Az egyén információbiztonsági tudatossági szintjének megállapítására elterjedt mérési módszerek összefoglaló elemzése nemzetközi kutatások alapján

Berek László[1], Som Zoltán[2], Bak Gerda[3], Ujhegyi Péter[4], Répás József[5], Pető Richárd[6]

1 Óbudai Egyetem - Egyetemi Könyvtár. 1034 Budapest, Bécsi út 96/B. berek.laszlo@uni-obuda.hu

2 Gábor Dénes Egyetem. 1119 Budapest, Fejér Lipót u. 70. somzoltan@gmail.com

3 Óbudai Egyetem - Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar. 1081 Budapest, Népszínház utca 8. bak.gerda@uni-obuda.hu

4 Óbudai Egyetem – Biztonságtudományi Doktori Iskola. 1081 Budapest, Népszínház utca 8. ujhegyi.peter@uni-obuda.hu

5 Gábor Dénes Egyetem. 1119 Budapest, Fejér Lipót u. 70. repas.jozsef@alverad.hu

6 Óbudai Egyetem - Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar. 1081 Budapest, Népszínház utca 8. peto.richard@bgk.uni-obuda.hu

Absztrakt: A Gábor Dénes Egyetem elkötelezett a társadalom információbiztonsági tudatosságának fejlesztése mellett, ezért nagy hangsúlyt helyez annak szintjének megállapítására és növelésére. Az információs társadalom dinamikus fejlődése, a globális krízisek és konfliktusok, valamint a kibertérben folyamatosan növekvő fenyegetések növelik az információbiztonsági ismeretek fontosságát. Ezen tudatosság fejlesztése az emberek, vállalatok és országok biztonságának növeléséhez és gazdasági szempontból is elengedhetetlen. Ez sok új kihívással jár, nem csak a fizikai, hanem a digitális térben is. Annak érdekében, hogy megértsük, a lakosság és a KKV szektor ezen tudatosságát hogyan lehet fejleszteni, elengedhetetlen a korábbi kutatási eredmények áttekintése, tanulmányozása. Kutatásunk során a Scopus tudományos adatbázisból származó szakirodalmat elemeztük a témában, amelyek a 1991 és 2022 közötti időszakot foglalták magukba. Értékeltük a korábbi vizsgálatok módszertanát, hogy a bevált gyakorlatokat és módszertanokat felhasználhassuk. A vizsgálat során előre meghatározott paraméterek alapján szűrtük a forrásokat, hogy a számunkra releváns és feldolgozható mennyiségű publikációt tudjuk áttekinteni. Kutatásunk célja, hogy az információbiztonsági tudatossággal kapcsolatos felmérések és fejlesztések eredményei elérhetővé váljanak a kis- és középvállalkozások számára, valamint elősegíteni,

hogy beépüljenek a lakosság életébe és az oktatásába. Ez hozzájárulhat a kibertérben rejlő kihívásokra való jobb felkészültségéhez.

Kulcsszavak: GDE, kiberbiztonság; biztonságtudatosság; szakirodalmi áttekintés; felmérés; HAIS-Q

1 Bevezetés

Az infokommunikációs technológiák rohamos fejlődése nem csupán a digitális jólét megteremtésével jár együtt, hanem egyúttal a polgári lakosság jólétét, kényelmét is elősegítheti. Az információtechnológia azonban egyúttal óriási kockázatot is jelent, amennyiben nem tudatosan használjuk, így kiemelt figyelmet kell fordítani a polgári lakosság digitális immunitásának erősítésére. Ez komplex feladat, hiszen nem elegendő az egyének információbiztonsági tudását növelni, hanem a tudatosságukat is erősíteni szükséges a témában, illetve akár az információbiztonsági kultúra kialakítása, formálása is szükséges lehet. [1]

A polgári lakosságban az információbiztonság tudatosítása a saját biztonságuk erősítése mellett együtt jár az adott állam nemzetbiztonsági szintjének növelésével, a kritikus infrastruktúrák kitettségének csökkenésével. Ehhez pedig folyamatos tudatosítási oktatásokra, képzésekre [2], valamint az egyes szervezetek és állami szervek aktív szerepvállalására [3] is szükség van.

Digitalizálódó világunkban kiemelt fontosságú feladat az állampolgárok, vállalkozások és a társadalom egyéb szereplőinek tudatosítása a digitális eszközök és szolgáltatások biztonságtudatos használatában, valamint a proaktív biztonságtudatos viselkedés elősegítésének érdekében.

A tudatosítás egyre fontosabb feladattá válik világszinten, és így fokozott aktivitást igényel Magyarország állampolgárai és a társadalom különböző szereplői esetében is, annak érdekében, hogy a mindennapok részévé váló digitális eszközök és szolgáltatások biztonságos használatát elsajátítsák. Mindezek mellett a nemzetközi területeken megfigyelhető trendek is indukálják, valamint erősítik a kutatási terület fontosságát. Ugyanakkor kevés és nem túl részletes információ áll rendelkezésre a lakosság, a gazdasági szereplők tájékozottságáról, tudatosságáról, fenyegetettségéről. A kiber bűncselekmények egyre növekvő száma, az okozott károk mértéke és értéke, illetve a fejlődő technológia és a kiberbűnözők által használt újabbnál újabb megoldások is növelik a kutatás jelentőségét, de a szabályozói oldal reaktív természete is idesorolandó. Mindazonáltal a kiberbűncselekmények okozta negatív hatásokat sem felejthetjük el, melyek a vállalatok esetében az anyagi károkon túl, fogyasztói elpártolást, reputáció veszteséget és a versenytársak erősödését is eredményezheti. [4][5] Valamint az állami szolgáltatások szempontjából is hasonló károkat okozhat.

1.1 Kutatási célok

A jelen tanulmányban először az 1991-2022 között publikált cikkeket tekintjük át, melyek a kiberbiztonság, információbiztonság területén valamilyen módon a biztonságtudatosság mérésével is foglalkoztak. Ezt követően megvizsgáljuk a megfigyelhető trendeket a publikációk és azok tudományterületi megoszlása szempontjából, azonosítjuk a kiemelkedő publikációkat és a leginkább hivatkozott kutatási eredményeket. Végül a szakirodalmi áttekintés következtetése kerül bemutatásra.

A kutatás elsődlegesen a vizsgált tématerület helyzetéről kíván képet adni, amely tartalmazza az elmúlt évek trendjeit, kiemelkedő publikációit és a jelentősebb szerzőket. Ezt alátámasztva az alábbi megközelítéssel éltünk: megvizsgáltuk, mely országok dominálnak a vizsgált témában, az elmúlt években miként változott a téma kutatottsága, az alkalmazott kulcsszavak, illetve mely országokhoz kapcsolódik jellemzően a kutatások publikálása.

A kutatás során a szakirodalmi áttekintés eredményei hozzájárulhatnak a legalkalmasabb felmérési módszer megalkotásához. A következő kutatási kérdésekre kerestük a választ:

K1: A kapcsolódó kutatások milyen tudományterületen jelentek meg?

K2: Mely országok, mely kutatók foglalkoznak leginkább a témával, hol találjuk a leginkább hivatkozott kutatási eredményeket?

K3: A vizsgált időszakokban milyen változások figyelhetők meg a kulcsszavak összetételében, használatában?

K4: A vizsgált szakirodalmi minta alapján a biztonságtudatosság mérése területén milyen sajátosságok figyelhetők meg? Mennyire jellemző a HAIS-Q alkalmazása, a saját kérdőív összeállítása, esetleg interjú, vagy más módszer használata?

2 Módszertan

A szakirodalom keresése a Scopus tudományos adatbázis platformján valósult meg 2023. októberében. A kutatás során a releváns nemzetközi szakirodalom áttekintésével mértük fel a kutatási eredmények alapján a biztonságtudatosságra vonatkozó mérések helyzetét. Fontos megemlíteni, hogy a kutatáshoz kapcsolódóan a Web of Science adatbázisban is végeztünk szakirodalmi áttekintést, ennek eredményeit is publikáltuk. [6]

2.1 Keresési stratégia

A keresés kulcsszavainak kiválasztásában alapul vettünk egy tesztkeresést, amelynek kulcsszókészletét elemezve jutottunk el a végső keresőkifejezés megalkotásához. A kereséskor alkalmazott kulcsszavak, illetve a kifejezések

csonkolt változatai a következők voltak: *awarene*, cybersecurit*, information securit*, IT securit*, questionn*, survey**.

A meghatározott kulcsszavak és boolean operátorok felhasználásával a következő CCL keresőkifejezést alkalmaztuk:

TITLE-ABS-KEY (awarene AND cybersecurit* AND questionn*) OR TITLE-ABS-KEY (awarene* AND cybersecurit* AND survey*) OR TITLE-ABS-KEY (awarene* AND "information securit*" AND questionn*) OR TITLE-ABS-KEY (awarene* AND "information securit*" AND survey*) OR TITLE-ABS-KEY (awarene* AND "IT securit*" AND questionn*) OR TITLE-ABS-KEY (awarene* AND "IT securit*" AND survey*) OR TITLE-ABS-KEY ("Cybersecurity skill*" OR "Cybersecurity awareness" OR "Information security awareness" OR "Information security behaviour")*

A keresőkifejezés alkalmazásával a Scopus adatbázisából 1857 találatot kaptunk, így a beválasztási kritériumok mellett kizárási kritériumokat is meghatároztunk.

2.2 Kiválasztási stratégia

A korlátozó, kizárási kritériumok a publikációk nyelvére, a dokumentumok típusára, illetve a megjelenés évére vonatkoztak.

1 Táblázat
Scopus keresés során alkalmazott korlátozó kritériumok

Korlátozó kritérium	Érték
Megjelenés éve	1991-2022
Nyelv	Angol
Dokumentumtípus	Folyóiratcikk

A beválasztási és kizárási kritériumok alkalmazásával a végső keresőkifejezésünk a következő volt:

TITLE-ABS-KEY (awarene AND cybersecurit* AND questionn*) OR TITLE-ABS-KEY (awarene* AND cybersecurit* AND survey*) OR TITLE-ABS-KEY (awarene* AND "information securit*" AND questionn*) OR TITLE-ABS-KEY (awarene* AND "information securit*" AND survey*) OR TITLE-ABS-KEY (awarene* AND "IT securit*" AND questionn*) OR TITLE-ABS-KEY (awarene* AND "IT securit*" AND survey*) OR TITLE-ABS-KEY ("Cybersecurity skill*" OR "Cybersecurity awareness" OR "Information security awareness" OR "Information security behaviour") AND PUBYEAR > 1990 AND PUBYEAR < 2023 AND (LIMIT-TO (DOCTYPE , "ar")) AND (LIMIT-TO (LANGUAGE , "English")) AND (LIMIT-TO (SRCTYPE , "j"))*

Az elsődleges korlátozási kritériumunk a publikációk megjelenési éve volt, a keresést szűkítettük az 1991 és 2022 között megjelent publikációkra. Ezzel a szűkítéssel 1602 publikációt kaptunk vissza. További kritériumnak határoztuk meg a publikáció nyelvét: angol. Mivel a Scopus adatbázis elsődlegesen angol nyelvű

publikációkat indexel, így ezzel nem sok találat esett ki, még mindig 1580 publikációnk volt. Az utolsó – de legfontosabb – kritériumunk a publikációk típusára vonatkozott: csak azon kutatási eredményeket vettük be a szakirodalmi áttekintésünkbe, amelyek folyóiratban, folyóiratcikk (*Article*) formájában jelentek meg. Ezzel a vizsgálandó publikációk száma 591 lett. Az elsődleges áttekintést ezen a mintán végeztük.

A kulcsszavak, tárgyszavak időbeli fejlődésének, változásainak vizsgálatához, illetve a tudományterületi megoszlás változásainak megjelenítéséhez további szűkítést is alkalmaztunk. A vizsgált időszak utolsó 10 évét megosztottuk két 5 éves időintervallumra: a 2013 és 2017 között, valamint a 2018 és 2022 között megjelent publikációkra.

2.3 Adatkinyerés és adatfeldolgozás

Az adatok feldolgozásában egyrészt a Scopus adatbázis felületén elérhető lehetőségeket alkalmaztuk a következő területeken: leghivatkozottabb publikációk kiválasztása, tudományterületi – subject area – szerinti megoszlás vizsgálata, a kutatási eredmények ország szerinti eloszlása, publikációk affiliáció szerinti megoszlása. Természetesen külső szoftvereket is alkalmaztunk az adatok feldolgozásakor, ilyen a PoP (Publish or Perish) és a VOSViewer.

A VOSviewer adatvizualizációra és elemzésre alkalmazható szoftver. Segítségével a tudományos publikációk, szerzők, kulcsszavak és más tudományos adatok elemzése és megjelenítése valósítható meg. A VOSViewer alkalmas a kutatási területek elemzésére, publikációs térképek létrehozására vagy a kulcsszavak közötti kapcsolatok feltárására és vizualizálására.

Az adatkinyerés a Scopus adatbázisából egyrészt közvetlenül a Zotero reference management szoftver segítségével, másrészt RIS formátum alkalmazásával történt. Ez a RIS Scopus export került feldolgozásra a Publish or Perish szoftver segítségével.

3 Eredmények

A szakirodalom áttekintése alapján megállapítható, hogy a téma az évek során egyre inkább kutatott. A biztonságtudatosság mérésével kapcsolatos kutatások száma évről-évre nő és ezzel együtt az egyes területek specializálódása is megfigyelhető.

3.1 Publikációk száma

A publikációk száma alapján, az elmúlt egy évtizedet vizsgálva kirajzolódni látszik, hogy egyre több minőségi – a Scopus adatbázisban indexelt – publikáció jelent meg, ahogy azt az 1. ábrán is láthatjuk. Az elmúlt évtizedben a kapcsolódó publikációk számának növekedése olyan mértékűvé vált, hogy az elmúlt 5 évben (2018-2022)

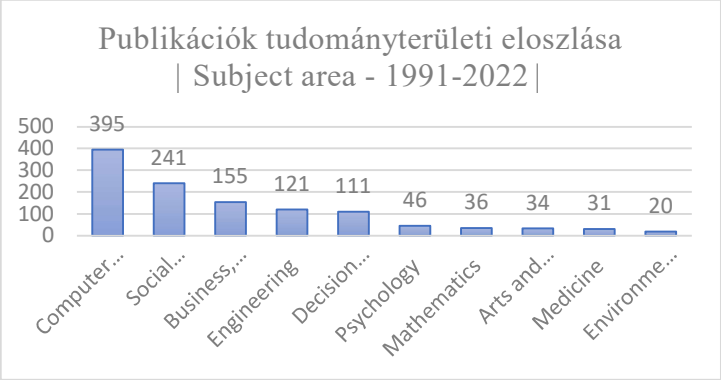
megjelent publikációk száma háromszorosa lett az azt megelőző 5 évben (2013-2017) publikáltaknak. Ezt az összehasonlítást láthatjuk a 3. ábrán. Prognosztizálható, hogy ez a következő években folytatódni fog.

1 ábra
Publikációk száma éves bontásban | 2013-2022 |

3.2 Tudományterületi megoszlás

A vizsgálatba bevont publikációk tudományterületi megoszlását a Scopus adatbázis "Subject area" besorolásai alapján végeztük. A Scopus adatbázisa által indexelt folyóiratokat a platform tudományterületekbe sorolja. Fontos megemlíteni, hogy egy-egy folyóirat ebben a rendszerben egyszerre több területre is besorolódhat, így több Subject area része lehet a vizsgált publikáció is.

Az 591 publikáció Subject area alapján történő eloszlása alapján elmondható, hogy a "Computer Science", a Social Sciences" és a "Business Management and Marketing" területeken (*informatika, társadalomtudomány, gazdaság-menedzsment és marketing*) működő folyóiratokban jelentek meg leginkább a biztonságtudatosság mérésével kapcsolatos kutatási eredmények. A top 10 tudományterületet a 2. ábra mutatja.

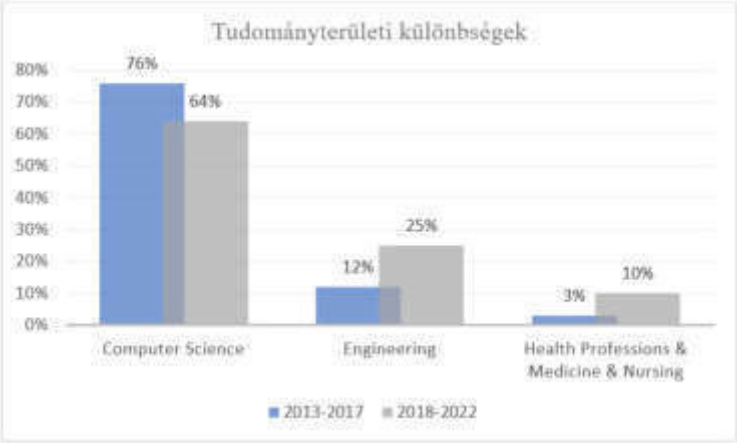


2 ábra
Publikációk tudományterületi eloszlása | Subject area - 1991-2022 |

Amennyiben az elmúlt 5 év (2018-2022) és az azt megelőző 5 év (2013-2017) publikált kutatási eredményeit a tudományterületi eloszlás alapján vizsgáljuk, úgy három "Subject area" esetében láthatunk jelentősebb változást. (4. ábra) Az informatika (Computer Science) területen működő folyóiratok esetében több mint 10%-os csökkenést láthatunk, amely mutatja azt, hogy a biztonságtudatossággal kapcsolatos kutatások egyre inkább érintik a többi tudományterületet is. A mérnöki tudományok (engineering) esetében jelentős növekedés látható: 12%-ról 25%-ra nőtt az ezen a területen működő folyóiratokban megjelent cikkek száma.

3 ábra
Publikációk száma a két vizsgált időszakban | 2013-2017 és 2018-2022 |

A harmadik fellelt, tudományterületeket érintő változás a legnagyobb arányú: az orvosi- és egészségtudományok területén működő folyóiratokban a témával kapcsolatban a 2013-2017 közötti időszakban a publikációk mindössze 3%-át találtuk. Ha viszont megnézzük a 2018-2022 közötti időszak publikációs termését, akkor azt láthatjuk, hogy 10%-ra emelkedett ez az arány. Leegyszerűsítve elmondható, hogy a témával kapcsolatban megjelent folyóiratcikkek közül minden 10. ilyen besorolású folyóiratban jelent meg. Jól látszik, hogy az orvosi-, egészséghez kötődő információk, informatikai rendszerek védelme, biztosítása egyre fontosabbá vált, amivel együtt jár a biztonságtudatosság kutatása is.



4 ábra
A két időszak jelentősebb változásai a tudományterület szempontjából | 2013-2017 és 2018-2022 |

3.3 Országok szerinti megoszlás

A biztonságtudatosság mérésével kapcsolatos kutatások tekintetében jól látható, hogy az Egyesült Államok kiemelkedik. Elmondható, hogy a vizsgált mintában minden 4. kutatási eredmény az Egyesült Államokhoz kapcsolódik. A szakirodalmi áttekintés alapján látható, hogy a közép-európai, kelet-európai, dél-amerikai országok nem szerepelnek nagy számú kutatási eredménnyel a témában. Erre az eredményre jutottak korábbi kutatások is a biztonságtudatosság szakirodalmának áttekintésekor. [7]

3 Táblázat
Publikációk országok szerinti eloszlása | 2013-2022 |

	Ország	**Publikációk száma**
1.	USA	145
2.	Egyesült Királyság	63
3.	Ausztrália	52
4.	Malajzia	46
5.	Kína	33
6.	Dél-Afrika	33
7.	Szaúd-Arábia	31
8.	Dél-Korea	29
9.	Törökország	20
10.	Tajvan	18

3.4 Kulcsszókészlet vizsgálata

A két vizsgált időszak kulcsszókészletének összehasonlításával képet kaphatunk a terület releváns kutatásaihoz kapcsolódó kifejezések, valamint a terminológia változásairól.

3 Táblázat
Leggyakrabban használt kulcsszavak a két időszakban | 2013-2017 | 2018-2022 |

	2013-2017	2018-2022
1.	Security Of Data	**Cybersecurity**
2.	Information Security	Security Of Data
3.	Information Security Awareness	Information Security
4.	Surveys	Surveys
5.	Security Systems	Information Security Awareness
…		
7.	**Cybersecurity**	

A két minta publikációinak kulcsszókészletét elemeztük, ennek során a leggyakrabban használt kulcsszavakat sorrendbe állítottuk az előfordulásuk gyakorisága alapján. A két időszak leginkább használt kulcsszavai láthatók a 3. táblázatban. A kutatók által leginkább használt kulcsszavak rangsorában egy komolyabb változást láthatunk, ez a kiberbiztonság kifejezés.

A kiberbiztonság kifejezés a vizsgált minta 2013-2017 közötti időszakában még csak a 7. helyen szerepelt, de a 2018-2022 közötti időszak szakirodalma már alap kulcsszóként használja. A terület terminológiai kiszélesedését, specializálódását jelzi, hogy míg az első 5 éves szakaszban a “cyber*” kezdetű kulcsszavakból mindössze 2 található a mintában (*Cybersecurity; Cyber Threats*) addig az elmúlt 5 év mintájában már 11 ilyen kifejezést azonosítottunk. (*Cybersecurity; Cybersecurity Awareness; Cyber-attacks; Cybersecurity Education; Cybercrime; Cyber-security Educations; Cyber Threats; Cybersecurity Skills; Cyber-crimes; Cyber-attack; Cyber Attacks*)

A teljes kulcsszókészletet vizsgálva megállapítható, hogy hasonló módon szélesedett ki az biztonságtudatosság oktatásával foglalkozó kutatások területe. Az education* kifejezés az elmúlt 5 év publikációi esetében sokkal több, speciális formában került be a publikációk kulcsszavai közé.

3.5 Mérési módszerek vizsgálata

A kutatási eredmények vizsgálata során a két 5 éves időszak szakirodalmából az 50-50 leghivatkozottabb publikációt értékeltük. Az áttekintés során a cím és az absztrakt alapján, majd a teljes szöveg vizsgálatával tudtuk tanulmányozni, hogy az adott kutatás során alkalmaztak-e valamilyen egyénre vonatkozó mérési módszert. Ennek eredménye lett 37 publikáció, amelyeket további vizsgálat alá vetettünk.

Megállapítható, hogy a fellelt kutatások túlnyomó része a biztonságtudatosság méréséhez kérdőívet alkalmazott. A 37 publikációból mindössze 3 alkalmazott interjút a felmérés során. [8-10] Ezen publikációk mindegyike céges környezetben vizsgálta a biztonságtudatosságot. Tehát elmondható, hogy a szakirodalmi mintánkban lakosságra vonatkozó felmérés során csak kérdőíves módszert találtunk. Itt kell újra megjegyezni, hogy az áttekintés során a 100 leghivatkozottabb publikációt vizsgáltuk, a tágabb tartományban természetesen előfordulhat példa arra, hogy interjút alkalmaztak lakossági felmérés során.

A vizsgálatba bevont publikációk közül 22 foglalkozott céges környezetben a biztonságtudatosság mérésével, 15 kutatás esetében az egyénre fókuszált a felmérés. Hozzá kell tenni természetesen, hogy a céges, vállalati környezetben lefolytatott kutatás is az egyén szempontjából vizsgálta a biztonságtudatosságot.

A kérdőíves felmérést alkalmazó kutatásokról megállapítható, hogy túlnyomó többségükben saját kérdőív összeállítása történt meg, bár ezek között több olyan volt, amelynél korábbi kérdőíveket használtak fel. A vizsgálatba bevont publikációk közül 6 esetben találtunk olyan kutatást, amelyben a HAIS-Q (*Human Aspects of Information Security Questionnaire*) kérdőívet alkalmazták. [11-16] További 4 esetben a publikációban hivatkoztak a HAIS-Q-ra. Megállapítható, hogy a szakirodalmi mintánkban nevesített kérdőívként egyedül a HAIS-Q szerepelt és ezekben a kutatásokban egyenlő arányban szerepeltek a kizárólag egyénre vonatkozó, illetve céges környezetben végzett felmérések. Árnyalja a képet, ha ezt a 6 publikációt megnézzük közelebbről, de legalábbis a szerzői közösséget, a kutatócsoportot. Látható, hogy a HAIS-Q első publikálását követően mindegyik ezt a módszert alkalmazó publikáció szerzői között több kutató szerepel az eredeti kutatócsoportból.

A bevont szakirodalom alapján megállapítható, hogy az utolsó 5 éves időszakban speciálisabb területeket is kutattak. Ilyenek például a kifejezetten az okostelefonok/mobileszközök (*mobil devices*) használatára vagy a közösségi média fogyasztásra fokuszáló biztonságtudatossági felmérések. Ezek mellett érdemes megemlíteni az egészségügyhöz kapcsolódó témák megjelenését, akár a kórházi informatikai rendszerre, akár a viselhető orvostechnikai eszközökre (*Wearable medical devices*) vonatkozó kutatásokat hozzuk fel példának.

4 Következtetések

Kutatásunk ezen szakaszában a fő célkitűzés a biztonságtudatosság mérésére alkalmazott módszerek összegyűjtése volt a kapcsolódó szakirodalom áttekintésével. Tanulmányunkban vizsgáltuk a kapcsolódó kutatások számának alakulását, valamint a tudományterületi megoszlásukat is. Az áttekintés során a bevont publikációkon keresztül vizsgáltuk a kutatások országok szerinti megoszlását is. Ezen túlmenően a vizsgálat célja volt a biztonságtudatosság, illetve

annak mérése témájában írt publikációkat alapul véve feltérképezni a kulcsszókészlet sajátosságait, illetve változásait és fejlődését.

Az eredmények alapján jól látható, hogy a terület kutatása egyre fontosabb lesz a jövőben. Az is megállapítható, hogy egyre speciálisabb részterületeken folynak kutatások és a terület kiszélesedése prognosztizálható. Ezt támasztja alá a kulcsszókészlet vizsgálata, illetve a részletes szakirodalmi áttekintés eredménye is.

A szakirodalom áttekintésével megfelelő képet kaptunk az elmúlt évek kutatásai során alkalmazott biztonságtudatosság mérési módszereiről. A tapasztalatokat a jövőben a kutatócsoport alkalmazni fogja a felmérési módszer kialakításakor. A Web of Science adatbázison alapuló, korábban lefolytatott kutatás eredményeit is felhasználva, további tudományos források bevonásával érdemes tovább bővíteni jelen kutatásunkat.

Összefoglalás

Tanulmányunkban az elmúlt évek releváns kutatásait vizsgálva a szakirodalom áttekintésével mutattuk be a biztonságtudatosság mérésének aktuális helyzetét. A kulcsszókészlet és a publikációk adatai segítségével azonosítottunk és jelenítettünk meg trendeket és jövőbeli irányokat.

A biztonságtudatosság mérésének vizsgálata hozzájárul a későbbi kutatás sikeréhez, a leginkább megfelelő mérési módszer megalkotásához vagy alkalmazásához mind a lakosság, mind a KKV-k vonatkozásában. A szakirodalom áttekintése a mérési módszerek vonatkozásában irányt mutat: túlnyomó többségben vannak a kérdőíves módszert alkalmazó publikációk, akár a lakossági, akár a céges környezetre vonatkozó kutatásokat vizsgáljuk. A konkrét mérési módszerek áttekintésekor a HAIS-Q kérdőíven kívül nem került azonosításra más nevesített kérdőív. Bár a fellelt, HAIS-Q-t alkalmazó kutatások esetében elmondható, hogy a szerzők között az eredeti kutatócsoport tagjai szerepelnek, mégis fontos tény a kérdőív szakirodalmi hivatkozottsága. Megfontolandó irány lehet a HAIS-Q kérdőív aktualizálása, kiegészítése, de mindenképp valamilyen formában történő alkalmazása a kutatócsoport saját felmérésének kidolgozásakor.

Köszönetnyilvánítás

A Gábor Dénes Egyetem, Lakossági és KKV információbiztonsági fejlesztések projekt a TKP2021-NVA-05 projekt keretében megvalósult kutatás.

A kutató csoport kiemelt célja, a magyar polgári lakosság digitális immunitásának erősítése. Ehhez szükséges felmérés elkészítése és lefolytatása az információbiztonság, digitális immunitás témakörében, valamint a polgári lakosságon keresztül a lakossági technológiát használó KKV-k információbiztonságának felmérése, annak fejlesztési lehetőségeinek feltárása.

A szerzők külön szeretnének köszönetet mondani az Alverad Technology Focus Kft. Kutatás, fejlesztés és Innováció üzletágának a kutatási munkához nyújtott támogatásért.

Felhasznált Irodalom

[1] Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. Computers & Security, 53, 65–78. https://doi.org/10.1016/j.cose.2015.05.012

[2] Nyikes, Z. (2021). Az információbiztonság növelése a felhasználó támogatásának lehetőségeivel [(PhD disszertáció)]. Óbuda Egyetem, Biztonságtudományi Doktori Iskola.

[3] Bencsik, B. & Tikos, A. (2018). A kiberbiztonsági kihívások globális és hazai trendjei. In Digitális környezetünk fenyegetettsége a mindennapokban (pp. 45–60). Dialóg Campus Kiadó.

[4] Modi, S. B., Wiles, M. A., & Mishra, S. (2014). Shareholder value implications of service failures in triads: The case of customer information security breaches. Journal of Operations Management, 35(1), 21–39. https://doi.org/10.1016/j.jom.2014.10.003

[5] Jeong, C. Y., Lee, S. Y. T., & Lim, J. H. (2019). Information security breaches and IT security investments: Impacts on competitors. Information & Management, 56(5), 681–695. https://doi.org/10.1016/j.im.2018.11.003

[6] Bak, G., Berek, L., Som, Z., Ujhegyi, P., Répás, J. & Pető, R. Nemzetközi kutatások áttekintő elemzése az egyén információbiztonság tudatossági szintjének mérési módszereire. Biztonságtudományi Szemle. (inprint)

[7] Bak, G. & Kiss, S. (2021). A biztonságtudatosság szisztematikus szakirodalmi áttekintése. Hadmérnök, 16(4) , 85-99. https://doi.org/10.32567/hm.2021.4.7

[8] Kessler, S.R., Pindek, S., Kleinman, G., Andel, S.A., Spector, P.E. (2020). Information security climate and the assessment of information security risk among healthcare employees. Health Informatics Journal, 26(1) , 461-473. https://doi.org/10.1177/1460458219832048

[9] Ali, O., Shrestha, A., Chatfield, A., Murray, P. (2020). Assessing information security risks in the cloud: A case study of Australian local government authorities. Government Information Quarterly, 37(1) https://doi.org/10.1016/j.giq.2019.101419

[10] Diesch, R., Pfaff, M., Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. Computers and Security, Vol. 92. Article number 101747.

https://doi.org/10.1016/j.cose.2020.101747

[11] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers and Security, Vol. 42. 165-176.
https://doi.org/10.1016/j.cose.2013.12.003

[12] McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., Pattinson, M.. (2017). Individual differences and Information Security Awareness. Computers in Human Behavior, Vol. 69. 151-156.

https://doi.org/10.1016/j.chb.2016.11.065

[13] Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Computers and Security, Vol. 66. 40-51.

https://doi.org/10.1016/j.chb.2016.11.065

[14] Hadlington, L., Parsons, K. (2017). Can Cyberloafing and Internet Addiction Affect Organizational Information Security? Cyberpsychology, Behavior, and Social Networking, 20(9), 567-571.
https://doi.org/10.1089/cyber.2017.0239

[15] Wiley, A., McCormac, A., Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. Cyberpsychology, Computers and Security, Vol. 88. Article number 101640.
https://doi.org/10.1016/j.cose.2019.101640

[16] McCormac, A., Calic, D., Parsons, K., Butavicius, M., Pattinson, M., Lillie, M. (2018). The effect of resilience and job stress on information security awareness, Information and Computer Security, 26(3). 277-289.
https://doi.org/10.1108/ICS-03-2018-0032