HADMÉRNÖK
VÉDELEMINFORMATIKA
16. évfolyam (2021) 4. szám 85–99.
DOI: 10.32567/hm.2021.4.7

Bak Gerda,[1] Kiss Sándor[2]

A biztonságtudatosság szisztematikus szakirodalmi áttekintése

Systematic Literature Review of Safety Awareness

Napjainkra a digitális eszközök a mindennapok elengedhetetlen részévé váltak, legyen szó munkáról vagy kikapcsolódásról, az élet minden területén jelen vannak, azonban számos veszélyt is magukban hordoznak. A technológia fejlődésével rengeteg információ cserél gazdát online, kerül fel a felhőbe, tároljuk a digitális eszközökön, amelyek feltételezhetően lehetőséget nyújtanak a magánszféra és az érzékeny adatok illetéktelenek általi megszerzésére, kiszivárogtatására. A potenciális veszélyek kivédésére megoldás lehet a digitális eszközöket használók tudatosítása. A kutatás célja áttekintést adni azokról a tényezőkről, amelyek az egyének biztonságtudatosságát befolyásolják. Ezeknek a tényezőknek a feltárására és összegyűjtésére szisztematikus irodalomelemzést alkalmaztunk a ScienceDirect, a Google Scholar és a Web of Science adatbázisokban 2012. január és 2020. december közötti időszakot vizsgálva. Az elemzés során kizárólag angol nyelvű és teljes terjedelmükben elérhető cikkek keresése történt, amihez megfelelő kulcsszavakat választottunk ki és alkalmaztunk. A keresés lefolytatása után potenciálisan 419 közlemény képezte a részletesebb elemzés tárgyát, amelyekből végül 92 felelt meg az előzetesen megfogalmazott kritériumoknak. Ezek alapján a biztonságtudatossági szintre hatással van többek között az egyén neme, kora, tanulmányai, gondolkodásmódja, továbbá a tapasztalatai és a személyisége is, valamint a vállalati kultúra.

Kulcsszavak: biztonságtudatosság, szisztematikus szakirodalmi áttekintés, 2012–2020

Today, digital devices have become an indispensable part of everyday life, whether for work or leisure; they are present in every aspect of life, but they also carry several dangers. As technology advances, a lot of information is exchanged online, uploaded to the cloud, stored on digital devices, potentially allowing privacy and sensitive data to be obtained or leaked by unauthorised parties. A solution to potential threats can be to raise awareness of the people using digital devices. This research aims

[1] Óbudai Egyetem Biztonságtudományi Doktori Iskola, doktori hallgató, e-mail: bak.gerda@uni-obuda.hu
[2] Nemzeti Közszolgálati Egyetem, egyetemi docens, e-mail: kiss.sandor@uni-nke.hu

to provide an overview of the factors that influence individuals' security awareness. To this end, a systematic literature review was conducted in ScienceDirect, Google Scholar and Web of Science databases between January 2012 and December 2020. The analysis was performed by searching only for articles in English and available in full text, for which appropriate keywords were selected and applied. After conducting the search, a potential 419 publications were analysed in more detail, of which 92 finally met the pre-defined criteria. They found that the level of safety awareness is influenced by, among other things, the individual's gender, age, education, mindset, experience and personality, as well as corporate culture.

Keywords: **security awareness, systematic literature review 2012–2020**

1. Bevezetés

A biztonságtudatosság minden biztonsági infrastruktúra fontos eleme, főként, mert gyakran az emberi tényező bizonyul a leggyengébb láncszemnek. Az utóbbi években a vállalatok és a különböző szervezetek is felismerték a biztonságtudatosság jelentőségét, aminek következtében olyan programokat dolgoztak ki, amelyek a biztonság népszerűsítését és fontosságának tudatosítását tűzték ki célul. Ez azonban nem egyszerű, hiszen a tudatosság növelése folyamatosságot igényel, különösen, hogy a technológia rohamos ütemben fejlődik, továbbá számos kampány nem hozza el a kívánt eredményt, mert az emberek viselkedésének megváltoztatásához a tudatosság és a tudás növelése önmagában nem elegendő.[3] Jelen tanulmány ezért a biztonságtudatosság humán aspektusával foglalkozó tanulmányokat gyűjti egybe és elemzi.

A tanulmány a következő részekből tevődik össze: elsőként bemutatjuk a szakirodalmi áttekintés módszerét, valamint az összegyűjtött tanulmányok fő jellemzőit. A következő részben összefoglaljuk a biztonságtudatosságot befolyásoló tényezőket, amelyeket az elemzett publikációk azonosítottak. A tanulmány végén pedig áttekintjük a tanulmányban bemutatott eredményeket és a jelentőségüket.

A tanulmány két kérdésre keresi a választ. Először is, hogy milyen tendencia figyelhető meg a biztonságtudatossági kutatásokban, illetve hogy melyek a biztonságtudatosság-kutatások főbb eredményei az emberi tényező kapcsán.

2. Biztonságtudatosság

Az információbiztonsági fenyegetések és incidensek komoly veszélyt jelentenek a digitalizált gazdaságok túlélésére. Az ilyen incidensek jelentős pénzügyi veszteségeket, csökkent tőzsdei értékelést, csorbult hírnevet és jogi szankciókat eredményeznek.[4] A bizalmas

[3] Maria Bada – Angela Sasse – Jason R. C. Nurse: *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?* In International Conference on Cyber Security for Sustainable Society. United Kingdom, Coventry University, 2015. 118–131.

[4] Daniele Bianchi – Onur Kemal Tosun: Cyber Attacks and Stock Market Activity. *International Review of Financial Analysis,* 76. (2019), 101795.

és érzékeny információk elvesztése vagy ellopása adatonként 150 dollár, évente pedig átlagosan 8,9 millió dolláros veszteséget eredményez az Amerikai Egyesült Államokban.[5]

A szervezetek az informatikai költségvetés mintegy 36%-át fordítják a Security Incident Managementre, amely érték várhatóan az elkövetkező években növekedni fog.[6] A Security Incident Management alatt a biztonsági fenyegetések vagy incidensek valós idejű azonosításának, kezelésének, rögzítésének és elemzésének folyamatát értjük. Célja, hogy megbízható és átfogó képet adjon az informatikai infrastruktúrán belüli biztonsági problémákról. A biztonsági incidens lehet bármi, az aktív fenyegetéstől kezdve a behatolási kísérleten át, a sikeres adatszerzésig. A biztonsági incidensekre példaként említhető a szabályzatok megsértése és az olyan adatokhoz való jogosulatlan hozzáférés, mint az egészségügyi, pénzügyi, társadalombiztosítási számok és személyazonosításra alkalmas adatok.

A szervezeti erőfeszítések és befektetések ellenére az adatvédelmi incidensek sokszorosára nőttek, különösen az ázsiai és a csendes-óceáni térségben.[7] Az egyik nemzetközi kutatás[8] arra a következtetésre jutott, hogy a biztonsági szakemberek nem képesek időben azonosítani a biztonsági incidenseket és azok hatókörét, aminek következtében negatív hatást gyakorolnak a szervezetre. Ezeknek a mulasztásoknak a kezelése létfontosságú a szervezeti üzletmenet folytonossága és túlélése szempontjából.

A digitális eszközök használatával összefüggő bűncselekményekkel növekvő számuk miatt feltétlenül foglalkozni kell. A felhasználók tudatosságának tanulmányozása elengedhetetlen ahhoz, hogy kellően védekezni tudjanak a támadások ellen, illetve tudatosabban létezhessenek a digitális világban.

3. A szisztematikus irodalmi áttekintés módszertana

A vizsgált kutatási területen a releváns publikációk kiválasztásához beválasztási és kizárási kritériumokat határoztunk meg. Úgy döntöttünk, hogy nemcsak az ajánlott[9] magas színvonalú szakirodalomra összpontosítunk, hanem olyan folyóiratokat is bevonunk, amelyek nem szerepelnek magasan a nemzetközi folyóiratrangsorokban. Erre azért volt szükség, mert e folyóiratok némelyike az információbiztonság területére specializálódott (például *Computers & Security* és *Information Management & Computer Security*), és számos olyan témával foglalkozó publikációt tartalmaz, amelyek relevánsak a jelen irodalmi áttekintés szempontjából.

A biztonságtudatosság és az emberi tényező kapcsolatának átfogó áttekintése céljából internetes szakirodalom-keresést folytattunk le a PRISMA protokoll módszertana alapján a Google Scholar, a Scopus-adatbázis és a Web of Science (WoS)

[5] IBM: *Cost of a Data Breach Report* (2019).
[6] Capgemini Consulting: *Information Security Benchmarking 2017*. Report. (2017).
[7] Frost & Sullivan: *Cybersecurity Threats to Cost Organizations in Asia Pacific US$1.75 Trillion in Economic Losses* (2018. május 18.)
[8] PwC: *Information Security Breaches Survey* (2015).
[9] Jane Webster – Watson T. Richard: Analyzing the Past to Prepare for the Future: Writing a Literature Review. *Management Information Systems Quarterly,* 26. (2002), 2. 13–23; Jan vom Brocke – Christian Buddendick: Security Awareness Management – Konzeption, Methoden und Anwendung. In Otto K. Ferstl et al. (szerk.): *Wirtschaftsinformatik 2005.* Heidelberg, Physica, 2005. 1227–1246.

elektronikus tudományos adatbázis-keresők felhasználásával. Az említett adatbázisok kiválasztását és használatát a következő tényezők indokolták:

A Google Scholars hatalmas adatbázissal rendelkezik, mivel nyilvános, és rengeteg, nem csak indexált folyóiratból származó tanulmányt tartalmaz(hat).

A Web of Science (WoS) esetében éppen fordítva van, mivel magas színvonalú, de nagyon korlátozott számú publikációval rendelkezik.[10]

A Scopus minőségi folyóiratokat tartalmaz, amelyek kiterjedt publikációs készletet fednek le.

Több tanulmány[11] is bizonyítja, hogy a Google Scholar számos témakörben lényegesen több hivatkozást és publikációt eredményez, mint a WoS és a Scopus, illetve mind a WoS-, mind a Scopus-adatbázisokban fellelhető publikációkat is tartalmazza. Ez azt jelenti, hogy az említett két adatbázis eredményeinek nagy arányát a Google Scholar is megtalálja, listázza.

Az internetes keresés a „security awareness" kifejezés segítségével történt, amelynek a keresett irodalom címében, absztraktjában vagy kulcsszavaiban kellett megjelennie.

Az egyszerűsítés kedvéért csak angol nyelven írt anyagok képezték a keresés fókuszpontját, illetve kizárólag a tudományos folyóiratcikkek (a könyvfejezetek vagy a teljes könyvek és a konferenciaanyagok nem képezték az elemzendő adatbázis részét). A releváns cikkek kiválasztásában a Covidence online szoftver nyújtott segítséget. Azokat a publikációkat kiszűrtük, amelyek elsősorban nem az emberi tényező és a biztonságtudatosság témakörével foglalkoznak.

A szisztematikus szakirodalmi áttekintés főbb kutatási kérdései a következők:

1. Milyen tendencia figyelhető meg a biztonságtudatossági kutatásokban?
2. Melyek a biztonságtudatosság-kutatások főbb eredményei az emberi tényező kapcsán?

3.1. Keresési és kiválasztási stratégia

A szakirodalom gyűjtése 2021 májusában zajlott. A szisztematikus irodalmi áttekintések a szakirodalomból nyert információk tudományos módszerekkel történő szintézisei, amelyek részletes, alapos kutatómunka alapján tartalmazzák a kiválasztott adatbázisokban megjelent tudományos eredményeket egy adott témával kapcsolatban.[12]

A cikkek beazonosítása, kiválasztása és elemzése az alábbi lépések mentén történt, a módszer lépéseit az 1. ábra mutatja be.

Adatbázisok: a vizsgálatba a Google Scholar, a Web of Science és a Scopus adatbázisokban megtalálható cikkek szolgáltak a keresés alapjául.

[10] Sandeep Kumar Sood – Navin Kumar – Munish Saini: Scientometric Analysis of Literature on Distributed Vehicular Networks: VOSViewer Visualization Techniques. *Artificial Intelligence Review,* (2021), 1–33.

[11] Alberto Martín-Martín et al.: Google Scholar, Web of Science, and Scopus: A Systematic Comparison of Citations in 252 Subject Categories. *Journal of Informetrics,* 19. (2018), 4. 1160–1177; Jean-François Gehanno – Laetitia Rollin – Stefan Darmoni: Is the Coverage of Google Scholar Enough to be Used Alone for Systematic Reviews. *BMC Medical Informatics and Decision Making,* 13. (2013), 7. 1–5.

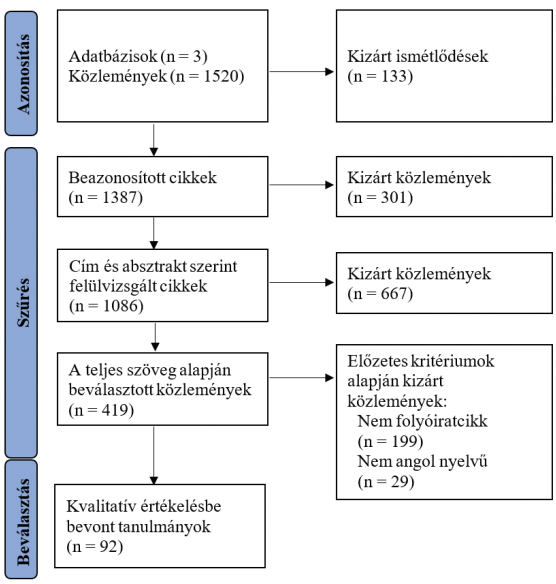
[12] Kamarási Viktória – Mogyorósy Gábor: Szisztematikus irodalmi áttekintések módszertana és jelentősége. Segítség a diagnosztikus és terápiás döntésekhez. *Orvosi Hetilap,* 156. (2015), 38. 1523–1531; Matthew J. Page et al.: The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. *British Medical Jorunal,* 372. (2021), n71.

A keresés kulcsszavának kiválasztása: az elemzés során az alábbi kifejezést alkalmaztuk: biztonságtudatosság („security awareness"). Mivel a felsorolt adatbázisokban főként angol nyelvű publikációk találhatók, így a kereséshez a kulcsszó angol nyelvű változatát használtuk, amelyet idézőjelek használata mellett alkalmaztunk, ezzel is minimalizálva a keresési feltételeknek nem megfelelő találatok számát. Mivel a kutatási terület legújabb eredményeinek elemzése a jelen tanulmány célja, ezért az elmúlt kilenc évben publikált, angol nyelven íródott és lektorált folyóiratcikkek képezték a fókuszt. Az online adatbázisokban lefolytatott keresés 1520 találatot eredményezett a korábban említett kifejezésre.

Kizáró kritériumok összegyűjtése: ismétlődéseket, biztonságtudatosság hatásain kívül eső tanulmányokat, nem a humán faktorra vonatkozó biztonságtudatosságot mérő, illetve az azt befolyásoló tényezőket vizsgáló cikkeket, a folyamatban levő kutatásokat, a biztonságtudatosság technológiai, illetve oktatási oldalról megközelítő tanulmányokat, valamint a 2012 előtt, illetve 2020 után publikált elemzéseket, továbbá a nem elérhető értekezéseket kizáró kritériumokként fogalmaztuk meg. A cím, az absztrakt és a kulcsszavak szűrése során 133 ismétlődést és 301 témán kívül eső publikációt azonosítottunk. Az ismétlődések esetében olyan publikációkról van szó, amelyek többször fordultak elő, aminek oka abban keresendő, hogy három különböző adatbázisból kérdeztük le az adatokat.

Az átvizsgálás során beválogatott közlemények kiválasztása: a kizáró kritériumok alapján kiszűrt publikációk eltávolítása után 419 cikk maradt a teljes vizsgálatra.

A kvalitatív értékelésben részt vevő publikációk kiválasztása: a teljes átvizsgálás során 92 cikket választottunk ki, amelyek a minőségi értékelés alapját képezték.



1. ábra

A szisztematikus irodalmi áttekintés folyamatábrája

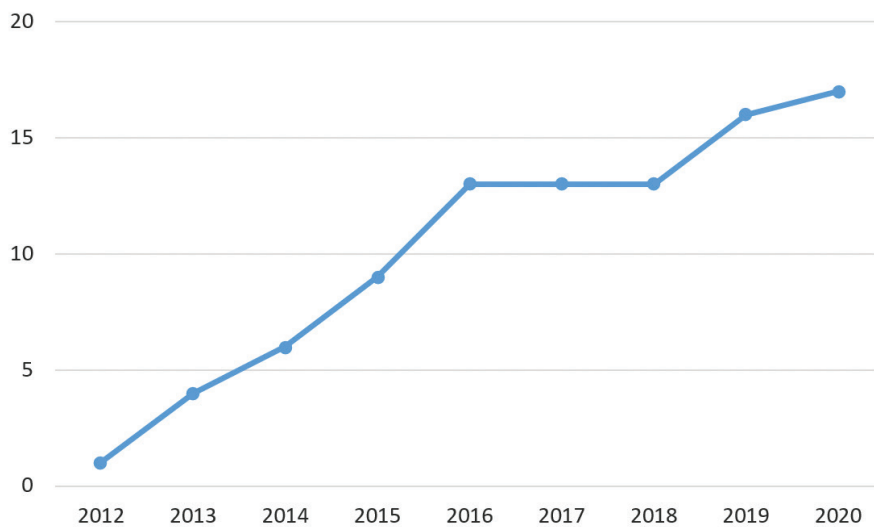
Forrás: a szerzők szerkesztése PRISMA ajánlás alapján

3.2. Adatkinyerés folyamata

A kiválasztott cikkek kvalitatív értékelése után az adatok kiválasztása és kódolása során rögzítettük az alapvető információkat, mint a szerzők neve, az első szerző országa, a publikálás éve, a folyóirat megnevezése, a publikáció nyelve. Ezt követte a témában megjelent közlemények vizsgálata területi eloszlás és megjelenési év alapján. Majd a megjelent publikációk kivonatának átvizsgálása, amely során a publikációkban alkalmazott kutatási módszerek feltárása történt. A beazonosított cikkek áttekintése után azokat az empirikus eredményeket rögzítettük, amelyek kapcsolatban állnak az emberi tényezővel.

4. A szisztematikus irodalmi áttekintés eredményei

A fejezet célja meghatározni a téma elhelyezkedését és beágyazottságát a nemzetközi irodalomban. A biztonságtudatosság humán aspektusait vizsgáló szakirodalmak köre nagymértékben növekszik, amint azt a 2. ábra is mutatja. A kvalitatív elemzésbe beválasztott cikkek alapján a vizsgált kilencéves időszakban évről évre növekedett a témában megjelent publikációk száma. A növekedés olyan mértékűvé vált az elmúlt években, hogy a vizsgált tanulmányok fele a vizsgált időszak utolsó három évében jelent meg, továbbá a téma beágyazottságára növekvő trend jellemző. A téma irodalmának nagy részét az informatikai és gazdasági-menedzsment folyóiratok közlik, azonban oktatás tematikájú területek is képviseltetik magukat.



2. ábra

Az elemzett cikkek számának alakulása 2012–2020 között

Forrás: a szerzők szerkesztése a minta adatai alapján

A biztonságtudatosság kapcsán keletkező kutatások tekintetében az Egyesült Államok, Törökország és Ausztrália emelkedik ki a publikációk számát tekintve (1. táblázat), ezt követi az Egyesült Királyság. Az elemzésekben vizsgált országok megjelenésének számossága azt mutatja, hogy a nemzetközi irodalomban az Egyesült Államok mellett Európa és Ázsia is jelentős figyelmet fordít a témára. Az eredményekből az is látható, hogy számos fejlődő ország igyekszik a biztonságtudatosságot és az emberi tényező kapcsolatát minél jobban megérteni. Azonban szakirodalmi publikációkat figyelembe véve az látható, hogy a közép-európai, kelet-európai, dél-amerikai és közép-ázsiai régiók a témában nem, vagy kis mértékben végeznek kutatásokat.

1. táblázat

Az elemzett országok 10 legtöbbet publikált eleme

Forrás: a szerzők szerkesztése a minta adatai alapján

	Ország	**N**
1.	USA	13
2.	Törökország	9
3.	Ausztrália	9
4.	UK	7
5.	Malajzia	6
6.	Dél-afrikai Köztársaság	5
7.	Horvátország	3
8.	Indonézia	3
9.	Dél-Korea	3
10.	Svédország	2

A teljesség igénye nélkül a következőkben bemutatjuk a főbb kutatási eredményeket a vizsgált szakirodalomból, amelyet a 2. táblázat foglal össze. A táblázatban az adott empirikus megállapításokat az elemzett publikációkban előforduló gyakorisága alapján tüntettük fel, a táblázat harmadik oszlopa az adott megállapítással foglalkozó cikkek számát jelöli.

A nemzetközi szakirodalom kutatási eredményeit áttekintve az látható, hogy a kutatók számos aspektusból igyekeznek a témában megközelíteni a biztonságtudatosságot befolyásoló emberi tényezőket. A legtöbb kutatás (29 db) az emberek szociodemografikus jellemzőire fókuszál, mint a nem, a kor, a jövedelem vagy az iskolázottság. E mellett még nagy hangsúlyt kapott a személyiségjegyek (16 db) vizsgálata is, mint hogy az adott illető mennyire introvertált, miként kezeli a stresszt és mennyire rugalmas. A kutatásba beválasztott publikációk között vannak olyanok is, amelyek jelenleg még a kevésbé vizsgált megközelítések táborába tartoznak, ilyen a biztonságtudatosság digitális írástudással való kapcsolata (8 db), valamint a közösségimédia-felületek használatához köthető jelenség, a FoMO *(fear of missing out)* befolyásoló hatása is (1 db).

2. táblázat

A vizsgált szakirodalom jelentősebb eredményei

Forrás: a szerzők szerkesztése a minta adatai alapján

	Empirikus megállapítások	**N**
1	A demográfiai (kor, nem, iskolai végzettség, lakhely, foglalkozás, munkában eltöltött évek száma) tényezők hatással vannak az egyén biztonságtudatossági szintjére.[13]	29
2	A személyiségjegyek összefüggésben állnak az egyén biztonságtudatosságával és magatartásával.[14]	14
3	A magasabb digitális írástudás magasabb biztonságtudatossággal jár együtt.[15]	14
4	A vállalaton belüli biztonsági irányelvek és a vállalati kultúra pozitív kapcsolatban állnak a biztonságtudatossággal.[16]	13
5	A biztonságtudatosságra vonatkozó tudás és magatartás eltérő.[17]	7
6	A felhasználók alábecsülik a biztonsági incidenseknek való kitettségüket, illetve nincsenek tisztában, hogy kihez fordulhatnak, ha megtörténik az incidens.[18]	6

[13] Atila Bostan – İbrahim Akman: Impact of Education on Security Practices in ICT. *Tehnički Vjesnik,* 22. (2015), 1. 161–168; Mehmet Tekerek – Adem Tekerek: A Research on Students' Information Security Awareness. *Online Submission,* 2. (2013), 3. 61–70; Christian Happ – André Melzer – Georges Steffgen: Trick with Treat – Reciprocity Increases the Willingness to Communicate Personal Data. *Computers in Human Behavior,* 61. (2016), 372–377.

[14] Ivana Borić Letica: Some Correlates of Risky User Behavior and ICT Security Awareness of Secondary School Students. *International Journal of Electrical and Computer Engineering Systems,* 10. (2019), 2. 85–89; Jaime Ortiz et al.: The Contradiction between Self-protection and Self-presentation on Knowledge Sharing Behavior. *Computers in Human Behavior,* 76. (2017), 406–416; Agata McCormac et al.: The Effect of Resilience and Job Stress on Information Security Awareness. *Information & Computer Security,* 26. (2018), 3. 277–289.

[15] Peter Sasvári – András Nemeslaki – Rauch Wolf: Old Monarchy in the New Cyberspace: Empirical Examination of Information Security Awareness among Austrian and Hungarian Enterprises. *Academic and Applied Research in Military and Public Management Science,* 14. (2015), 1. 63–78; Özgün Ünal: During COVID-19, Which is More Effective in Work Accident Prevention Behavior of Healthcare Professionals: Safety Awareness or Fatalism Perception? *Work,* 67. (2020), 4. 783–790.

[16] Lee Hadlington – Kathryn Parsons: Can Cyberloafing and Internet Addiction Affect Organizational Information Security? *Cyberpsychology, Behavior, and Social Networking,* 20. (2017), 9. 567–571; Ashleigh Wiley – Agata McCormac – Dragana Calic: More than the Individual: Examining the Relationship between Culture and Information Security Awareness. *Computers & Security,* 88. (2020), 101640; Duy Dang-Pham – Siddhi Pittayachawan – Vince Bruno: Why Employees Share Information Security Advice? Exploring the Contributing Factors and Structural Patterns of Security Advice Sharing in the Workplace. *Computers in Human Behavior,* 67. (2017), 196–206.

[17] Hanieh Yaghoobi Bojmaeh: Mediating Role of Information System Security Awareness in the Relationship between Self-Efficacy, Security Practice and Information System Security Behavior. *International Journal of Science and Engineering Applications,* 4. (2015), 6. 361–365; Zakaria I. Saleh – Ahmad Mashhour: Evaluating Security Awareness Impact on Perceived Risk and Trust: The Case of Social Networks. *International Journal in IT & Engineering,* 4. (2016), 5. 99–110.

[18] Awil Ahmed Mohamed – Othman Ibrahim – Mehrbakhsh Nilashi: The Security Awareness Framework for Social Network Sites Facebook: Case Study in Universiti Teknologi Malaysia. *Journal of Soft Computing and Decision Support Systems,* 2. (2015), 3. 1–8; Puspita Kencana Sari – Candiwan Candiwan: Measuring Information Security Awareness of Indonesian Smartphone Users. *Telkomnika,* 12. (2014), 2. 493–500; Adedayo Williams – Akanmu Semiu Ayobami: Relationship between Information Security Awareness and Information Security Threat. *International Journal of Research in Commerce,* IT & Management, 3. (2013), 8. 115–119.

	Empirikus megállapítások	N
7	Az egyén gondolkodásmódja és információmegosztási hajlandósága hatással van a biztonságtudatossági szintre.[19]	6
8	A biztonsági incidensekkel való tapasztalat pozitívan befolyásolja a biztonságtudatossági szintet.[20]	2
9	A FoMO *(fear of missing out)* negatívan befolyásolja az egyén információbiztonság-tudatosságát.[21]	1

A 3. táblázatban az elemzett 92 publikáció látható aszerinti bontásban, hogy mely célcsoportot, mintát vizsgálta, és mik voltak a kutatás céljai, továbbá milyen módszerrel vizsgálták azt, valamint hogy számszakilag mennyi publikáció tartozik az adott csoportba.

Az alábbi táblázatból láthatjuk, hogy a vizsgálatba bevont publikációk nagy része (40 db; 43,5%) a munkavállalókra vagy munkatapasztalattal rendelkező egyénekre fókuszált. Ezeknek a kutatásoknak a vizsgálati fókuszában áll az elemzett minta biztonságtudatossági szintjének feltérképezése, illetve hogy milyen tényezők (életkor, iskolázottság, jövedelem stb.) hatnak rá, hogyan lehet növelni ezt a szintet, milyen munkahelyi körülmények (vezetői stílus, vállalati policy) tudják szintén befolyásolni, valamint, hogy maga az egyén viselkedésmódja, gondolkodása, problémamegoldó képessége és szociális készségei miként határozzák meg. Mindezeknek a tesztelésére az alkalmazott módszerek között megtalálható a kérdőív alkalmazása, interjú lefolytatása, valamint a kísérlet.

A kutatók által másik gyakran vizsgált minta a tanulók csoportja (33 db), mind az egyetemisták (27 db), mind az általános és középiskolás (6 db) korosztály. A két csoport között feltűnő különbség, hogy míg a fiatalabb korosztály tagjait a biztonságtudatossági szintjük és a kapcsolódó viselkedésük vizsgálata kapcsán elemezték, addig az egyetemisták esetében a kockázatok mérséklése, valamint a használati szokások feltérképezése és a tudásmegosztási hajlandóság is a vizsgálat tárgyát képezte.

Érdekességként megemlítendő, hogy a mobil-, illetve okostelefon-használók körében végzett kutatások száma a legalacsonyabb (4 db) a vizsgált mintában, valamint csak az egyének biztonságtudatossági szintjének mérésére koncentrál, amelyet kérdőívvel vizsgáltak.

[19] Gizem Öğütçü – Özlem Müge Testik – Oumout Chouseinoglou: Analysis of Personal Information Security Behavior and Awareness. *Computers & Security,* 56. (2016), 83–93; Charlette Donalds – Kweku-Muata Osei-Bryson: Cybersecurity Compliance Behavior: Exploring the Influences of Individual Decision Style and Other Antecedents. *International Journal of Information Management,* 51. (2020), 102056; Wasim Qazi – Syed Ali Raza – Komal Akram Khan: The Contradiction between Self-protection and Self-presentation on Knowledge Sharing Behaviour: Evidence from Higher Education Students in Pakistan. *International Journal of Knowledge and Learning,* 13. (2020), 3. 246–271.

[20] Pelin Bolat – Gizem Kayişoğlu: Antecedents and Consequences of Cybersecurity Awareness: A Case Study for Turkish Maritime Sector. *Journal of ETA Maritime Science,* 7. (2019), 4. 344–360; Bartlomiej Hanus – John C. Windsor – Yu Wu: Definition and Multidimensionality of Security Awareness. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems,* 49. (2018), 49. 103–133.

[21] Lee Hadlington – Jens Binder – Natalia Stanulewicz: Fear of Missing Out Predicts Employee Information Security Awareness Above Personality Traits, Age, and Gender. *Cyberpsychology, Behavior, and Social Networking,* 23. (2020), 7. 459–464.

3. táblázat

A vizsgált szakirodalom kutatási céljai és vizsgált mintái

Forrás: a szerzők szerkesztése a minta adatai alapján

Minta	Kutatási célok	Módszer	N
munkavállalók	biztonságtudatosság szintjének mérése, illetve az azokra ható tényezők biztonságtudatosságot mérő eszköz létrehozása, tesztelése biztonságtudatosság növelését célzó programok, tréningek hatása a biztonságtudatosságra a munkahelyi környezet hatása a biztonságtudatosságra az egyén személyiségjegyei, kockázatvállalási hajlama miként befolyásolja a biztonságtudatosságot okoseszközök használatához kapcsolódó viselkedés megismerése információbiztonsági tudásmegosztási hajlandóság mérése	kérdőív, interjú, kísérlet	40
egyetemisták	információbiztonsági kockázatok mérséklése, lehetőségeinek azonosítása biztonságtudatosság szintjének mérése, illetve az azokra ható tényezők a biztonságtudatosságról alkotott elképzelések feltárása biztonságtudatosságot mérő eszköz létrehozása, tesztelése információbiztonsági tudásmegosztási hajlandóság mérése digitális/okoseszközök használati mintázata okoseszközök használatához kapcsolódó viselkedés megismerése	kérdőív	27
lakosság vagy vegyes csoport	biztonságtudatosság szintjének mérése, illetve az azokra ható tényezők biztonságtudatosságot mérő eszköz létrehozása, tesztelése biztonságtudatosság növelését célzó programok, tréningek hatása a biztonságtudatosságra	kérdőív, kísérlet	9
általános vagy középiskolás tanulók	biztonságtudatosság szintjének mérése, illetve az azokra ható tényezők okoseszközök használatához kapcsolódó viselkedés megismerése	kérdőív	6
közösségimédia-felhasználók	biztonságtudatosság szintjének mérése, illetve az azokra ható tényezők biztonságtudatosságot mérő eszköz létrehozása, tesztelése közösségimédia-oldalak használatához köthető kockázatok észlelésének mérése információbiztonsági, tudásmegosztási hajlandóság mérése	kérdőív	6
mobiltelefon-használók	biztonságtudatosság szintjének mérése, illetve az azokra ható tényezők	kérdőív	4

5. Következtetések

Jelen kutatás célja a biztonságtudatosság szisztematikus áttekintése volt. A tanulmány azt is megvizsgálta, hogy a biztonságtudatosság és az ember kapcsolatát mely országok kutatják a legnagyobb részben, valamint hogy miként változott a kutatási téma az elmúlt években. Figyelembe véve a tanulmányban bemutatott empirikus

irodalmat és eredményeit, az látható, hogy az egyén biztonságtudatosságát számos tényező befolyásolhatja. Ezek a befolyásoló tényezők lehetnek a szociodemografikus tényezők, mint a nem, a kor, az iskolázottság, vagy a jövedelem, lakhely, azonban számos olyan tényező is akad, amelyek kevésbé egzaktak, illetve azok meghatározása, mérése sem egyszerű. Egyrészt ilyen az egyén attitűdje, én-hatékonysága és egyéb más személyiségjegyek, vagy akár maga a szervezeti kultúra. Azonban nem árt figyelembe venni, hogy e befolyásoló tényezők hatása régiónként, kultúránként változhat.

A biztonságtudatosságot befolyásoló emberi tényezők és az ezt vizsgáló kutatások feltérképezésére azért volt szükség, mert így képet kaphatunk a tématerület aktuális állásáról, illetve eredményeiről. Ezáltal kirajzolódhat előttünk, hogy mik azok a tényezők, amelyekre egy-egy tréning, vagy a biztonságtudatosság felmérése során érdemes hangsúlyt fektetni. Másik szempontból pedig hozzájárul a biztonságtudatosság és a már kapcsolódó társtudomány-területek feltérképezéséhez, vagy akár egy teljesen új megközelítési módon, más tudományterületről érkező kutatást vezethet elő. Ezt alapul véve a kutatás következő szakaszában érdemes lehet megvizsgálni a biztonságtudatossággal foglalkozó publikációk esetében kialakult hálózatokat is mind a kutatói együttműködések, hivatkozások, mind a kulcsszavak tekintetében.

Továbbá megfontolandó a következő kutatások során más adatbázisokat is bevonni a szélesebb körű ismeretek feltérképezésére, valamint az egyes publikációk közötti kapcsolatok feltérképezésére is.

6. Összefoglalás

Ebben a tanulmányban a PRISMA-módszertant alkalmaztuk, amely során a kutatás célja volt többek között a minél szélesebb és alaposabb összegyűjtése a fókuszt képező tanulmányoknak. Annak ellenére, hogy az elemzés főként a nemzetközi adatbázisokra koncentrált, illetve a folyóirat-publikációkra, és ezáltal biztosítva van a bevont tanulmányok minősége, a vizsgált minta alacsony száma miatt felvetődhet a kérdés, érdemes volt-e ilyen szigorú megkötéseket alkalmazni. Ezt figyelembe véve a jövőre nézve érdemes megfontolni a szigorú kritériumok enyhítését, azaz a konferenciatanulmányok és más adatbázisok bevonását, ezáltal biztosítva a szélesebb nemzetközi palettát.

A szakirodalmi áttekintésben az elmúlt kilenc évben keletkezett empirikus tanulmányok felhasználásával történt a biztonságtudatosság emberi vonzatainak bemutatása. Az eredmények alapján elmondható, hogy bár a tématerület viszonylag új keletű, számos kutatás zajlik, amelyek mind igyekeznek csökkenteni az emberi hibából, óvatlanságból bekövetkező hibák mértékét, azáltal, hogy felfedik, milyen tényezők játszanak szerepet a mulasztások kialakulásában és bekövetkezésében.

Jelen kutatás korlátai közé sorolható, hogy a kutatott tématerület feltérképezését, annak helyzetét és az eddigi kutatási irányok, illetve eredmények megismerését célozta, ezáltal segítve a kiválasztott tématerületen való mélyebb kutatások előkészítését mind további tudománymetriai, mint pedig primer adatok elemzésével.

Bár a releváns szakirodalom felkutatására szigorú megközelítést alkalmaztunk, a felhasznált keresőkifejezés és az azonosított szakirodalom tekintetében vannak

korlátok. Csak angol nyelvű keresőkifejezést használtunk. Más nyelvű publikációkat nem vizsgáltunk. Ezenkívül a keresőkifejezést előre meghatároztuk, és nem induktív módon alakítottuk ki. A későbbiekre tekintettel egy második keresési folyamatot is kell végezni az irodalomelemzés során összegyűjtött kifejezésekkel, hogy további, a jelen szakirodalmi áttekintés szempontjából releváns szakírásokat találjunk. A nem lektorált publikációk (például könyvek, reportok) kizárásával csak az ellenőrzött minőségű publikációk kerültek be az elemzési folyamatba. Ennek ellenére úgy véljük, hogy a könyvek is tartalmazhatnak értékes konferenciaanyagokat, kutatásokat, amelyek hiányozhatnak ebből a szakirodalmi áttekintésből.

Felhasznált irodalom

Bada, Maria – Angela Sasse – Jason R. C. Nurse: *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?* In International Conference on Cyber Security for Sustainable Society. United Kingdom, Coventry University, 2015. 118–131.

Bianchi, Daniele – Onur Kemal Tosun: Cyber attacks and Stock Market Activity. *International Review of Financial Analysis,* 76. (2019), 101795. Online: https://doi.org/10.1016/j.irfa.2021.101795

Bojmaeh, Hanieh Yaghoobi: Mediating role of Information System Security Awareness in the relationship between Self-Efficacy, Security Practice and Information System Security Behavior. *International Journal of Science and Engineering Applications,* 4. (2015), 6. 361–365. Online: https://doi.org/10.7753/IJSEA0406.1006

Bolat, Pelin – Gizem Kayişoğlu: Antecedents and Consequences of Cybersecurity Awareness: A Case Study for Turkish Maritime Sector. *Journal of ETA Maritime Science,* 7. (2019), 4. 344–360. Online: https://doi.org/10.5505/jems.2019.85057

Borić Letica, Ivana: Some Correlates of Risky User Behavior and ICT Security Awareness of Secondary School Students. *International Journal of Electrical and Computer Engineering Systems,* 10. (2019), 2. 85–89. Online: https://doi.org/10.32985/ijeces.10.2.4

Bostan, Atila – İbrahim Akman: Impact of Education on Security Practices in ICT. *Tehnički Vjesnik,* 22. (2015), 1. 161–168. Online: https://doi.org/10.17559/TV-20140403122930

Capgemini Consulting: *Information Security Benchmarking 2017.* Report. (2017). Online: www.capgemini.com/consulting-de/wp-content/uploads/sites/32/2017/11/information-security-benchmark-2017.pdf

Dang-Pham, Duy – Siddhi Pittayachawan – Vince Bruno: Why Employees Share Information Security Advice? Exploring the Contributing Factors and Structural Patterns of Security Advice Sharing in the Workplace. *Computers in Human Behavior,* 67. (2017), 196–206. Online: https://doi.org/10.1016/j.chb.2016.10.025

Donalds, Charlette – Kweku-Muata Osei-Bryson: Cybersecurity Compliance Behavior: Exploring the Influences of Individual Decision Style and Other Antecedents. *International Journal of Information Management,* 51. (2020), 102056. Online: https://doi.org/10.1016/j.ijinfomgt.2019.102056

Frost & Sullivan: *Cybersecurity Threats to Cost Organisations in Asia Pacific US$1.75 Trillion in Economic Losses* (2018. május 18.). Online: https://news.microsoft.com/apac/2018/05/18/cybersecurity-threats-to-cost-organizations-in-asia-pacific-us1-75-trillion-in-economic-losses/

Gehanno, Jean-François – Laetitia Rollin – Stefan Darmoni: Is the Coverage of Google Scholar Enough to be Used Alone for Systematic Reviews. *BMC Medical Informatics and Decision Making,* 13. (2013), 7. 1–5. Online: https://doi.org/10.1186/1472-6947-13-7

Hadlington, Lee – Jens Binder – Natalia Stanulewicz: Fear of Missing Out Predicts Employee Information Security Awareness Above Personality Traits, Age, and Gender. *Cyberpsychology, Behavior, and Social Networking,* 23. (2020), 7. 459–464. Online: https://doi.org/10.1089/cyber.2019.0703

Hadlington, Lee – Kathryn Parsons: Can Cyberloafing and Internet Addiction Affect Organisational Information Security? *Cyberpsychology, Behavior, and Social Networking,* 20. (2017), 9. 567–571. Online: https://doi.org/10.1089/cyber.2017.0239

Hanus, Bartlomiej – John C. Windsor – Yu Wu: Definition and Multidimensionality of Security Awareness. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems,* 49. (2018), 49. 103–133. Online: https://doi.org/10.1145/3210530.3210538

Happ, Christian – André Melzer – Georges Steffgen: Trick with Treat – Reciprocity Increases the Willingness to Communicate Personal Data. *Computers in Human Behavior,* 61. (2016), 372–377. Online: https://doi.org/10.1016/j.chb.2016.03.026

IBM: Cost of a Data Breach Report (2019). Online: https://doi.org/10.1016/S1361-3723(19)30081-8

Kamarási Viktória – Mogyorósy Gábor: Szisztematikus irodalmi áttekintések módszertana és jelentősége. Segítség a diagnosztikus és terápiás döntésekhez. *Orvosi Hetilap,* 156. (2015), 38. 1523–1531. Online: https://doi.org/10.1556/650.2015.30255

Martín-Martín, Alberto – Enrique Orduna-Malea – Mike Thelwall – Emilio Delgado López-Cózar: Google Scholar, Web of Science, and Scopus: A Systematic Comparison of Citations in 252 Subject Categories. *Journal of Informetrics,* 19. (2018), 4, 1160–1177. Online: https://doi.org/10.1016/j.joi.2018.09.002

McCormac, Agata – Dragana Calic – Kathryn Parsons – Marcus Butavicius – Malcolm Pattinson – Meredith Lillie: The Effect of Resilience and Job Stress on Information Security Awareness. *Information & Computer Security,* 26. (2018), 3. 277–289. Online: https://doi.org/10.1108/ICS-03-2018-0032

Mohamed, Awil Ahmed – Ibrahim, Othman – Nilashi, Mehrbakhsh: The Security Awareness Framework for Social Network Sites Facebook: Case Study in Universiti Teknologi Malaysia. *Journal of Soft Computing and Decision Support Systems,* 2. (2015), 3. 1–8. Online: www.jscdss.com/index.php/files/article/view/33

Ortiz, Jaime – Shu-Hao Chang – Wen-Hai Chih – Chia-Hao Wang: The Contradiction Between Self-protection and Self-presentation on Knowledge Sharing Behavior. *Computers in Human Behavior,* 76. (2017), 406–416. Online: https://doi.org/10.1016/j.chb.2017.07.031

Öğütçü, Gizem – Özlem Müge Testik – Oumout Chouseinoglou: Analysis of Personal Information Security Behavior and Awareness. *Computers & Security,* 56. (2016), 83–93. Online: https://doi.org/10.1016/j.cose.2015.10.002

Page, Matthew J. – Joanne E. McKenzie – Patrick M. Bossuyt – Isabelle Boutron – Tammy C. Hoffmann – Cynthia D. Mulrow – Larissa Shamseer – Jennifer M. Tetzlaff – Elie A. Akl – Sue E Brennan et al.: The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. *British Medical Jorunal,* 372. (2021), n71. Online: https://doi.org/10.1136/bmj.n71

PwC: *Information Security Breaches Survey* (2015). Online: www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf

Qazi, Wasim – Syed Ali Raza – Komal Akram Khan: The Contradiction between Self-protection and Self-presentation on Knowledge Sharing Behaviour: Evidence from Higher Education Students in Pakistan. *International Journal of Knowledge and Learning,* 13. (2020), 3. 246–271. Online: https://doi.org/10.1504/IJKL.2020.10032181

Saleh, Zakaria I. – Ahmad Mashhour: Evaluating Security Awareness Impact on Perceived Risk and Trust: The Case of Social Networks. *International Journal in IT & Engineering,* 4. (2016), 5. 99–110.

Sari, Puspita Kencana – Candiwan Candiwan: Measuring Information Security Awareness of Indonesian Smartphone Users. *Telkomnika,* 12. (2014), 2. 493–500. Online: https://doi.org/10.12928/TELKOMNIKA.v12i2.2015

Sasvári, Péter – András Nemeslaki – Wolf Rauch: Old Monarchy in the New Cyberspace: Empirical Examination of Information Security Awareness among Austrian and Hungarian Enterprises. *Academic and Applied Research in Military and Public Management Science,* 15. (2015), 1. 63–78. Online: https://doi.org/10.32565/aarms.2015.1.6

Sood, Sandeep Kumar – Navin Kumar – Munish Saini: Scientometric Analysis of Literature on Distributed Vehicular Networks: VOSViewer Visualization Techniques. *Artificial Intelligence Review,* (2021), 1–33. Online: https://doi.org/10.1007/s10462-021-09980-4

Tekerek, Mehmet – Adem Tekerek: A Research on Students' Information Security Awareness. *Online Submission,* 2. (2013), 3. 61–70. Online: https://doi.org/10.19128/turje.181065

Ünal, Özgün: During COVID-19, Which is More Effective in Work Accident Prevention Behavior of Healthcare Professionals: Safety Awareness or Fatalism Perception? *Work,* 67. (2020), 4. 783–790. Online: https://doi.org/10.3233/WOR-203327

Vom Brocke, Jan – Christian Buddendick: Security Awareness Management – Konzeption, Methoden und Anwendung. In Otto K. Ferstl – Elmar J. Sinz – Sven Eckert – Tilman Isselhorst (szerk.): *Wirtschaftsinformatik 2005. Heidelberg,* Physica, 2005. 1227–1246. Online: https://doi.org/10.1007/3-7908-1624-8_64

Webster, Jane – Richard T. Watson: Analyzing the Past to Prepare for the Future: Writing a Literature Review. *Management Information Systems Quarterly,* 26. (2002), 2. 13–23.

Wiley, Ashleigh – Agata McCormac – Dragana Calic: More than the Individual: Examining the Relationship between Culture and Information Security Awareness.

Computers & Security, 88. (2020), 101640. Online: https://doi.org/10.1016/j.cose.2019.101640

Williams, Adedayo – Akanmu Semiu Ayobami: Relationship between Information Security Awareness and Information Security Threat. *International Journal of Research in Commerce,* IT & Management, 3. (2013), 8. 115–119.