HADMÉRNÖK
VÉDELEMINFORMATIKA

21. évfolyam (2026) 1. szám 77–92.
DOI: 10.32567/hm.2026.1.5

Répás József,[1] Berek László,[2] Oláh Norbert[3], Ujhegyi Péter,[4] Vinogradov Szergej[5]

Felsőoktatási hallgatók biztonságtudatossága a SAM-modell alapján[6]

Security Awareness among Higher Education Students Based on the SAM Model

Absztrakt

A digitális környezet gyors fejlődése és a kibertámadások növekvő száma a humán tényezőt a kiberbiztonság legsebezhetőbb elemévé tette. A felhasználók biztonságtudatosságának mérése ezért kulcsfontosságú a hatékony védelem és a célzott oktatási programok kialakítása szempontjából. Jelen kutatás a Security Awareness Model (Biztonságtudatossági Modell, SAM) bemutatására és empirikus tesztelésére vállalkozik, amely a korábbi Human Aspects of Information Security Questionnaire (HAIS-Q) modellt továbbfejlesztve a tudás–attitűd–viselkedés dimenziókat tíz szakmai terület mentén – többek között jelszóhasználat, webes biztonság, személyes adatok védelme vagy incidensmenedzsment – integrálja. A 2025 tavaszán végzett pilotkutatás 132 felsőoktatási hallgató válaszain alapult, és célja a modell konstrukcióinak megbízhatósági és érvényességi vizsgálata volt. Az eredmények alapján mindhárom komponens dimenziói szignifikánsan hozzájárulnak az általános biztonsági tudáshoz, ugyanakkor néhány tétel újrafogalmazása indokolt a mérési pontosság javítása

[1] Gábor Dénes Egyetem, e-mail: repas.jozsef@alverad.hu
[2] Óbudai Egyetem Egyetemi Könyvtár; Óbudai Egyetem Innováció Menedzsment Doktori Iskola, e-mail: berek.laszlo@uni-obuda.hu
[3] Debreceni Egyetem Informatikai Kar Adattudomány és Vizualizáció Tanszék, e-mail: olah.norbert@inf.unideb.hu
[4] Óbudai Egyetem Biztonságtudományi Doktori Iskola, e-mail: ujhegyi.peter@uni-obuda.hu
[5] Budapesti Metropolitan Egyetem, Módszertan Intézet, e-mail: szvinogradov@metropolitan.hu
[6] A cikk a TKP2021-NVA-05 számú projekt a Kulturális és Innovációs Minisztérium Nemzeti Kutatási Fejlesztési és Innovációs Alapból nyújtott támogatásával, a TKP 2021 pályázati program finanszírozásában valósult meg.

érdekében. A hallgatók a legnagyobb egyetértést a klasszikus biztonsági kockázatok (például ismeretlen USB-eszközök, adathalászat) terén mutatták, míg a szabályozási tudatosság és az új technológiákhoz kapcsolódó attitűdök esetében jelentős bizonytalanság tapasztalható. A SAM-modell alkalmas az információbiztonsági tudatosság komplex, többdimenziós feltárására, és alapot nyújt nagymintás, országos vizsgálatokhoz, amelyek hozzájárulhatnak a biztonsági kultúra fejlesztéséhez a felsőoktatásban és a társadalom szélesebb körében.

Kulcsszavak: információbiztonság, biztonságtudatosság, SAM-modell, HAIS-Q, felsőoktatás, pilotkutatás

Abstract

The rapid development of the digital environment and the increasing number of cyberattacks have made the human factor the most vulnerable element of cybersecurity. Measuring users' security awareness is crucial for adequate protection and developing targeted education programmes. This research aims to present and empirically test the Security Awareness Model (SAM), which builds on the previous HAIS-Q model by integrating the Knowledge–Attitude–Behaviour dimensions across ten professional areas, including password use, web security, personal data protection, and incident management. The pilot study, conducted in the spring of 2025, was based on the responses of 132 higher education students and aimed to test the reliability and validity of the model's constructs. Based on the results, all three component dimensions contribute significantly to general security knowledge, but some items need to be reworded to improve measurement accuracy. The students agreed on classic security risks (e.g., unknown USB devices, phishing). At the same time, there was significant uncertainty in regulatory awareness and attitudes toward new technologies. The SAM model is suitable for the complex, multidimensional exploration of information security awareness and provides a basis for large-scale, nationwide studies that can contribute to developing a security culture in higher education and society.

Keywords: information security, security awareness, SAM model, HAIS-Q, pilot research, higher education

Bevezetés

Az információbiztonság napjaink egyik kiemelt területe, mivel a technológia rohamos fejlődésével párhuzamosan a kibertámadások egyre gyakoribbak és súlyos pénzügyi, reputációs, sőt érzelmi károkat okozhatnak az érintett szervezeteknek és felhasználóknak.[7] Az információbiztonság tág értelemben magában foglalja mind a digitális, mind a nem digitális formában kezelt információk védelmét, míg a kiberbiztonság ennek azon részterületét jelenti, amely kifejezetten a hálózati és online környezetben megjelenő fenyegetésekre és védelmi mechanizmusokra fókuszál. A digitális társadalomban az információbiztonság szerepe felértékelődött, hiszen a technológiai

[7] Ahlan–Lubis–Lubis 2015.

védelem hatékonyságát egyre inkább az emberi tényező határozza meg. A mesterséges intelligencia, a felhőszolgáltatások, az online tanulási környezetek és az okoseszközök elterjedése soha nem látott mértékben tágította a digitális ökoszisztéma határait, miközben a kiberfenyegetések száma és komplexitása is rohamosan nő.

A nemzetközi szakirodalom egyre inkább rámutat arra, hogy a technológiai fejlesztések önmagukban nem elegendőek a kockázatok csökkentésére: a biztonságos működés kulcsa az információbiztonsági tudatosság fejlesztése és mérése. Az információbiztonsági tudatosság olyan komplex kompetencia, amely magában foglalja a biztonsági ismeretek meglétét, a fenyegetések felismerését, az azokhoz való attitűdöt, valamint a biztonságos viselkedés gyakorlati megvalósítását. A digitális korszakban az egyének – különösen a felsőoktatási hallgatók – nem csupán információfogyasztók, hanem aktív tartalom-előállítók és hálózati szereplők, akik döntéseikkel közvetlenül befolyásolják az egyetemi és intézményi vagy céges biztonsági környezet stabilitását.

Számos kutatás igazolja, hogy a biztonságtudatos viselkedés hiánya közvetlenül növeli az adatszivárgások, az adathalász-támadások és a jogosulatlan hozzáférések kockázatát.[8] Mindez különösen releváns a felsőoktatásban, ahol a digitális transzformáció, a távoktatás és az online kollaborációs platformok mindennapos használata új biztonsági kihívásokat teremt. A hallgatók nagy része a fiatal felnőtt korosztályba tartozik, akik magas technológiai jártassággal, de gyakran alacsony biztonsági tudatossággal rendelkeznek. Ennek következtében a felsőoktatási intézmények számára az információbiztonsági kultúra fejlesztése nem csupán technikai, hanem stratégiai oktatáspolitikai feladat is.

Ebben a kontextusban válik relevánssá a biztonságtudatosság mérésének modernizálása, olyan eszközökkel, amelyek képesek a felhasználók tudását, attitűdjeit és viselkedését egyaránt feltárni, és figyelembe veszik a környezeti, kulturális és intézményi hatásokat is. A SAM-modell ezen elvek mentén épül fel, és célja, hogy átfogóbb és korszerűbb képet adjon a felhasználók biztonságtudatossági szintjéről.[9]

Ebben a dinamikusan változó környezetben az információbiztonsági tudatosság kiemelt, mivel a humán tényező gyakran a leggyengébb láncszem, így a felhasználók biztonságtudatosságának szintje döntően befolyásolja a szervezetek és egyének védettségét. A biztonságtudatosság méréséhez hatékony módszerekre van szükség, hiszen csak így azonosíthatók a gyenge pontok és alakíthatók ki célzott védelmi stratégiák.

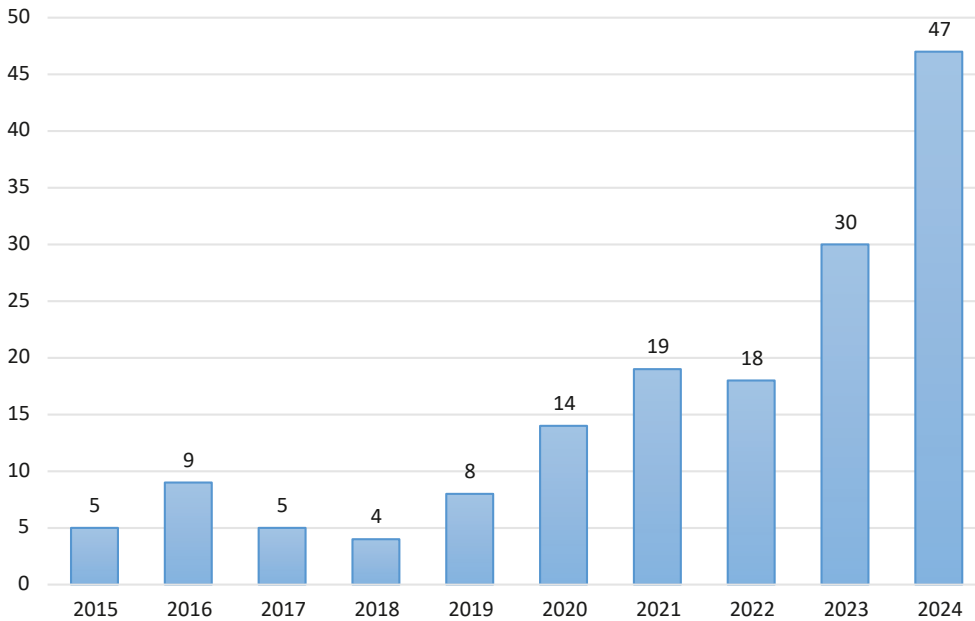
Tudományos megközelítés és a kapcsolódó modell

Az információbiztonsági tudatossági szint mérése hangsúlyos volt mind nemzetközi, mind hazai vonatkozásban az elmúlt évtizedekben. A témában megjelent kutatási eredmények, publikációk feltérképezését a Scopus adatbázis felületén végeztük el. A keresőkifejezésben kifejezetten a felsőoktatási környezetben végzett, az információbiztonsági tudatosságra irányuló felmérésekre voltunk kíváncsiak. A Scopusban alkalmazott, konkrét keresőkifejezésünk a következő volt:

[8] Parsons et al. 2017; Hong–Furnell 2021.
[9] Répás et al. 2024.

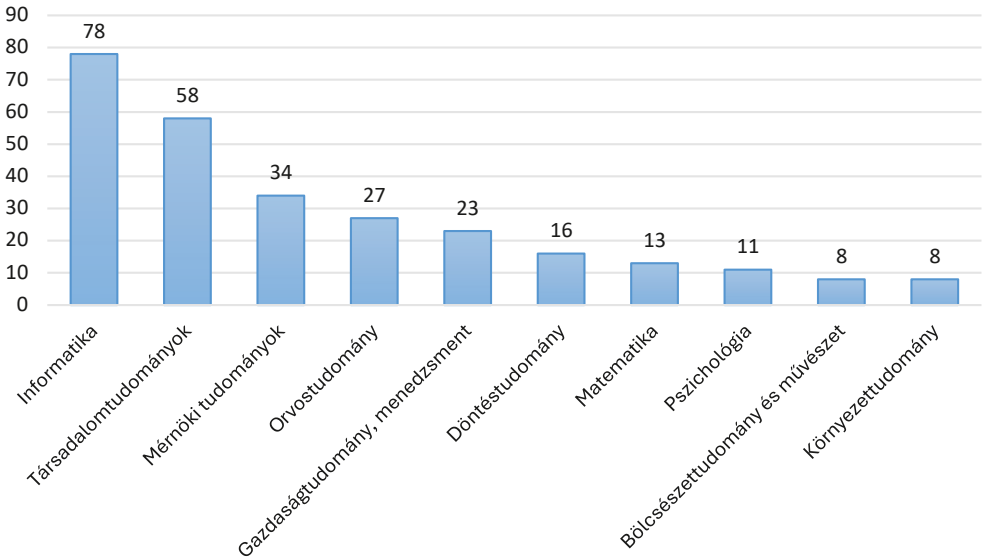
TITLE-ABS-KEY („information security" OR „cybersecurity" OR „data protection" OR „infosec") AND TITLE-ABS-KEY („awareness" OR „understanding") AND TITLE-ABS-KEY („survey" OR „questionn*") AND TITLE-ABS-KEY („higher education" OR „universit*" OR „college" OR „students") AND PUBYEAR > 2014 AND PUBYEAR < 2025 AND (LIMIT-TO (DOCTYPE,"ar") OR LIMIT-TO (DOCTYPE,"re")) AND (LIMIT-TO (LANGUAGE,"English"))

A kapott eredmény egyértelműen mutatja, hogy a témával kapcsolatos kutatások száma évről évre nő. Természetesen a tudományos kutatások színterei leginkább az egyetemek, felsőoktatási intézmények, így kézenfekvő, hogy hasonló felmérések a legegyszerűbben, leggyorsabban az egyetemi hallgatók bevonásával végezhetők el (1. ábra).



1. ábra: Kapcsolódó publikációk száma, 2015–2024, Scopus
Forrás: a szerzők szerkesztése

A publikációk szakterületi eloszlás szerinti vizsgálata igazolja, hogy a vizsgált terület multidiszciplináris megközelítésben is értelmezhető. A vizsgált folyóiratcikkek a legkülönbözőbb *subject area* besorolásba tartozó folyóiratokban jelentek meg. A 2. ábra a top 10 szakterületet mutatja be. Ebben is látható, hogy – természetesen – az informatika besorolású folyóiratok állnak az első helyen, de rögtön mögötte már a társadalomtudomány áll, sőt az üzleti tudományok is bekerült az első 5 közé.



2. ábra: Publikációk szakterület szerint, Scopus/Scimago
Forrás: a szerzők szerkesztése

A találatok közül a legtöbb citációval rendelkező 20 publikáció áttekintésével a méréshez használt eszközökről, a viselkedést befolyásoló fő tényezőkről, illetve a kutatások ajánlásairól is képet kaptunk.

A kutatások módszertani szempontból túlnyomórészt kvantitatív kérdőíves felmérésekre épültek,[10] kisebb részben vegyes módszertanú vizsgálatokra,[11] amelyek interjúkkal és fókuszcsoportokkal mélyítették el a hallgatói attitűdök megértését. A mérési keretek közül a legelterjedtebb a HAIS-Q – amely a tudás *(knowledge),* attitűd *(attitude)* és viselkedés *(behaviour)* összefüggéseit vizsgálja[12] –, valamint a tervezett viselkedés elmélete (*theory of planned behaviour,* TPB), amely az attitűd, a szubjektív norma és az észlelt viselkedéses kontroll kapcsolatát modellezi.[13]

A kutatások eredményei alapján az információbiztonsági viselkedést több, egymással összefüggő tényező befolyásolja. Az oktatási háttér és a szakterület fontos szerepet játszik: az informatikai és mérnöki képzéseken tanuló hallgatók információbiztonsági tudatossága és ismeretszintje szignifikánsan magasabb, mint más szakterületek hallgatóié. Ezt a különbséget részben a technikai ismeretek mélysége, részben pedig az adott képzési területeken nagyobb hangsúlyt kapó adatvédelem és információbiztonsági oktatás magyarázza.

A demográfiai tényezők szintén hatással vannak a tudatosságra: a férfi hallgatók és a városi környezetben tanulók jellemzően magasabb információbiztonsági

[10] Alqahtani 2022; Taha–Dahabiyeh 2021.
[11] Módné Takács – Pogátsnik 2024; Blažič–Blažič 2022.
[12] Parsons et al. 2017.
[13] Alanazi–Freeman–Tootell 2022.

tudatosságot mutatnak, mint női és vidéki társaik.[14] Ezek a különbségek arra utalnak, hogy a társadalmi és környezeti háttér is alakítja az információbiztonsággal kapcsolatos attitűdöket és viselkedést.

A személyiségvonások vizsgálata további fontos összefüggéseket tárt fel. A lelkiismeretesség, a barátságosság és a nyitottság pozitív kapcsolatban áll a biztonságosabb online viselkedéssel, ami azt jelenti, hogy az egyéni pszichológiai jellemzők befolyásolják, mennyire hajlamos valaki a biztonsági szabályok betartására és a kockázatok tudatos kezelésére.[15] A személyiség tehát meghatározó pszichológiai prediktornak tekinthető a biztonságtudatos magatartás kialakulásában.

Ezzel párhuzamosan az intézményi és helyzeti támogatásnak is jelentősége van. Az eredmények szerint a megfelelő intézményi háttér, a támogató környezet és a korábbi tréningek egyaránt javítják a hallgatók információbiztonsági tudatosságát.[16] A kutatások hangsúlyozzák, hogy a biztonsági magatartás nemcsak az egyéni döntésektől, hanem a felsőoktatási intézmény szervezeti kultúrájától is függ: a példamutató oktatói gyakorlat, az elérhető támogató infrastruktúra és a rendszeres képzések mind növelik a biztonságos viselkedés valószínűségét.

Végül az attitűdök és a viselkedési szándék is lényeges tényezőknek bizonyultak. Az attitűdök, a szubjektív normák és az észlelt viselkedéses kontroll – a TPB alapján – kimutathatóan befolyásolják a biztonságos viselkedésre irányuló szándékot.[17] Ugyanakkor a tényleges viselkedés gyakran csak részben követi a szándékot, ami rávilágít arra, hogy a szokások és a környezeti támogatás nélkülözhetetlenek ahhoz, hogy a tudás és a szándék ténylegesen biztonságtudatos cselekvéssé alakuljon.

A korábbi mérési megközelítések közül a legismertebb a HAIS-Q, amely a KAB-keretet alkalmazva vizsgálta a felhasználók biztonsági ismereteit, hozzáállását és viselkedését.[18] Bár a HAIS-Q széles körben használt és megbízható eszköz, a gyorsan változó technológiai és szabályozási környezetben több hiányosság is felszínre került. A klasszikus kérdőív ugyanis nem tudta teljes mértékben lefedni azokat a modern kihívásokat, amelyeket a felhőalapú szolgáltatások, a többfaktoros hitelesítés, a kollaborációs platformok vagy éppen a GDPR- és a NIS2-szabályozások teremtettek. Ezen hiányosságok kiküszöbölésére született meg a SAM-modell, amely a HAIS-Q alapjaira épít, ugyanakkor jelentősen modernizálja és kibővíti azt.

SAM-modell

A biztonságtudatosság mérésének szükségességét korábban a HAIS-Q-modell alapozta meg, amely a KAB-keretet használta a felhasználói biztonsági magatartás vizsgálatára. Ez a struktúra lehetővé teszi, hogy ne csak az ismeretek szintjét, hanem a belső motivációkat és a tényleges cselekvési mintákat is feltárjuk. Ugyanakkor a digitális környezet átalakulása (felhő, kollaborációs platformok, MFA, AI, szabályozások) indokolttá tette

[14] Hong–Furnell 2021; Aljohni et al. 2021.
[15] Shappie–Dawson–Debb 2020.
[16] Répás et al. 2024; Alharbi–Tassaddiq 2022; Al-Janabi – Al-Shourbaji 2016.
[17] Alanazi–Freeman–Tootell 2022.
[18] Parsons et al. 2017; Parsons et al. 2014; Parsons et al. 2013; McCormac et al. 2017.

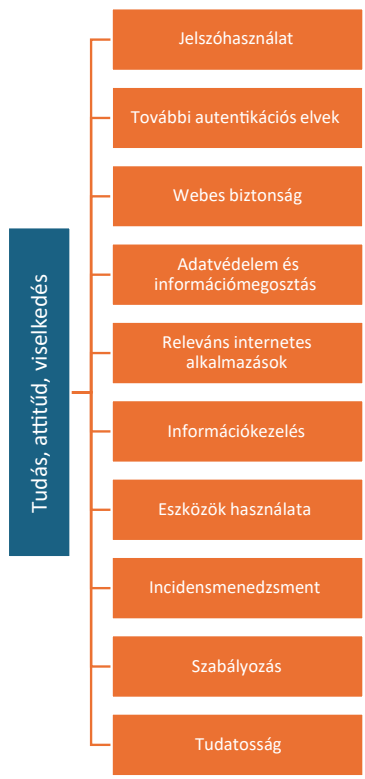
a modell kiterjesztését. A SAM ezért a HAIS-Q modernizált, kibővített változatának tekinthető, amely a kontingenciaelmélet szellemében alkalmazkodik a környezeti és technológiai változásokhoz. A SAM struktúrája alapvetően a tudás–attitűd–viselkedés (TAV) logikára épül. A modellben minden dimenziót három aspektusból vizsgálunk: egyrészt azt mérjük, hogy a válaszadók milyen ismeretekkel rendelkeznek az adott területen, másrészt feltárjuk a biztonsághoz kapcsolódó attitűdjeiket, végül pedig a tényleges cselekvéseket és viselkedési mintákat is rögzítjük. Ez a megközelítés lehetővé teszi, hogy ne csupán a tudás meglétét, hanem annak attitűdökön keresztüli átfordulását és gyakorlati alkalmazását is vizsgáljuk.[19]

A modell tíz szakmai dimenzió mentén közelíti meg a biztonságtudatosság mérését, amelyet a 3. ábra mutat be, és a kérdőívben szereplő tételek ezekre a dimenziókra épülnek. A többdimenziós szakmai felépítés jelentősége abban rejlik, hogy lehetővé teszi a biztonságtudatosság komplex, rendszerszintű értelmezését, azaz nem csupán az elszigetelt ismeretek meglétét vizsgálja, hanem feltárja az egyes szakmai területek közötti különbségeket és hiányosságokat is. A modell így alkalmas a kritikus tudáshiányok, a kockázatos attitűdök és a fejlesztést igénylő viselkedési minták azonosítására, valamint megalapozza a célzott, dimenzióspecifikus tudatosítási beavatkozások tervezését. A jelszóhasználat dimenziója a jelszavak létrehozásának, kezelésének és frissítésének gyakorlatát vizsgálja, valamint feltárja a jelszóválasztással kapcsolatos tipikus hibákat. A további autentikációs elvek dimenziója a modern hitelesítési gyakorlatokra koncentrál, különös tekintettel a többfaktoros hitelesítésre (MFA), amelyekre napjainkban példa az SMS-ben vagy mobilalkalmazásban kapott kódok és a biometrikus azonosítás alkalmazása. A webes biztonság dimenziója az internetböngészés során jelentkező fenyegetések kezelését vizsgálja, beleértve az adathalász-támadások felismerését, a biztonságos weboldalak (HTTPS) használatát és a gyanús letöltések elkerülését. A *privacy* és információmegosztás a személyes adatok és információk tudatos kezelésére irányul, különösen a közösségimédia-használat során.

Az internetszolgáltatások használata a felhőalapú platformok, az e-mail-rendszerek és a kollaborációs eszközök biztonságos használatát értékeli, hangsúlyozva a jogosultságkezelés és az adatmegosztás biztonsági kérdéseit. Az információkezelés a bizalmasság, integritás és rendelkezésre állás elveinek megvalósulását méri, kitérve az adattárolási, adatkezelési és titkosítási gyakorlatokra. Az eszközhasználat dimenziója a digitális eszközök védelmét vizsgálja, különös figyelmet fordítva a frissítések rendszeres elvégzésére, a vírusirtó és tűzfal használatára, valamint a saját eszközök munkahelyi használatának (*bring your own device,* BYOD – „hozd a saját eszközödet") biztonsági vonatkozásaira. Az incidensmenedzsment-dimenzió azt méri, hogy a válaszadók képesek-e felismerni a gyanús eseményeket, tudják-e, hogyan kell azokat jelenteni, és mennyire ismerik az incidensek kezelésére vonatkozó eljárásokat. A szabályozás dimenziója a kiberbiztonsági és adatvédelmi szabályok – különösen a GDPR és a NIS2 – ismeretét és gyakorlati alkalmazását vizsgálja. Végül a tudatosság dimenziója az általános biztonsági kultúrára és a humán tényezőkre fókuszál, mérve a kockázatészlelés szintjét és a tudatos magatartás jelenlétét, amelyet gyakran a *human firewall* koncepcióval írnak le.

[19] Répás et al. 2024; Bak et al. 2024; Berek et al. 2024; Répás et al. 2025.

A SAM újdonsága több dimenzióban is megnyilvánul. Elsőként: a modell holisztikus szemléletet képvisel, mivel nem csupán a technikai ismeretek szintjére korlátozódik, hanem a jogszabályi megfelelést, a felhasználói attitűdöket és a szervezeti kultúra szempontjait is integrálja. A SAM nemcsak az egyéni tudatosságot, hanem a tágabb társadalmi és intézményi környezethez való alkalmazkodást is képes így értékelni. Másodsorban a modell naprakészen követi a digitális környezet kihívásait, hiszen beépíti azokat a területeket, amelyek a legújabb technológiai trendekből fakadóan váltak fontossá. Ilyen például a felhőalapú szolgáltatások biztonsága, a mesterséges intelligencia által támogatott rendszerek használatának kockázatai, az IoT-eszközök elterjedése vagy a távmunkához kapcsolódóan megjelenő biztonsági kockázatok, amelyek új típusú sebezhetőségeket és adatvédelmi problémákat hoztak magukkal. Harmadrészt a SAM rugalmas és adaptív keretrendszert kínál, amely a kontingenciaelmélet alapján különböző szervezeti és társadalmi környezetekhez is illeszkedik, ezáltal nem statikus mérőeszközként, hanem folyamatosan fejleszthető modellként működik. Végül a SAM a KAB (tudás–attitűd–viselkedés) keretet magasabb szintre emeli: nem elszigetelt komponensekként kezeli a három tényezőt, hanem dinamikus kölcsönhatásban vizsgálja őket. Ez a komplexitás teszi lehetővé, hogy a SAM pontosabb, mélyebb és a gyakorlati kontextusban is jobban értelmezhető eredményeket adjon, mint a korábbi modellek.



3. ábra: A kutatás elméleti modellje
Forrás: a szerzők szerkesztése ***Répás*** *et al. 2024 alapján*

Eredmények

A 2025 tavaszán lebonyolított pilot-adatfelvétel célja az volt, hogy a felsőoktatási hallgatók körében tesztelje az információbiztonsági tudatosság mérésére szolgáló kérdőívet. A vizsgálat fókusza az elemek érthetőségének, megkülönböztető erejének és a válaszmegoszlások jellegzetességeinek feltárása volt, mielőtt a nagymintás, országos adatfelvétel megkezdődne. Az adattisztítás eredményeként a minta összesen 132 fő hallgatót foglalt magában, amely nagyságrendileg elegendő arra, hogy a kérdőív megbízhatóságát és belső logikáját ellenőrizze. Az adatfelvétel célja a kérdőív tételeinek kipróbálása és a statisztikai jellemzők feltárása volt. Az állításokat a válaszadók 1–6 fokozatú Likert-skálán értékelték (1 = egyáltalán nem ért egyet, 6 = teljes mértékben egyetért), külön „Nem tudom" opció nem volt.

A felsőoktatási hallgatói pilotminta főbb jellemzői

A minta szinte teljes egészében a fiatal felnőttek korcsoportját képviseli. A válaszadók többsége 19 és 22 év közötti: a 20 évesek (31,8%) és a 21 évesek (28,8%) adják a legnagyobb arányt. Az idősebb hallgatók (23–27 évesek) aránya alacsony (összesen ~ 6%), míg a 30 év feletti korosztály csak szórványosan fordul elő. Ez a megoszlás jól tükrözi a nappali tagozatos alapképzésben részt vevő hallgatók életkori szerkezetét, ugyanakkor a felsőoktatás teljes hallgatói populációjához képest alulreprezentált a mesterszakos (23 év feletti) korosztály. A nemek szerinti eloszlás jelentős férfitöbbséget mutat: a válaszadók 79,5%-a férfi, 18,2%-a nő, míg 2,3% nem adott választ. Ez eltér az országos felsőoktatási tendenciáktól, ahol jellemzően enyhe női többség figyelhető meg. A minta tehát az életkor tekintetében közelíti, a nemek arányában viszont eltéríti a felsőoktatási hallgatói populáció szerkezetét. A válaszadók döntő része városi környezetben él. A legnagyobb arányban megyei jogú városból érkeztek (36,4%), őket az „egyéb városok" követik (31,8%). A községekben vagy falvakban élők aránya 25,0%, míg a fővárosból mindössze 3,8% került a mintába. A mintát erősen dominálja az Észak-Alföld régió (73,5%), amely összefügg a mintavétel debreceni központjával. A többi régió marginális arányban szerepel: Észak-Magyarország (6,1%), Dél-Alföld (3,0%), valamint a dunántúli régiók, Pest és Budapest egyenként 2–3%-os arányban jelennek meg. Így az adatfelvétel nem országos lefedettséget, hanem inkább regionális próbavizsgálatot biztosított. A minta szerkezeti jellemzői közvetlenül hatással vannak az eredmények értelmezésére is. A fiatal, döntően alapképzésben tanuló hallgatók digitális környezete és tapasztalati háttere magyarázza, hogy bizonyos kérdéskörökben határozott válaszokat adtak, más területeken viszont inkább bizonytalanságot jeleztek.

A biztonságtudatosság mintázatai a hallgatói pilotmintában

Azokban az esetekben merülhet fel bizonytalanság, ha a válaszadók jelentős része a skála középső értékeit (3 vagy 4) választja. A felmérés eredményei szerint néhány

szakmai kérdésnél a középértékválaszok aránya meghaladta az 50%-ot, ami a hallgatók bizonytalanságát vagy kialakulatlan attitűdjeit tükrözi. Ezek a témakörök a szabályozási kérdések és az új technológiák, amelyek terén a hallgatók válaszaiban bizonytalanság mutatkozott meg, például az előírások és szabályok ismeretét mérő tételnél (átlag: 3,41; szórás: 1,01). Ezzel szemben a klasszikus információbiztonsági helyzetekben határozott konszenzus figyelhető meg. A legnagyobb egyetértést az a kijelentés váltotta ki, hogy a hallgatók nem csatlakoztatnának nyilvános helyen talált USB-pendrive-ot a számítógépükhöz (átlag: 5,61; szórás: 0,70). Magas értéket kapott továbbá az a megállapítás is, hogy a mesterségesintelligencia-alapú alkalmazások adatbiztonsági kockázatokat hordoznak (átlag: 5,36; szórás: 0,77). Ezzel szemben a legkisebb egyetértést olyan állítások váltották ki, amelyek a felhasználói tudatosság és a képzés szerepéhez, illetve a technológiai környezet biztonságának megítéléséhez kapcsolódnak. A hallgatók körében alacsony volt a támogatottsága annak, hogy mindig átnéznék a használati feltételeket és szabályzatokat (átlag: 2,84), vagy hogy az információbiztonsági képzések érdemben segítenének az online veszélyek felismerésében (átlag: 2,78). Gyenge egyetértés mutatkozott a törölt adatok visszaállíthatóságának problémáját (átlag: 2,74) és különösen a felhőben tárolt adatok biztonságának kérdését illetően (átlag: 1,92). Mindez arra utal, hogy míg a hallgatók a klasszikus biztonsági kockázatokat egyértelműen felismerik, addig a szabályozási tudatosság, a képzések hatékonysága és az új technológiákhoz kapcsolódó attitűdök terén nagy fokú bizonytalanság és széttartás tapasztalható.

Az itemek többségénél a szórás alacsony vagy közepes szintet mutatott, ami a válaszadók közötti konszenzus jele. Ugyanakkor néhány állításnál szokatlanul magas szórás jelentkezett, ami a hallgatói közösség megosztottságát tükrözi. Ilyen például az a kijelentés, miszerint a bizalmas adatokat tartalmazó nyomtatványok ugyanolyan módon megsemmisíthetők, mint azok, amelyek nem tartalmaznak bizalmas adatokat (szórás: 1,61). Ez jól jelzi, hogy a hallgatók egy része tisztában van az iratmegsemmisítés sajátos biztonsági követelményeivel, míg mások ezt nem tekintik lényeges különbségnek. Hasonlóképpen magas szórás mutatkozott a törölt adatok visszaállíthatóságáról szóló tételnél (szórás: 1,59), ami arra utal, hogy a válaszadók eltérően ítélték meg az adattörlés és a formázás biztonsági kockázatát. A legnagyobb megosztottság azonban a jelszavak böngészőben való tárolásának megítélésében mutatkozott („Az eszközeim böngészőjében nem mentem el a jelszavaimat", szórás: 1,69). E tétel esetében világosan elkülönültek azok, akik biztonsági kockázatként értékelik a böngészőben mentett jelszavakat, és azok, akik a kényelmi szempontokat előtérbe helyezve elfogadják ezt a gyakorlatot. Ezek a magas szórású tételek különösen fontosak a pedagógiai beavatkozások szempontjából, mivel rámutatnak azokra a területekre, ahol a tudatosítás és az egységes minimumszint kialakítása a hallgatói közösségben elengedhetetlen.

A tudás modellelem empirikus érvényessége

Jelen fejezetben az információbiztonsági tudatosság mérésére kidolgozott SAM-modell tudás komponensének empirikus érvényességét vizsgáljuk. A teljes modell három fő komponensből épül fel, azonban a cikkben a tudás dimenziót mutatjuk be részletesen és teszteljük statisztikailag. A tudás komponenst a SAM elméleti keretrendszerének megfelelően hierarchikus, két szintből álló formatív mérési struktúrában operacionalizáltuk, amelynek empirikus vizsgálatát a következő alfejezetekben mutatjuk be. A hierarchikus felépítés lehetővé teszi, hogy az egyes szakmai dimenziók külön-külön is értelmezhetők legyenek, miközben együttesen alkotják az általános információbiztonsági tudás konstrukcióját.

Elsődleges formatív szint (indikátorok → dimenziók)

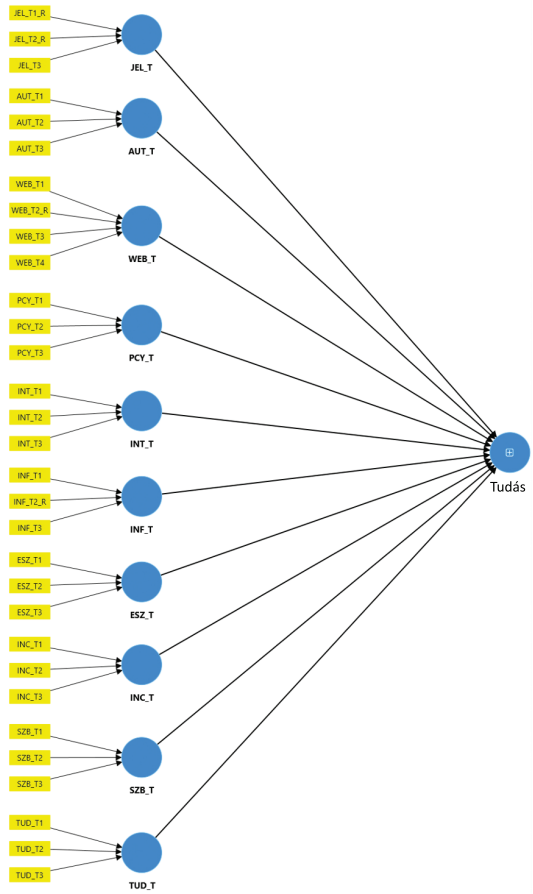
Az információbiztonsági tudást tíz különálló dimenzió mentén ragadtuk meg. Ezek a dimenziók a jelszóhasználathoz, az autentikációhoz, a webes biztonsághoz, az adatvédelemhez és információmegosztáshoz, a releváns internetes alkalmazások használatához, az információkezeléshez, az eszközhasználathoz, az incidensmenedzsmenthez, a szabályozási ismeretekhez, valamint az általános tudatossághoz kapcsolódnak (JEL_T, AUT_T, WEB_T, PCY_T, INT_T, INF_T, ESZ_T, INC_T, SZB_T, TUD_T). Minden dimenziót három, Likert-skálán mért állítás reprezentált, amelyek az adott tudásterület különböző aspektusait ragadták meg. Az indikátorok formatív módon járultak hozzá az adott dimenzió kialakításához, vagyis a dimenzió értékét nem tükrözték, hanem annak konstitutív elemeiként építették fel a konstrukciót.

Másodlagos formatív szint (dimenziók → tudás)

Az általános „tudás" konstrukciót a tíz dimenzió kompozit módon alkotja meg, amelyeket a 4. ábra szemléltet. Az egyes dimenziók nem feltétlenül korrelálnak egymással, de együtt képezik a biztonságtudatos gondolkodás alapját. Így az „általános tudás" nem egy egységes, homogén képesség, hanem több, egymást kiegészítő terület eredője.

Az adattisztítás eredményeként kapott adatállományból került sor a tudás komponens elméleti modelljének empirikus érvényességi vizsgálatára, a SmartPLS 4 szoftver[20] alkalmazásával, PLS-alapú strukturális egyenletmodellezés (PLS-SEM) módszerével.

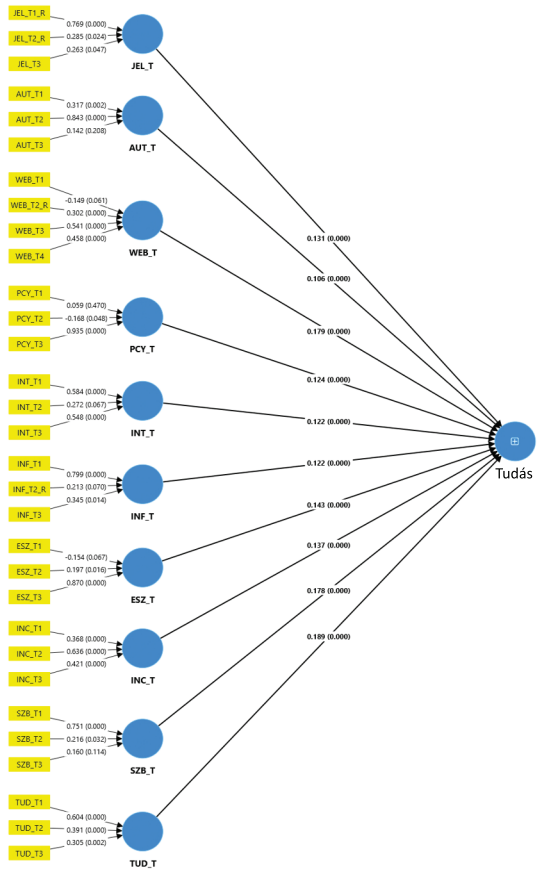
[20] A SmartPLS 4 egy grafikus felülettel rendelkező PLS-SEM (partial least squares structural equation modeling) szoftver, amely látens változós mérési és strukturális modellek elemzésére szolgál.



4. ábra: A tudás modellelem hierarchikus felépítése
Forrás: a szerzők szerkesztése

Az „R" jelölés az indikátorok (állítások) kódjában azt jelöli, hogy az adott állítás ellentétes tartalmú a dimenzió többi tételéhez képest, így a tudás konstruktum megfelelő mérhetősége érdekében inverz módon került be a modellbe. A tudás modellelem empirikus vizsgálata (5. ábra) eredményeként megállapítható, hogy a modell minden dimenziója szignifikáns súllyal járul hozzá az általános „tudás" konstrukcióhoz (minden út együttható esetében: $p < 0{,}001$), ami azt jelenti, hogy a dimenziók empirikusan megalapozottan képezik az általános tudáskomponenst.

Ugyanakkor néhány indikátor (például PCY_T1, WEB_T1, AUT_T3) alacsony vagy nem szignifikáns hozzájárulást mutatott a saját dimenziójához, ami a mérési modell finomításának szükségességére hívja fel a figyelmet.



5. ábra: A tudásmodell és annak aldimenziói empirikus érvényessége
Forrás: a szerzők szerkesztése

A tudás – adatvédelem és információmegosztás szakterületen például a PCY_T1 állítás („Privát böngésző használatakor a böngészési előzmények nem tárolódnak, de tevékenységünk nincs titkosítva") nem járult hozzá szignifikánsan a konstrukció méréséhez (β = 0,059; p = 0,470), míg a PCY_T2 tétel („Nem minden információ tehető közzé bármilyen weboldalon, még akkor sem, ha az a feladataim elvégzését segítené") negatív súlyt mutatott (β = –0,168; p = 0,048), ami fogalmi vagy értelmezési problémára utalhat. Hasonló jelenségek más dimenziókban is megfigyelhetők. Az autentikáció területen az AUT_T3 indikátor (β = 0,142; p = 0,208) nem mutatott szignifikáns kapcsolatot a mögöttes konstrukcióval, ami arra utal, hogy a tétel tartalma nem illeszkedik kellő pontossággal a mérni kívánt fogalomhoz. A webes biztonság esetében a WEB_T1 állítás (β = –0,149; p = 0,061) egyszerre gyenge (nem

szignifikáns) és inverz (negatív irányú) kapcsolatot jelez, ami a tétel újrafogalmazásának és tartalmi érvényességének újragondolását indokolja. Ezek az eredmények nem gyengítik a modell általános érvényességét, ugyanakkor rámutatnak arra, hogy a jövőbeni adatgyűjtések és modellépítések során érdemes lehet a mérési állításokat finomítani, pontosítani és a kulturális-nyelvi kontextushoz igazítani a megbízhatóság további növelése érdekében. Mindezek arra utalnak, hogy bizonyos állítások esetében nem csupán a statisztikai szignifikancia hiánya, hanem az értelmezési kontextus, a nyelvi megfogalmazás és a kulturális sajátosságok is befolyásolhatják a mérés megbízhatóságát. A jövőbeli adatgyűjtések és modellépítések során ezért indokolt ezen tételek átfogó tartalmi és módszertani felülvizsgálata, illetve szükség esetén új, pontosabban operacionalizált mérési állítások kidolgozása. Összességében a modell alkalmas az információbiztonsági tudás komplex, többdimenziós mérésére.

Jövőbeli tervek

A hallgatói adatokon végzett pilotkutatás eredményei megteremtik az alapot a kutatási és fejlesztési lépések következő szakaszához, amelyek végső célja a biztonságtudatosság átfogóbb vizsgálata és gyakorlati erősítése, amelyhez a közeljövőben nagymintás adatfelvételek indulnának mind a lakosság, mind a vállalati szféra körében. A lakossági vizsgálatok lehetőséget adnak arra, hogy feltárjuk a társadalom különböző csoportjai közötti tudás- és attitűdbeli eltéréseket, míg a vállalati minták elemzése rávilágít a szervezeti kultúra erősségeire, valamint azokra a hiányosságokra, amelyek fokozott kockázatot jelenthetnek. Az adatfelvételt részletes statisztikai elemzések és összehasonlító vizsgálatok követik, amelyek azonosítani tudják majd a kritikus tudáshiányokat, a kockázatos attitűdöket és a fejlesztést igénylő viselkedésmintákat.

A kutatás nem csupán diagnosztikai célokat szolgál, hanem közvetlen fejlesztési és felhasználási lehetőségeket is nyújtana. Az eredmények alapján célzott oktatási és biztonságtudatossági programok készülhetnek, amelyek magukban foglalhatják az iskolai és felsőoktatási tananyagok bővítését, felnőttképzési modulok kialakítását, valamint a vállalatokra szabott tréningek és belső szabályozási ajánlások kidolgozását. Emellett szektor- és régióspecifikus programokhoz, valamint széles körű tudatosító kampányokhoz nyújthat segítséget, így a felhasználók jobban felismerhetik a biztonsági kockázatokat, és elsajátíthatják a helyes gyakorlatokat.

Hosszú távú cél, hogy a kutatás egy fenntartható és folyamatosan fejlődő biztonsági kultúra kialakításához járuljon hozzá. Ez a kultúra nemcsak az egyéni felhasználók mindennapi digitális biztonságát erősíti, hanem a vállalatok és intézmények működését is támogatja, elősegítve a tudatos, felelős és reziliens részvételt a digitális környezetben.

Összegzés

Napjainkban a humán tényező továbbra is meghatározó szerepet tölt be az információbiztonságban, és a felhasználók tudás-, attitűd- és viselkedésbeli sajátosságai alapvetően befolyásolják a szervezetek és egyének kiberrezilienciáját. A Security

Awareness Model empirikus vizsgálata igazolta, hogy a tudás–attitűd–viselkedés dimenziókra épülő, többdimenziós megközelítés alkalmas az információbiztonsági tudatosság komplex feltárására és mérésére. A modell erőssége, hogy nem csupán a technikai ismeretek meglétét értékeli, hanem képes feltárni a mögöttes kognitív és viselkedési mintázatokat is, ezáltal hozzájárulva a biztonságtudatosság mélyebb, strukturáltabb megértéséhez.

Az eredmények rámutattak arra, hogy a hallgatók megfelelően azonosítják a klasszikus kockázatokat és alapvető biztonsági elveket, azonban jelentős hiányosságok figyelhetők meg a szabályozási ismeretek, az új technológiákhoz való viszonyulás és a tudatos viselkedés dimenzióiban. E hiányosságok azt jelzik, hogy az információbiztonsági képzéseknek túl kell mutatniuk a puszta ismeretátadáson: szükség van az attitűdformálásra, a kritikus gondolkodás fejlesztésére és a biztonságtudatos döntéshozatal támogatására is. A modell validálása alátámasztotta annak mérési megbízhatóságát, ugyanakkor rávilágított a mérőtételek tartalmi pontosításának szükségességére, ami a jövőbeli kutatások egyik fő feladata lehet. A hosszú távú cél az adaptív, reziliens biztonsági kultúra kialakítása, amely képes alkalmazkodni a gyorsan változó technológiai és szabályozási környezethez, és hozzájárul a digitális ökoszisztéma fenntartható, biztonságos fejlődéséhez.

Felhasznált irodalom

Ahlan, Abdul Rahman – Lubis, Muharman – Lubis, Arif Ridho (2015): Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures. *Procedia Computer Science,* 72, 361–373. Online: https://doi.org/10.1016/j.procs.2015.12.151

Alanazi, Marfua – Freeman, Mark – Tootell, Holly (2022): Exploring the Factors that Influence the Cybersecurity Behaviors of Young Adults. *Computers in Human Behavior,* 136, 107376. Online: https://doi.org/10.1016/j.chb.2022.107376

Alharbi, Talal – Tassaddiq, Asifa (2021): Assessment of Cybersecurity Awareness Among Students of Majmaah University. *Big Data and Cognitive Computing,* 5(2). Online: https://doi.org/10.3390/bdcc5020023

Aljohni, Wejdan et al. (2021): Cybersecurity Awareness Level: The Case of Saudi Arabia University Students. *International Journal of Advanced Computer Science and Applications,* 12(3), 276–281. Online: https://doi.org/10.14569/IJACSA.2021.0120334

Alqahtani, Mohammed A. (2022): Factors Affecting Cybersecurity Awareness among University Students. *Applied Sciences (Switzerland),* 12(5). Online: https://doi.org/10.3390/app12052589

Al-Janabi, Samaher – Al-Shourbaji, Ibrahim (2016): A Study of Cyber Security Awareness in Educational Environment in the Middle East. *Journal of Information and Knowledge Management,* 15(1). Online: https://doi.org/10.1142/S0219649216500076

Bak, Gerda et al. (2024): On the Way to Updating the Measurement of Information Security Awareness – A Literature Analysis. *Interdisciplinary Description of Complex Systems,* 22(3), 305–316. Online: https://doi.org/10.7906/indecs.22.3.6

Berek László et al. (2024): Az egyén információbiztonsági tudatossági szintjének megállapítására elterjedt mérési módszerek összefoglaló elemzése nemzetközi kutatások alapján. In Molnár György – Temesvári Zsolt – Wührl Tibor (szerk.): *XXXIX. Kandó Konferencia 2023*. Budapest: Óbudai Egyetem, 265–277. Online: https://oda.uni-obuda.hu/bitstream/handle/20.500.14044/25752/ksc_22.pdf?sequence=1&isAllowed=y

Blažič, Borka Jerman – Blažič, Andrej Jerman (2022): Cybersecurity Skills among European High-School Students: A New Approach in the Design of Sustainable Educational Development in Cybersecurity. *Sustainability (Switzerland),* 14(8). Online: https://doi.org/10.3390/su14084763

Hong, Yuxiang – Furnell, Steven (2021): Understanding Cybersecurity Behavioral Habits: Insights from Situational Support. *Journal of Information Security and Applications,* 57. Online: https://doi.org/10.1016/j.jisa.2020.102710

McCormac, Agata et al. (2017): Individual Differences and Information Security Awareness. *Computers in Human Behavior,* 69, 151–156. Online: https://doi.org/10.1016/j.chb.2016.11.065

Módné Takács, Judit – Pogátsnik, Monika (2024): The Presence of Cybersecurity Competencies in the Engineering Education of Generation Z. *Acta Polytechnica Hungarica,* 21(6), 107–127. Online: https://doi.org/10.12700/APH.21.6.2024.6.6

Parsons, Kathryn et al. (2013): The Development of the Human Aspects of Information Security Questionnaire (HAIS-Q). In Deng, Hepu – Standing, Craig (szerk.): *ACIS 2013: Information Systems: Transforming the Future: Proceedings of the 24th Australasian Conference on Information Systems.* RMIT University, 1–11. Online: https://bit.ly/4xeFK1v

Parsons, Kathryn et al. (2014): Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security*, 42, 165–176. Online: https://doi.org/10.1016/j.cose.2013.12.003

Parsons, Kathryn et al. (2017): The Human Aspects of Information Security Questionnaire (HAIS-Q): Two Further Validation Studies. *Computers and Security*, 66, 40–51. Online: https://doi.org/10.1016/j.cose.2017.01.004

Répás József et al. (2024): HAIS-Q-tól a SAM-ig, a biztonságtudatosság mérésének modernizációja. *Hadmérnök,* 19(4), 183–198. Online: https://doi.org/10.32567/hm.2024.4.13

Répás József et al. (2025): Kisvállalkozások Nagy Kihívásai: Útmutató az Információbiztonsághoz. In Wührl Tibor (szerk.): *XL. Kandó Konferencia Kiadvány.* Óbudai Egyetem Kandó Kálmán Villamosmérnöki Kar, 179–186. Online: https://oda.uni-obuda.hu/bitstream/handle/20.500.14044/30380/Kiadv%C3%A1ny_Kando_XL_Konferencia.pdf

Shappie, Alexander T. – Dawson, Charlotte A. – Debb, Scott M. (2020): Personality as a Predictor of Cybersecurity Behavior. *Psychology of Popular Media,* 9(4), 475–480. Online: https://doi.org/10.1037/ppm0000247

Taha, Nashrawan – Dahabiyeh, Laila (2021): College Students Information Security Awareness: A Comparison Between Smartphones and Computers. *Education and Information Technologies,* 26(2), 1721–1736. Online: https://doi.org/10.1007/s10639-020-10330-0