzések tanterve. Ennek keretében rövid áttekintést adnak a NICE Keretrendszerről és egyéb, például információbiztonsággal kapcsolatos programokról, illetve ezek követelményeiről. Ezt követően bemutatják, milyen változások figyelhetők meg a kiberbiztonsági oktatásban a tantervek tekintetében.[18]

Összegezve megállapítható, hogy a NICE Keretrendszeren alapuló egyetemi oktatás megfelelő szaktudást biztosít a kiberbiztonság témakörében. Azonban az is

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

[13] Miriam E. Armstrong – 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.

[14] Ronald C Dodge – Costis Toregas – Lance Hoffman: Cybersecurity Workforce Development Directions. *HAISA,* (2012), 1–13.

[15] Andrew McGettrick: Toward Effective Cybersecurity Education. *IEEE Security & Privacy,* 11. (2013), 6. 66–68.

[16] Adriane C. Estes – Dan J. Kim – T. Andrew Yang: Exploring How the NICE Cybersecurity Workforce Framework Aligns Cybersecurity Jobs with Potential Candidates. In *Proceedings of the 2018 International Conference on Frontiers in Education: Computer Science & Computer Engineering.* Las Vegas, Nevada, CSREA Press 2018. 1–7.

[17] Travis Scheponik et al.: How Students Reason about Cybersecurity Concepts. In *IEEE Frontiers in Education Conference* (FIE). 2016. 1–5.

[18] Ali Bicak – Michelle (Xiang) Liu – Diane Murphy: Cybersecurity Curriculum Development: Introducing Specialties in a Graduate Program. *Information Systems Education Journal,* 13. (2015), 3. 99–110.

látható, hogy a keretrendszer hatékony integrálása az egyetemi oktatásba nagyban függ a hallgatók kezdeti tudásának mértékétől.

2.4. Certified Information Systems Security Professional (CISSP) vizsga

A CISSP egy nemzetközi tanúsítvány az információbiztonság területén. A tanúsítvánnyal rendelkező információbiztonsági szakemberek képesek megérteni és alkalmazni a kiberbiztonsági stratégiákat, illetve kellően részletes szaktudással és gyakorlati ismeretekkel rendelkeznek, hogy képesek legyenek megtervezni és vezetni egy szervezeti egység teljes biztonsági struktúráját. A képzés nyolc fő témából áll, amelyeket minden jelöltnek el kell sajátítania.[19] Ezek az alábbiak:

- biztonsági kockázatok és kockázatkezelés;
- vagyon- és eszközbiztonság;
- biztonsági architektúra és tervezés;
- kommunikáció és hálózati biztonság;
- identitás és hozzáférés-kezelés;
- biztonsági értékelés és tesztelés;
- biztonsági műveletek;
- szoftverfejlesztési biztonság.

A CISSP-képesítés megszerzéséhez számos követelmény teljesítése szükséges. A jelölteknek legalább ötéves szakmai tapasztalattal kell rendelkezniük a fentebb említett témakörökből minimum kettő vagy több témát érintően. Amennyiben a jelölt négyéves főiskolai végzettséggel vagy azzal egyenértékű regionális tanúsítvánnyal, illetve kiegészítő tanúsítvánnyal rendelkezik az ISC által jóváhagyott listáról, akkor azt egyéves munkatapasztalatként ismerik el. A vizsgával kapcsolatos főbb információk az alábbi táblázatban láthatók:

1. táblázat
CISSP-vizsga adatai
Forrás: (ISC)² (2018): i. m.

A vizsga időtartama	3 óra
Kérdések száma	10–150
Kérdések formátuma	Feleletválasztós és kifejtős
Minimum pontszám	700 (1000-ből)
Vizsga nyelve	Angol
Vizsgaközpont	ISC által engedélyezett vizsgaközpontok

[19] (ISC)²: Certification Exam Outline (2018. április).

2.5. Pedagógiai értékelések

Több hazai egyetemen is megtalálható az oktatók értékelési rendszere, ezáltal megvalósíthatóvá válik az oktatók minőségellenőrzése, többek között a Nemzeti Közszolgálati Egyetemen, a Budapesti Műszaki Egyetemen, valamint az Óbudai Egyetemen. Nemzetközi szinten is gyakran alkalmazzák ezen értékelési módszereket. Samian és Noor is bemutatnak cikkükben egy ilyen hallgatói benyomásokon alapuló értékelési rendszert. A visszacsatolást minden félévben elvégezik az egyetem összes kurzusán. A hallgatóknak a félév végén több hét áll rendelkezésükre, hogy az általuk elvégzett kurzusokat és azok előadóit értékeljék. Ezt követi a kiértékelés, valamint a felsővezetés és az oktatók általi megismerés.[20]

Kumaladewi és Sugiarti tanulmányukban bemutatott módszer segítségével a hallgatók visszajelzésén keresztül megkapott adatok alapján nemcsak egyszerű méréseket képesek végrehajtani, hanem stratégiai döntéseket és előrejelzéseket is.[21]

Falusi Iván és társai definiálják a tantervi vagy programértékelést mint kutatási módszert, aminek célja, hogy egy adott tanterv, taneszközegyüttes stb. hatékonyságát a saját maga elé tűzött célok elérése szempontjából értékelje.[22]

Összegezve kijelenthető, hogy a pedagógiai-statisztikai szakirodalom elsősorban statikus ellenőrzéseket használ a tantervek és programok fejlesztésére (például a követelmények teljesülnek-e), illetve az oktatók teljesítményértékelése határozza meg a tudásátadás minőségét a hallgatók szubjektív benyomásai, érzései alapján. Kijelenthető, hogy olyan módszertant a szakirodalom ezidáig nem definiált, amely a tudásátadás hatékonyságát objektív módon mérné és biztosítaná egy tantárgy fejlesztésének lehetőségét.

3. A NICE, a CISSP és az oktatási anyag kapcsolata

Az oktatási anyag kidolgozása során a NICE Framework keretrendszer kiberbiztonsági pozíciói közül az adatvédelmi tisztviselő munkakört választottuk ki, amely tartalmazza mindazon tudást, képességeket és készségeket, ami a leginkább illeszkedik a célcsoport előképzettségéhez, a tantárgy kimeneti követelményeihez, valamint az általuk megszerezhető szakképzettséghez. Ezt követően megvizsgáltuk a keretrendszer által előírt tudás, feladat, képesség és készség halmazát, és kiválasztottuk azokat, amelyek az általunk átadni kívánt tudás és a tantárgy kimeneti követelményei szempontjából relevánsak.

Ezek alapján az alábbi, 2. táblázat tartalmazza e feladatokat, tudást, képességeket és készségeket:

[20] Yahya Samian – Norah Md Noor Student's Perception on Good Lecturer based on Lecturer Performance Assessment. *Procedia-Social and Behavioral Sciences,* 56. (2012), 8. 783–790.

[21] Nia Kumaladewi – Yuni Sugiarti: Design Analysis of Data Warehouse for Lecturer Performance Evaluation (Case study: Faculty of science and technology UIN Jakarta). In 4*th* International Conference on Cyber and IT Service Management. 2016. 1–6.

[22] Falus Iván (szerk.): *Bevezetés a pedagógiai kutatás módszereibe.* Budapest, Keraban, 1996.

2. táblázat

Az átadni kívánt tudás és a vizsgált tantárgy kimeneti követelményei szempontjából releváns elvárások
Forrás: a szerző szerkesztése a NICE Keretrendszer alapján

Tudás
• számítógép-hálózatokhoz kapcsolódó alapfogalmak ismerete • kockázatkezelési folyamatok ismerete • kiberbiztonsági, adatvédelmi alapelvek ismerete • az alkalmazandó üzleti folyamatok működésének ismerete • kibertérből érkező fenyegetések ismerete • vezeték nélküli technológiák ismerete
Feladat
• tanácsadás a felsővezetésnek a kockázatértékelési folyamatról, kockázati szintekről, az információbiztonsági programokról, rendszerekről, irányelvekről, folyamatokról és eljárási szabályokról • üzletmenet-folytonossági tervek elkészítése, tesztek elvégzése • belső audit végrehajtása, auditjelentések elkészítése • közvetítés a műszaki és nem műszaki szakemberek között • adatbiztonsági követelmények megvalósulásának biztosítása • együttműködés az informatikai, információbiztonsági politikák és eljárások területén • közreműködés az információs infrastruktúra kialakításában, fejlesztésében • incidenskezelési folyamat kialakítása, incidensek kezelése • figyelemmel kíséri a szervezet folyamatait, az infokommunikációs rendszerek fejlesztését, működését a biztonsági és az adatvédelmi szabályok betartásának ellenőrzése céljából • adatvédelmi események, incidensek, jogsértések kezelése, dokumentálása, intézkedési terv készítése és megvalósítása
Képesség
• egyértelmű, világos, átlátható stratégia, iránymutatások, szabályok, eljárások, folyamatok és képzési anyagok, dokumentációk kidolgozásának képessége • szabványos működési eljárások, folyamatok kidolgozásának és folyamatos fejlesztésének képessége • a releváns adatvédelmi, kiberbiztonsági jogszabályok, technológiák változásának nyomon követésének képessége
Készség
• adatvédelmi szabályok, irányelvek készítésének készsége • adatvédelmi eljárások, folyamatok, gyakorlatok kialakításának készsége • különböző szintű kommunikációs készség a szervezet különböző területeinek megfelelően

A NICE Keretrendszerből kiválasztott tudás-, képesség-, készséghalmazt az általunk szükségesnek ítélt további elvárásokkal kiegészítve összeállítottuk azon elvárásokat, amelyek jelen tanulmányban vizsgált tantárgy szempontjától relevánsak, és ez alapján készítettük el a vizsgált félév tananyagát. Mindezt annak fényében, hogy a félév végi vizsgán a hallgatók meg tudnak-e olyan tipikus vizsgakérdéseket oldani, amelyek a CISSP-képesítés mintafeladatai között szerepelnek.

A CISSP-képesítésre több okból esett a választás. Először is, nevesítve szerepel a magyarországi információbiztonsági jogszabály oktatással kapcsolatos végrehajtási rendeletében. A 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének

és továbbképzésének tartalmáról 7. § (2) szerint: „Az Ibtv. 13. § (10) bekezdése alapján nem kell a 4. § (1) bekezdése szerinti végzettséget megszereznie annak a személynek, aki rendelkezik: […] *b)* az International Information Systems Security Certification Consortium Inc. által kiadott Certified Information Systems Security Professional (CISSP) érvényes oklevéllel." Másrészt az irodalomkutatás alapján a CISSP-vizsga tudásanyaga jól illeszkedik a NICE Keretrendszer elvárásaihoz.

Összegezve, a releváns szakirodalom és a kapcsolódó munkák mélyebb vizsgálata elengedhetetlen az átadni kívánt tudás meghatározásához, ennek következtében pedig a tudástranszfer méréséhez egyaránt, hiszen a hazai és nemzetközi oktatásban megjelenő kiberbiztonsággal kapcsolatos képzések, képességfejlesztést célzó tréningek elemzésével feltárhatók azok tapasztalatai, valamint azon „jó gyakorlatok", amelyek a hazai kiberbiztonsági oktatásba történő átültetésével jelentősen növelhető azok hatékonysága és eredményessége.

4. Mérési körülmények, módszertan

Jelen fejezetben szeretnénk prezentálni a mérésekhez kapcsolódó körülményeket, a mérés lefolytatásának jellemzőit, illetve módszertanát. A fejezet végén bemutatjuk a mérési eredményeket befolyásoló tényezőket is.

4.1. A tárgy jellegzetességei

A tantárgy során az adatvédelem és az adatbiztonság által meghatározott követelmények informatikai leképeződését kell elsajátítania a hallgatóknak. Itt kifejtik a következőket:

- számítógépes, hálózati és internetes biztonság;
- a védelem szintjei – fizikai védelem;
- a védelem szintjei – informatikai védelem;
- a biztonsági protokoll, a tűzfal és a biztonsági támadások;
- rendszergazdai irányelvek.

Ezenkívül a tantárgy segít megismertetni a hallgatókkal a kibertérből érkező fenyegetéseket és az információs társadalom új típusú kihívásait, valamint bemutatja az adatbiztonság összetevőit, a védelem lehetséges eszközeit, módszereit.

Jelen tantárgyat az Eötvös Lóránd Tudományegyetem Állam- és Jogtudományi Kar által szervezett Adatbiztonság és adatvédelmi szakjogász képzés második félévében tartották meg 6 kredit értékben,[23] kizárólag előadások formájában, gyakorlati oktatásra nem került sor. A tárgy teljesítése kollokvium keretében, tesztfeladatok megoldásával történik a félév végén. A mérést a 2018/19-es tanév tavaszi szemeszterében végeztük.

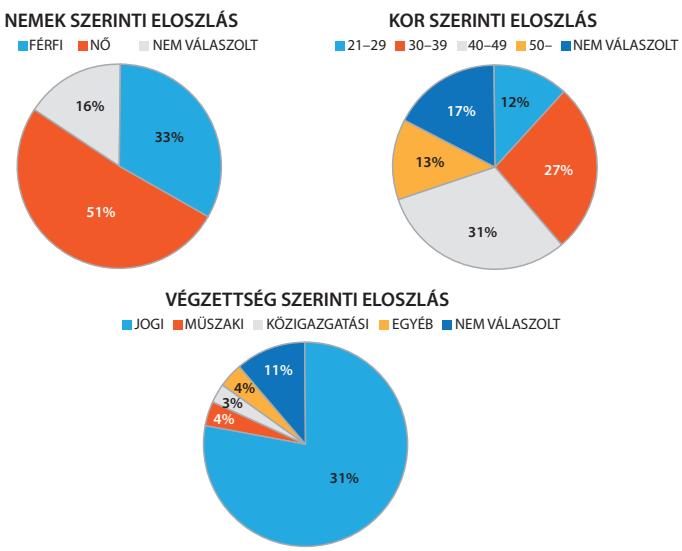
[23] A jelenlegi felsőoktatási rendszerben a kredit a tanulmányok elvégzése során alkalmazott mérőeszköz, amely a tantárgy súlyozására és típusának meghatározására szolgál.

4.2. A mérés körülményei

Az első előadás során egy átlagos információbiztonság-tudatosság mérésére szolgáló tesztet töltettünk ki a hallgatókkal. Ennek célja, hogy felmérjük a hallgatók általános biztonságtudatosságának szintjét, valamint a statisztikai kérdéseknek köszönhetően számos további következtetést határozzunk meg az egyes témakörök esetében. Ezt követően minden témakör oktatása előtt és után egy, a témára vonatkozó tesztet töltöttek ki. Témakörönként különböző kérdések, de a témakörök előtt és után azonos kérdéseket válaszoltak meg a hallgatók. A témakörökhöz kapcsolódó kérdések minden esetben szorosan illeszkedtek az előadáson elhangzott tananyaghoz. Tesztenként öt feleletválasztós kérdésre kellett válaszolniuk a hallgatóknak négy lehetséges opcióból a Kahoot alkalmazáson[24] keresztül. Ezek a kérdések a félév végén bekerültek a vizsgakérdések közé is, amelyet az egyetem Moodle rendszerén keresztül töltöttek ki.

4.3. A hallgatóság összetétele

A hallgatóság összetételét az első, általános információbiztonság-tudatosság mérésére szolgáló teszt alapján vizsgáltuk nem, kor és végzettség szerint, amelyek eloszlását az 1. ábra szemlélteti. A teszt kitöltése előtt a hallgatók beleegyezését kértük azzal kapcsolatban, hogy a félév során összegyűjtött adatokat anonim módon a kutatásban felhasználhassuk, ezzel teljesítve az adatvédelmi követelményeket.



1. ábra

A hallgatóság összetétele nem, kor, végzettség szerint

Forrás: a szerző szerkesztése

[24] A Kahoot kvízalapú oktatási platform, amely lehetővé teszi a hallgatók ismereteinek áttekintését, értékelését feleletválasztós kvíztesztek segítségével. Bővebb információ elérhető a következő weboldalon: https://kahoot.com/

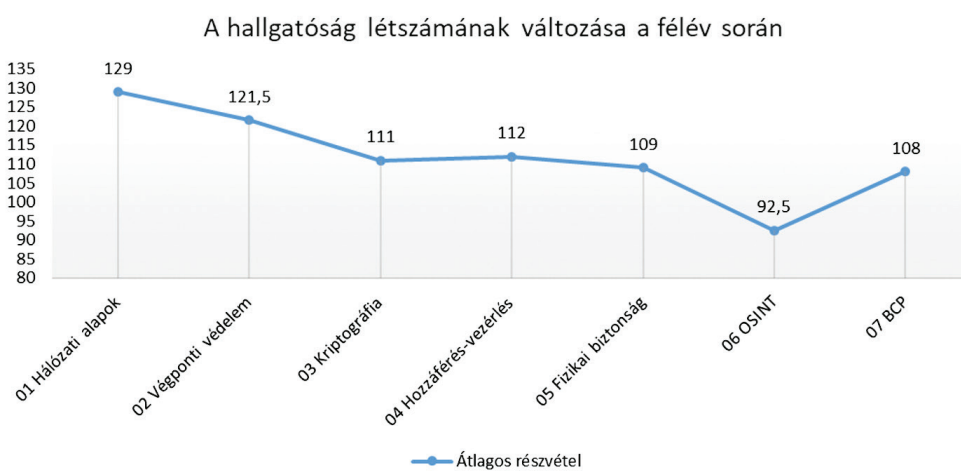
Összesen 130 hallgató töltötte ki a tesztet, 51%-uk nő (66 fő) és 33%-uk férfi (43 fő), a maradék 16% (21 fő) erre a kérdésre nem válaszolt. A nemek szerinti eloszlás alapján megállapítható, hogy a hallgatók többsége nő.

A kor szerinti eloszlás vizsgálatára négy életkori kategóriát állapítottunk meg. A hallgatók 12%-a (16 fő) 21–29 év közötti, 27%-a (35 fő) 30–39 év közötti, 31%-a (40 fő) 40–49 év közötti, 13%-a (17 fő) 50 éves vagy annál idősebb. Az életkorra vonatkozó kérdésre a hallgatók 17%-a, összesen 22 fő nem válaszolt. A kor szerinti eloszlás alapján a kérdésre válaszoló hallgatók többsége a 40–49 év közötti kategóriába tartozik.

A hallgatók végzettségének megállapítására szintén négy kategóriát határoztunk meg. A hallgatók 72%-a (102 fő) jogi, 4%-a (5 fő) műszaki, 3%-a (4 fő) közigazgatási és 4%-a (5 fő) valamilyen egyéb területen szerzett végzettséget. Erre a kérdésre a hallgatók 11%-a (14 fő) nem válaszolt. Ezek alapján megállapítható, hogy a hallgatók túlnyomó többsége jogi végzettséggel rendelkezik, de más előképzettséggel rendelkező hallgatók is részt vettek a képzésen.

4.4. A hallgatóság létszámának változása

A mérés eredményeinek érvényességét befolyásolta a tesztet kitöltő hallgatók létszáma az adott témakör előadásán. A 2. ábra a hallgatók létszámváltozását szemlélteti a félév során. Ezek alapján megállapítható, hogy kis mértékben, de folyamatosan csökkent a létszám. A hallgatói létszámcsökkenés számos okkal magyarázható, köszönhető többek között a féléves terhelésnek, a házi feladatok és zárthelyi dolgozatok gyakoriságának.



2. ábra

A hallgatóság létszámának változása a félév során

Forrás: a szerző szerkesztése

4.5. A kutatást befolyásoló tényezők

Jelen pontban szükséges megemlíteni a kutatás eredményét befolyásoló egyéb tényezőket. A kutatás során számos olyan tényező befolyásolta a kutatás lefolytatását és annak eredményét, amelyet mindenképp szükséges figyelembe venni a kutatás értékelésekor, a hipotézisek megválaszolásakor, illetve a következtetések megfogalmazásakor. Ezek alapján felmerülhet a kérdés, hogy milyen tényezők befolyásolhatták az eredményeket?

Az első ilyen tényező, hogy jelen kutatásban kizárólag egy évfolyamot vizsgáltunk, mivel korábbi évek statisztikái nem állnak rendelkezésre. Így csak ezen évfolyam tekintetében tudunk következtetéseket megfogalmazni. Jelen kutatásban ellenpéldát egyelőre még nem elemeztünk. Ennek következtében további megválaszolandó kérdések merülnek fel, például milyen eredmények születnének abban az esetben, ha nagyobb mennyiségű, illetve részletesebb ismeretanyagot adnának át a hallgatók számára.

Ezenkívül az eredmények kiértékelését nehezítette, valamint az elemezhető hallgatói eredmények számát csökkentette az a tény, hogy voltak olyan hallgatók, akik vagy az óra elején nem voltak még jelen, vagy pedig korábban távoztak az előadásról.

Továbbá meg kell még említeni mint befolyásoló, illetve nehezítő körülményt, hogy a negyedik hipotézisben említett kiberbiztonsági képzés esetén csak feltételezéssel élünk a hallgatók előképzettségének aránya tekintetében, illetve nem tudhatjuk, hogy az adott ismeretanyagot milyen mértékben képesek elsajátítani az egyes területekről érkező személyek, még hogyha a tudásuk azonos szinten is van az adott témában.

Ezek mellett érdemes megvizsgálni a továbblépési lehetőségeket is, a tananyag hosszú távú beépülésével kapcsolatban. Ezt a félévi vizsga útján lehet megtenni. A vizsgált szemeszterben a vizsgáztatás során lehetővé tettük, hogy a hallgatók egy 24 órás időintervallumban megnyithassanak egy Moodle-alapú tesztfelületet és ott egy előre megkonstruált kérdéssort tölthessenek ki. Ez 20 kérdésből állt, és összesen 30 perc állt rendelkezésre a kitöltéshez. A számonkérés megkönnyítése érdekében a teszt mindenkinek ugyanaz volt, de a feleletválasztós tesztek és ezeken belül a lehetséges megoldások véletlenszerűen keverve jelentek meg. A kérdések a CISSP-vizsga mintakérdései közül kerültek ki. Összesen 218 kitöltés született, átlagosan a 93,58%-os végső eredménnyel. A magas sikerrátában szerepe van annak, hogy a jó megoldásokat az évfolyamon belül a hallgatók megosztották egymással, de mivel módszertanilag jelen tanulmányban nem volt célunk objektív mérést végezni ezen a területen, pusztán a mérési módszertan lehetőségeit kívántuk kipróbálni, az eredmény nem befolyásolja megállapításainkat. További kutatásaink során azonban ezt a faktort is alaposabban tervezzük megvizsgálni.

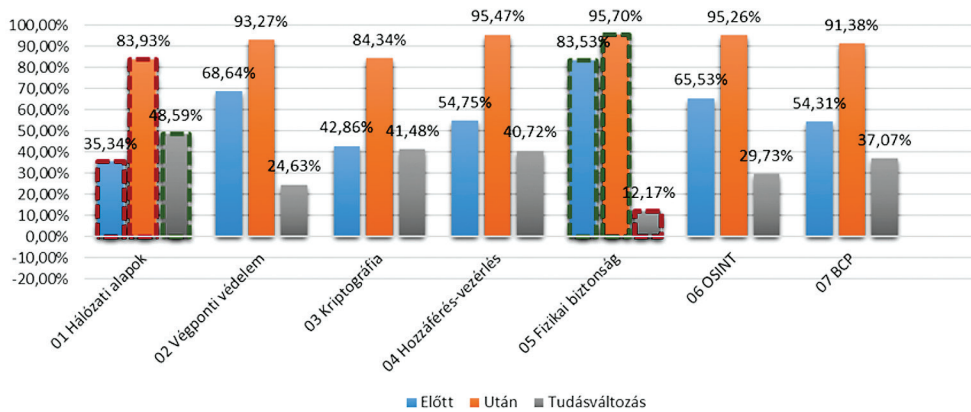
Összességében megállapítható, hogy a korábban említett befolyásoló tényezők ellenére is jelen kutatás megfelelő kiindulóalapot jelent a kiberbiztonsági képzés tantárgyi programjainak kidolgozásához.

5. Adatelemzés és a témakörök osztályozása

Jelen fejezetben bemutatjuk a hallgatók által kitöltött tesztek eredményeit, az azok alapján levonható következtetéseket, valamint az egyes témakörök előadásai során átadott tudás hallgatók általi elsajátítása alapján történő osztályozást.

5.1. Adatelemzés

Az egyes témakörök előtt és után kitöltött tesztek százalékos arányát, valamint az egyes témakörök tudástranszferjének hatékonyságát vizsgáltuk, aminek eredményeit a 3. ábra mutatja be.



3. ábra

Az egyes témakörök előtt és után mért összesített eredmények

Forrás: a szerző szerkesztése

A 3. ábra eredményeibe minden olyan hallgató válasza beleszámít, akik részt vettek a teszt kitöltésében, függetlenül attól, hogy kitöltötték-e az első órán megtartott általános kérdőívet.

1. témakör – Hálózati alapok

Az első témakör a *Hálózati alapok* címet viseli, amely összefoglalja és részletezi a számítógép-hálózatokhoz kapcsolódó alapfogalmakat, alapismereteket. A téma oktatása előtt egy öt kérdésből álló tesztet töltöttek ki, amelyre a hallgatók 35,34%-ban válaszoltak helyesen. Az óra végén ugyanazt a kérdéssort kapták a hallgatók, amely esetén már 83,93%-ban választották ki a megfelelő megoldásokat. Ezen téma esetében 48,59%-os tudásváltozás állt be, amely azt mutatja, hogy az órán elhangzottak

alkalmasak voltak tudásuk bővítésére. Jelen témakör esetében megállapítható, hogy az összes téma közül itt teljesítettek a legrosszabbul az oktatás előtti teszten a hallgatók (35,34%), és a tanítás utáni kérdéssorok esetében is (83,93%). Az összes témakörhöz viszonyítva ennek ellenére jelen témakörnél valósult meg a leghatékonyabb tudástranszfer, ugyanis a korábban említett 48,59%-os tudásváltozás a legmagasabb az összes témakör között.

2. témakör – Végponti védelem

A második, *Végponti védelem* című témakör a különféle kártékony programokat és az ezek elhárítására, megelőzésére szolgáló lehetséges alternatívákat, védelmi mechanizmusokat ismerteti. Ez esetben a tanítás előtti kérdéssorra 68,64%-os arányban érkeztek helyes válaszok, míg az előadás végén 93,27%-os arányban. A hallgatók tudásának változása az előadás előtthöz viszonyítva 24,63%-os volt.

3. témakör – Kriptográfia

A harmadik téma a *Kriptográfia* kérdéskörét öleli fel, amelyben kifejtették többek között a főbb alapfogalmakat, a kriptográfia történetét és módszereit, valamint az elektronikus aláírást is. Az oktatás előtti tesztre a hallgatók 42,86%-os arányban válaszoltak helyesen, az előadás végén pedig 84,34%-os arányban érkeztek helyes válaszok. A *Kriptográfia* téma esetében a tudásváltozás az összes téma tekintetében a második legmagasabb, 41,48%-os volt.

4. témakör – Hozzáférés-vezérlés

A negyedik témakör a *Hozzáférés-vezérlés* címet viseli, amely részletezi a kapcsolódó fogalmakat, elveket, a hozzáférés-ellenőrzés típusait, az esetleges védelmi intézkedéseket és a mobilbiztonság alapvető elemeit, lehetőségeit. Az előadás előtti kérdéssorra 54,75%-ban érkeztek helyes válaszok, míg a végén 95,47%-ban, amely a második legjobbnak értékelhető az összes témakör között. A hallgatók tudásváltozása 40,72%-os volt a két teszt között.

5. témakör – Fizikai biztonság

Az ötödik, *Fizikai biztonság* nevű témakör összefoglalja a fizikai biztonság alapjait, szükségességét, módszereit, a különféle információbiztonsági követelmények tartalmát, valamint a biztonsági technológiák és eszközök fontosságát és lehetőségeit. Az oktatás előtti tesztre 83,53%-ban, míg az oktatást követően 95,70%-os arányban érkeztek helyes válaszok. Az összes témakör közül a Fizikai biztonság esetén érkezett a legtöbb jó válasz a témáról tartott előadás előtt és után is, kifejezetten magas

értéket mutatott az előadás előtti teszt is, amelyből következik, hogy a tudásváltozás, a magas bemeneti értéknek köszönhetően jelen témánál volt a legalacsonyabb, mindössze 12,17%.

6. témakör – Nyílt forrású információszerzés (OSINT)

A hatodik téma az OSINT (*Open Source Intelligence* vagy más néven nyílt forrású információszerzés) kérdéskörét felölelő előadás, amely tartalmazza többek között az ehhez kapcsolódó alapismeretek, a lehetséges eszközök és módszerek, valamint a védelem alternatíváit is. Az előadás előtti teszten a hallgatók 65,53%-os arányban, míg az előadást követően 95,26%-os arányban válaszoltak helyesen. Ezek alapján megállapítható a hallgatók tudásváltozása, amely 29,73%-os arányú volt.

7. témakör –Üzletmenet-folytonossági terv (BCP)

A hetedik, vagyis az utolsó téma a BCP (*Business Continuity Plan*, más néven üzletmenet-folytonossági terv, amely magában foglalja az üzletmenet-folytonosság alapjait, az ehhez szükséges dokumentációkat és azok tartalmát. A témából tartott előadás megtartása előtt a hallgatók 54,31%-os arányban teljesítették jól a tesztet, míg az oktatást követően 91,38%-os arányban, ezek alapján a tudásuk változása 37,07%-os volt.

Összességében megállapítható, hogy minden témakör esetén megvalósult valamilyen szintű tudásátadás, átlagosan 33,48%-os tudásváltozás volt jellemző az oktatást követően, az oktatást megelőző tudásszinthez viszonyítva. Az ötödik, fizikai biztonság nevű téma esetében rendkívül alacsony (12,17%-os) volt a tudástranszfer, amelyből további következtetések vonhatók le. Általában, amennyiben a tudásváltozás alacsony, úgy mélyebb, részletesebb tudásátadásra van szükség, tehát ilyen esetekben az adott témakör ismereteinek mélyítése indokolt. A konkrét esetben azonban magas bázisról indult a teszt, azaz a hallgatók jól ismerték a fizikai biztonsággal kapcsolatos alaptéziseket, köszönhetően annak, hogy míg a kibertéri veszélyek a felmért csoport számára meglehetősen absztraktak, a fizikai tér kihívásait jól ismerik.

5.2. A témakörök osztályozása

A cél a korábban ismertetett NICE Keretrendszer általunk kiválasztott kiberbiztonsági munkakör esetén meghatározott követelmények hatékony átadása. Szükséges megvizsgálni minden témakör esetén, hogy a hallgatók e tudást maradéktalanul elsajátították-e. A témakörök előadásai után kitöltött teszek eredményei alapján a témakörök osztályozhatók aszerint, hogy a NICE Keretrendszerben rögzített ismereteket milyen mértékben sajátították el a hallgatók. Ehhez egy speciális szempontrendszert dolgoztunk ki. Ez azért elengedhetetlen, mert ennek segítségével megállapítható

minden egyes témakör tekintetében, hogy a továbbiakban szükséges-e mélyebb tudásátadás az előadásokon, kellően részletes-e az adott témakör, illetve indokolt-e a téma egyszerűsítése.

A témakörök csoportosításához az átadott tudás szintjét használjuk fel. Ezek alapján a következő csoportosítás alkalmazható:

- 90% felett: Kiváló
- 80%–90%: Jó
- 70%–80%: Közepes
- 60%–70%: Elégséges
- 60% alatt: Nem megfelelő

A bemutatott témaköröket ez alapján az alábbi csoportokba lehet helyezni:

- 1. témakör – Hálózati alapok: Jó
- 2. témakör – Végponti védelem: Kiváló
- 3. témakör – Kriptográfia: Jó
- 4. témakör – Hozzáférés-vezérlés: Kiváló
- 5. témakör – Fizikai biztonság: Kiváló
- 6. témakör – OSINT: Kiváló
- 7. témakör – BCP: Kiváló

E szempontrendszer és csoportosítás alapján megállapítható, hogy a célul kitűzött tudásmennyiséget szinte kiválóan sikerült átadni a hallgatók számára a tárgy keretében, hiszen a hét témakörből öt esetén 90% feletti eredményt értek el, és a maradék két témakör is jó „osztályzatot" ért el.

5.3. Következtetések

Ahhoz, hogy a tárgy keretében minden témakör kiváló minősítést kapjon, érdemes lenne a két „Jó" minősítéssel rendelkező témakört részletesebben oktatni, ami egyben azt is jelenti, hogy ezen előadások tekintetében az előadás hosszát, idejét növelni kell. Ennek következménye, hogy más témaköröknek az előadási idejét rövidíteni kell, célszerű azon témakörök előadásának hosszát csökkenteni, amelyek esetében a bemeneti tudás 80% feletti (például a fizikai biztonság témaköre, ahol a témakör előtti teszteredmények 83,53%-osak voltak).

A rosszabb eredményt elért témakörök esetén előfordulhat, hogy túl bonyolult volt a tananyag, ezért annak egyszerűsítése válik szükségessé.

További következtetések fogalmazhatók meg a „Kiváló" minősítéssel rendelkező témakörök esetében is. Ezen témakörök ismeretanyaga kellően részletes és megfelelően fedi a szükséges alapismereteket, így ezen előadások tartalmát tekintve további változtatási, módosítási teendő nincs. Kivételt képez ez alól a fentebb említett magas bemeneti értékű témakör, amely esetén a hallgatók alaptudása magas volt, így e témáknál lehetőség nyílik az előadások időtartamának rövidítésére a többi témakör javára.

6. Összefoglalás és következtetések

Tanulmányunkban definiáltuk a kibervédelmi képesség kialakításához szükséges készségek, képességek elsajátításához szükséges informatikai alapismeretek halmazát, amely nélkülözhetetlen a hatékony közszolgálati kiberbiztonság elérése érdekében. Az informatikai alapismeretek meghatározása egy, már folyamatban lévő rokon területen megvalósított képzés keretében oktatott tantárgy hatékonyságának elemzésével történt. A cél annak feltárása, hogy a vizsgált tantárgy tematikája esetlegesen felhasználható-e a közszolgálati kiberbiztonsági képzéshez.

Ennek megállapításához hipotéziseket fogalmaztunk meg, amelyek bizonyítására méréseket végeztünk a hallgatók már meglévő és az előadások segítségével elsajátított tudása tekintetében.

Ezenkívül felállítottunk egy szempontrendszert, amely segítségével osztályoztuk a témaköröket. A csoportosítás alapján javaslatokat fogalmaztunk meg az oktatás hatékonyságának fejlesztése, és a hallgatók által elsajátítható tudás növelésének elérése érdekében.

Az első hipotézisünkben azt vizsgáltuk, hogy a korábbiakban bemutatott tantárgy keretein belül hatékony volt-e a tudástranszfer. A hatékonyság fogalmát az első pontban, az 1. egyenlet segítségével definiáltuk. Ezek alapján a 4. pontban megvizsgáltuk az egyes tárgyak hatékonyságát (lásd 3. ábra), amely megmutatja, hogy minden témakör esetében hatékony volt a tudástranszfer. Ez alapján az első hipotézis igaznak bizonyult.

A második hipotézis esetében arra a kérdésre kerestük a választ, hogy a tantárgy tematikája alkalmas-e a szükséges informatikai alapismeretek elsajátítására, átadására. Az állítottuk, hogy a korábbiakban meghatározott ismeretanyag megfelelően fedi a szükséges informatikai alapismeretek halmazát, amely magában foglalja az általunk kiválasztott és 2. pontban ismertetett NICE Keretrendszerben rögzített adatvédelmi tisztviselő munkakör betöltéséhez elsajátítandó informatikai alapismereteket. Ezért jelen tantárgy a hipotézisben szereplő szükséges informatikai alapismeretek átadását maradéktalanul teljesíti. Továbbá extra témákat is érint (például OSINT), amely a kezdeti célokat túl is teljesíti.

A harmadik hipotézis esetében azt feltételeztük, hogy definiálható egy szempontrendszer, amely alapján osztályozható, hogy a témakörök során átadott tudás kellően részletes-e. A hipotézis bizonyításához a szempontrendszert az 5. pontban definiáltuk és fejtettük ki, amely alapján a témák megfelelően kategorizálhatók és osztályozhatók voltak. Ez alapján a harmadik hipotézis szintén igaznak bizonyul, hiszen a szempontrendszer segítségével megállapítható, hogy melyik témakört szükséges részletesebben oktatni, illetve melyhez szükségesek további előadások.

A negyedik hipotézis esetén azt vizsgáltuk, hogy az oktatott tantárgy felhasználható-e a kiberbiztonsági képzés során. E hipotézis igazolására az előző három hipotézis eredményét vesszük alapul. Az első hipotézis igaznak bizonyult, amely azt jelenti, hogy a tárgy keretén belül hatékony volt a tudástranszfer. Ezek alapján megállapítható, hogy az általunk elérni kívánt cél teljesült, a kiválasztott ismerethalmazt a hallgatók eredményesen sajátították el. A második hipotézisben bebizonyítottuk, hogy a tantárgy

tematikája és tananyaga megfelelően fedi a szükséges informatikai alapismereteket a NICE Keretrendszerben meghatározott és az általunk definiált elvárások szerint.

Ezt továbbá a leadott tananyag hatékonysága és a hallgatók által teljesített tanórai tesztek, valamint a félév végi vizsga is bizonyítja. A harmadik hipotézis alapján definiált szempontrendszer és az ezek segítségével megvalósuló osztályozás, vagyis az egyes témakörök csoportosításával megállapítottuk, hogy az átadott ismeretanyag kellően részletes volt-e, szükséges-e módosítani a hallgatók számára leadott tananyagot. Ezenkívül arra is választ kaptunk, hogy milyen módosításra, kiegészítésre szorul az adott témakör.

A három hipotézis teljesülése esetén megállapítható, hogy a negyedik hipotézis is igaznak bizonyul, amennyiben a harmadik hipotézisben foglalt változtatásokat végrehajtjuk, a vizsgált tantárgy felhasználható a kiberbiztonsági képzés során.

Meggyőződésünk szerint jelen kutatás eredményei megfelelő és hasznos kiinduló alapot jelentenek további kutatások számára, a jelen a tanulmányban említett kiberbiztonsági képzés szempontjából releváns további tantárgyak elemzése, illetve más képzések esetében egyaránt. Ezenkívül a kutatás folytatásaként a korábbiakban említett változtatások végrehajtását követően a vizsgált tantárgy újabb kiértékelése indokolt. Amennyiben az általunk definiált szempontrendszer alapján javasolt módosításoknak köszönhetően a tudástranszfer hatékonysága nő, úgy a szempontrendszer más tantárgyi struktúrák esetére is kiterjeszthető.

Felhasznált irodalom

Alsmadi, Izzat: Cybersecurity Education Based on the NICE Framework: Issues and Challenges, *ISACA Journal, 4.* (2018), 1–6. Online: www.isaca.org/Journal/archives/2018/Volume-4/Pages/cybersecurity-education-based-on-the-nice-framework.aspx

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

Bicak, Ali – Michelle (Xiang)Liu – Diane Murphy: Cybersecurity Curriculum Development: Introducing Specialties in a Graduate Program. *Information Systems Education Journal,* 13. (2015), 3. 99–110. Online: http://isedj.org/2015-13/n3/ISEDJv13n3p99.pdf

Dodge, Ronald C – Costis Toregas – Lance Hoffman: Cybersecurity Workforce Development Directions. *HAISA,* (2012), 1–13. Online: https://cspri.seas.gwu.edu/sites/g/files/zaxdzs1446/f/downloads/costis_-_cybersecurity_workforce_development_directions_0.pdf

Estes, Adriane C. – Dan J. Kim – T. Andrew Yang: Exploring How the NICE Cybersecurity Workforce Framework Aligns Cybersecurity Jobs with Potential Candidates. In *Proceedings of the 2018 International Conference on Frontiers in Education: Computer Science & Computer Engineering.* CSREA Press, Las Vegas, Nevada, 2018. 1–7. Online: https://par.nsf.gov/servlets/purl/10094856

Falus Iván (szerk.): *Bevezetés a pedagógiai kutatás módszereibe.* Budapest, Keraban, 1996.

Illésy Miklós – Nemeslaki András – Som Zoltán: Elektronikus információbiztonság-tudatosság a magyar közigazgatásban. *Információs Társadalom,* (2014), 1. 52–73. Online: http://epa.oszk.hu/01900/01963/00043/pdf/EPA01963_informacios_tarsadalom_2014_1_052-073.pdf

(ISC)²: *Certification Exam Outline* (2018. április). Online: www.isc2.org/-/media/ISC2/Certifications/Exam-Outlines/CISSP-Exam-Outline-2018-v718.ashx

Kumaladewi, Nia – Yuni Sugiarti: *Design Analysis of Data Warehouse for Lecturer Performance Evaluation (Case study: Faculty of science and technology UIN Jakarta).* 4th International Conference on Cyber and IT Service Management. 2016. 1–6. Online: https://doi.org/10.1109/CITSM.2016.7577531

McGettrick, Andrew: Toward Effective Cybersecurity Education, *IEEE Security & Privacy,* 11. (2013), 6. 66–68. Online: https://doi.org/10.1109/MSP.2013.155

Nagyné Takács Veronika – Kovács László: Az információbiztonsági vezető szakirányú továbbképzés tapasztalatai. *Pro Publico Bono – Magyar Közigazgatás,* 3. (2015), 4. 85–99. Online: https://folyoirat.ludovika.hu/index.php/ppbmk/article/view/2653/1918

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

Samian, Yahya – Norah Md Noor: Student's Perception on Good Lecturer based on Lecturer Performance Assessment. *Procedia-Social and Behavioral Sciences,* 56. (2012), 783–790. Online: https://doi.org/10.1016/j.sbspro.2012.09.716

Scheponik, Travis – Alan T. Sherman – David DeLatte – Dhananjay Phatak – Linda Oliva – Julia Thompson – Geoffrey L. Herman: How Students Reason about Cybersecurity Concepts. In *IEEE Frontiers in Education Conference (FIE)*. 2016. 1–5. https://doi.org/10.1109/FIE.2016.7757363

Jogi forrás

26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszerbiztonságáért felelős személyek képzésének és továbbképzésének tartalmáról