AZ UTOLSÓ VÉDELMI VONAL: INFORMÁCIÓBIZTONSÁG-TUDATOSSÁG A DIGITÁLIS SZERVEZETEK KORÁBAN

THE LAST LINE OF DEFENSE: INFORMATION SECURITY AWARENESS IN THE AGE OF DIGITAL ORGANIZATIONS

VÁGÁNY Péter

Kulcsszavak: *DIKW-modell, információbiztonság-tudatosság, mesterséges intelligencia*

Keywords: *DIKW model, information security awareness, artificial intelligence*

JEL kódok: M15, D83, O33, J24

https://doi.org/10.33565/MKSV.2025.01.04

ABSZTRAKT

A digitális fenyegetések folyamatos térnyerése új kihívások elé állítja a gazdasági szervezeteket, miközben egyre nyilvánvalóbbá válik, hogy az információbiztonság nem kizárólag technológiai, hanem humán és szervezeti kérdés is. A tanulmány középpontjában a magyar munkavállalók információbiztonság-tudatosságának vizsgálata áll, különös tekintettel arra, hogy milyen tényezők befolyásolják a biztonságtudatos magatartást.

A kutatás empirikus alapját egy kérdőíves adatfelvétel képezte, amely során 525 fő válaszai kerültek elemzésre statisztikai módszerekkel. A válaszadók tudatossági szintje életkor, iskolai végzettség és munkahelyi környezet alapján került megállapításra.

Az eredmények rámutatnak arra, hogy az információbiztonság-tudatosság szintje jelentős eltéréseket mutat az egyes társadalmi és szervezeti csoportok között. A válaszadók egy része alacsony védekezőképességet tanúsít a leggyakoribb fenyegetésekkel szemben, míg mások már integráltan alkalmazzák a biztonságtudatos magatartás alapelveit. A vállalati méret, a szervezeti kultúra, valamint az oktatás és képzés rendszere kiemelkedő hatással bír a tudatosság kialakulására.

A tanulmány arra hívja fel a figyelmet, hogy a kiberbiztonság nem pusztán technikai kérdés: a jövő védelme az emberekben, nem pedig kizárólag az algoritmusokban rejlik – különösen egy olyan korszakban, ahol a mesterséges intelligencia térnyerése az információbiztonság etikai, jogi és társadalmi dimenzióit is új szintre emeli.

ABSTRACT

The continuous expansion of digital threats presents economic organizations with new challenges, while it is becoming increasingly evident that information security is not exclusively a technological matter, but also a human and organizational issue. The study focuses on investigating the information security awareness of Hungarian employees, with particular attention to the factors that influence security-conscious behavior.

The empirical basis of the research was a questionnaire-based data collection, during which the responses of 525 individuals were analyzed using statistical methods. The level of awareness was determined by age, educational attainment, and workplace environment.

The results point out that the level of information security awareness shows significant differences among various social and organizational groups. A portion of the respondents show low defensive capabilities against the most common threats, while others already apply the basic principles of security-conscious behavior in an integrated way. Company size, organizational culture, as well as the system of education and training have a remarkable impact on the development of awareness.

The study draws attention to the fact that cybersecurity is not merely a technical issue: the protection of the future lies in people, not exclusively in algorithms — particularly in an era where the expansion of artificial intelligence raises the ethical, legal, and societal dimensions of information security to a new level.

BEVEZETŐ

A digitalizáció térnyerése következtében az információbiztonság kérdésköre napjainkra mind szervezeti, mind egyéni szinten kiemelt jelentőséggel bír. A technológiai fejlődés gyors üteme nem csupán új lehetőségeket teremt, hanem korábban nem tapasztalt kockázatok és sérülékenységek előtt is ajtót nyitott. E folyamat eredményeként az információbiztonság már nem kizárólag technikai szempontok mentén értelmezhető, és nem tekinthető kizárólag az informatikai szakemberek feladatának. Egyre inkább egy olyan komplex, szervezeti és emberi tényezőkből álló rendszerként értelmezhető, amelyben a felhasználók biztonságtudatos magatartása kulcsszerepet tölthet be.

A sajtóban is gyakran megjelenő információbiztonsági incidensek nemcsak az érintett szervezetek reputációját veszélyeztetik, de jelentős anyagi károkat is eredményezhetnek. A releváns szakirodalom és gyakorlati tapasztalatok egyaránt alátámasztják, hogy az információbiztonsági incidensek túlnyomó többsége nem technológiai hibákból, hanem emberi mulasztásokból, figyelmetlenségből vagy tudáshiányból fakad. A biztonságtudatossági képzések hiánya, illetve az azok során megszerzett ismeretek hiányos vagy téves alkalmazása hozzájárul a szervezeti szintű kitettség növekedéséhez.

A szervezetek számára ezért elengedhetetlen, hogy alkalmazottjaik ne csupán passzív végrehajtói, hanem aktív és tudatos szereplői legyenek az információbiztonsági folyamatoknak.

A munkavállalók gyakran a leggyengébb láncszemként, vagy más megközelítésben az utolsó védelmi vonalként jelennek meg a szervezeti biztonság struktúrájában - attól függően, milyen szintű tudatosság és gyakorlati felkészültség társul hozzájuk. A hatékony kockázatkezelés érdekében nélkülözhetetlen a strukturált, készségszintű tudásra épülő biztonságtudatossági programok alkalmazása. Az információ védelme nem kizárólag az informatikai terület feladata, hanem a szervezet minden tagjának közös felelőssége, amely csak tudatos hozzáállással valósítható meg.

IRODALMI ÁTTEKINTÉS

Mielőtt részletesebben áttekintenénk az információbiztonsággal kapcsolatos égető kérdéseket, tisztázzunk néhány alapfogalmat!

A DIKW-modell

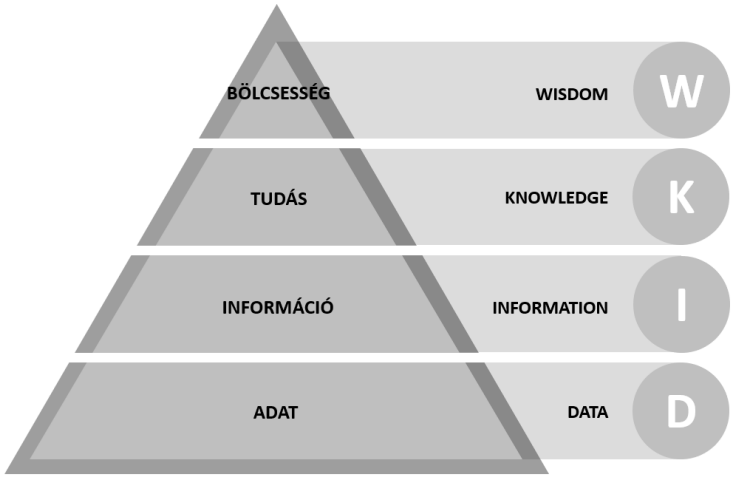
Az adat, az információ, a tudás, valamint a bölcsesség multidiszciplináris fogalmak: különböző tudományterület szakemberei kutatják az összefüggésüket, kölcsönhatásukat. Az információbiztonság területén is nagy jelentőséggel bírnak ezek a fogalmak.

Koltay (2008) a bölcsesség hierarchiájáról ír, ami az adat, az információ, a tudás, valamint a bölcsesség közötti összefüggéseket, ezek láncolatát mutatja be. A tudással- és információval foglalkozó szakirodalom szerint egy alapvető modellről van szó, amely leírja, hogyan lesz az adatból információ, ebből tudás, majd pedig bölcsesség. A nemzetközi szakirodalom DIKW (Data, Information, Knowledge, Wisdom) modellként ismeri, amit általában piramiselrendezésben ábrázolnak (1. ábra).

A hierarchia megértéséhez a modell alkotó fogalmak jelentéseit is érdemes megvizsgálni, mivel különböző szakterületeken más-más megfogalmazásban ismertek.

Ackoff (1989) alapján Koltay (2008) a DIKW-modellben szereplő fogalmakra a következő meghatározásokat javasolja:

- Az adatok megfigyelés és tapasztalat által jönnek létre. Olyan szimbólumokról van szó, amelyek tárgyak, események és környezetük tulajdonságait mutatják be. Releváns formába kerülésük után használhatók csak fel (addig lényegében önmagukban értéktelenek), hiszen csak akkor lesznek értelmezhetők, ha megfelelő kontextusba, környezetbe kerülnek.
- Az információ értelmezett adat, amit következtetés, vagy értelmezés útján nyerjük az adatokból. Legtöbbször a ki?, a mi?, a mennyi? és a mikor? kérdésekre válaszol.
- A tudást know how-ként definiálja, amit oktatáson keresztül vagy tapasztalati úton szerezhetünk meg olyantól, aki már rendelkezik vele. A tudás segítségével alakítható az információ utasítássá, tehát feldolgozott információról van szó.
- Az intelligencia az eredményesség fokozásának képessége,
- a bölcsesség pedig nem más, mint a felhalmozott tudás összessége, a hatékonyság növelésének képessége.



***1. ábra* A DIKW-modell**
Forrás: saját szerkesztés

Zeleny (1987) a tudás hierarchiáját egy új fogalommal egészítette ki, a megvilágosodással (enlightenment), amely az ő elképzelésében a képzeletbeli piramis csúcsára kerül, a bölcsesség fölé. Ackoff (1989) ezzel szemben a megértést (understanding) illesztette be a tudás és a bölcsesség közé a hierarchiába. Bár Ackoff külön szintként említi a megértést, a későbbi szakirodalmak vitatják, hogy valóban külön szintről van-e szó, vagy csak egy átmeneti fázisról.
Rowley (2007) tanulmánya szerint több szerző egyetért abban, hogy a hierarchia első megjelenése T.S. Elliot 1934-es The Rock (A szikla) című versében található. Egész pontosan így említi a fogalmakat a híres költő:
„Where is the *wisdom* that we have lost in *knowledge*?
Where is the *knowledge* that we have lost in *information*?"

Egy táblázatban Rolwey összefoglalta Ackoff és Zeleny definícióit az adat, információ, tudás, bölcsességgel kapcsolatban (1. táblázat).

1. táblázat. **Zeleny és Ackoff definícióinak összefoglaló táblázata**

	Zeleny	Ackoff
Adat	Nem tudunk semmit. (Az adat önmagában nem hordoz jelentést)	Szimbólumok. (Önmagukban nem értelmezhetők)
Információ	Tudjuk mit. (Az adat értelmezése útján létrejövő jelentéstartalom)	Feldolgozott adatok, amelyek válaszokat adnak a ki?, mi?, hol? és mikor? kérdésekre.
Tudás	Tudjuk hogyan. (Az információk gyakorlati alkalmazására való képesség)	Az adatok és információk alkalmazása, amely választ ad a hogyan? kérdésekre.
Megértés	-	A miért? kérdések értelmező felismerése
Bölcsesség	Tudjuk miért. (Az okok és célok felismerése, összefüggések látása)	Értékelt megértés. (Ismeretek kontextuális értékelése)
Megvilágosodás	Az igazság, a jó és a rossz érzékelésének elérése, ezek ezek társadalmi elfogadottsága és elismertsége	

Forrás: saját szerkesztés, Rowley (2007) alapján

A bölcsesség hierarchiáját alkotó fogalmakhoz Ackoff és Zeleny mellett más kutatók, szakemberek különböző definíciókat alkottak.

Az alábbi meghatározás szerepel az adatra vonatkozóan a 2024. évi LXIX. törvényben, amely Magyarország kiberbiztonságáról rendelkezik:

„adat: az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas." (I. fejezet 4. § 1.)

Az információ definíciója a 2013. évi L. törvény szerint (ez a törvény a 2024. évi LXIX. törvény 116. § szerint hatályát vesztette):

„információ: bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti." (I. fejezet, 1. § (1) 25.)

Davenport (2001) szerint az információ egy használható és megfelelő adat, aminek célja az új ismeret megszerzése, ami hatással van a befogadó személy viselkedésére és szemléletére.

A mesterséges intelligencia térhódítása, valamint az adatok és információk birtoklása és felhasználása segítségével jelentősen befolyásolni tudjuk az emberi viselkedést és szemléletet. Nem mindegy tehát, hogy milyen adatokat osztunk meg magunkról felhasználóként és az sem, hogy a birtokunkban került adatokat hogyan kezeljük és használjuk.

Informatikai biztonság, információbiztonság

Az alapfogalmak áttekintését követően az információbiztonságról is ejtsünk néhány szót.

Az információ védelme, az információbiztonság az első emberi társadalmak kialakulásáig nyúlik vissza. Az idő előrehaladtával az információ megszerzési-, valamint annak védelmi módszerei is jelentősen alakultak, fejlődtek. Az írás megjelenése alapvetően átalakította az információközlés módját, ennek hiányában a mai civilizáció jelenlegi formájában valószínűleg nem alakulhatott volna ki. A történelem későbbi szakaszaiban a nagyobb terjedelmű írott információkat és üzeneteket már futárok továbbították, mely új kockázatokat is magában hordozott információbiztonság szempontjából, hiszen elegendő volt a futárt elfogni ahhoz, hogy a bizalmas üzenet illetéktelen kezekbe kerüljön. A támadók ráadásul akár válaszolhattak is az eredeti címzett nevében, megtévesztve ezzel a feladót.

Korábban az írás elsajátítása csak kevesek kiváltsága volt, ám az írástudók számának növekedésével egyre inkább szükségessé vált az információk védelme, például kódolás vagy titkosítás révén. Az elektronikus hírközlés megjelenése és elterjedése lehetővé tette, hogy az információ gyorsan és egyidejűleg nagy tömegekhez jusson el. A rádiótechnológia megjelenését szinte azonnal követte az információk lehallgatásának és zavarásának lehetősége. (Gémes, 2017)

A második világháború során a világhírű brit matematikus, Alan Turing fontos szerepet játszott a német Enigma-kódok feltörésében. Ez jelentős stratégiai előnyt biztosított a szövetségesek számára, mivel hozzáférést nyertek a náci Németország titkos kommunikációjához. Történészek szerint a korábban feltörhetetlennek gondolt kódolt információk megfejtése akár évekkel is lerövidíthette a háború időtartamát. Mindez jól példázza, hogy az információ védelme, titkosítása – illetve annak visszafejtése – a háborús hadviselésben is meghatározó szerepet töltött be. (Copeland, 2004)

Az elmúlt évtizedek robbanásszerű technológiai fejlődésének hatására az információtechnológiai megoldások alkalmazása már nem csupán az állami és vállalati szférában vált általánossá, hanem a magánszemélyek körében is széles körben elterjedtté válhatott. Ugyanakkor fontos kiemelni, hogy az új technológiák megjelenése – minden előnyük mellett – új, rejtett kockázatokat is magában hordozhat. (Gémes, 2017)

Napjainkban az informatikai eszközök, az internet és az okostelefonok már a háztartások jelentős részében megtalálhatók. Az okoseszközök otthoni alkalmazása egyre elterjedtebb, azonban ezek használata fokozott kockázatot is jelenthet a magánszféra számára. Nem minden eszköz rendelkezik megfelelő biztonsági megoldásokkal, így például előfordulhatnak beépített hátsó kapuk, a titkosítás hiánya vagy gyenge/nem megfelelő jelszóhasználat, amelyek sebezhetővé tehetik a felhasználókat. Ha Magyarországot vizsgáljuk, a Digital Economy and Society Index (DESI) 2022-es jelentése szerint a digitális gazdaság és társadalom fejlettséget mérő mutató alapján a 27 uniós tagállam között a 22. helyen áll, a háztartások 22%-ban található legalább 1Gbps sebességű széles sávú internet-hozzáférés.

Az internet széles körű elterjedése alapvetően átalakította a mindennapi életet: a világ korábban elképzelhetetlen közelségbe került, néhány kattintással elérhetővé váltak új szolgáltatások, valamint számos hétköznapi tevékenység a digitális térbe helyeződött át. Több új, internetre épülő üzleti modell és digitális iparág is

létrejött, melyek közül több az ezredfordulón bekövetkezett úgynevezett „dotkom lufi" következtében össze is omlott.

Az internet a tanulás és a munkavégzés formáit is jelentősen átalakította. Mindezek mellett azonban az új platform új kihívásokat, kockázatokat és biztonsági fenyegetéseket is magában hordozott és hordoz napjainkban is. (Munk, 2008)

Ezeket a kihívásokat egyéni és szervezeti szinten együttesen szükséges kezelni.

A kibertér, mint az ötödik lehetséges hadszíntér, hivatalosan a NATO 2016-os varsói csúcstalálkozóján került a hagyományos négy (szárazföldi, légi, tengeri és űrbéli) hadműveleti terület mellé. (Gémes, 2017)

Ez is jól alátámasztja az információbiztonság létjogosultságát. De mi is pontosan az információbiztonság?

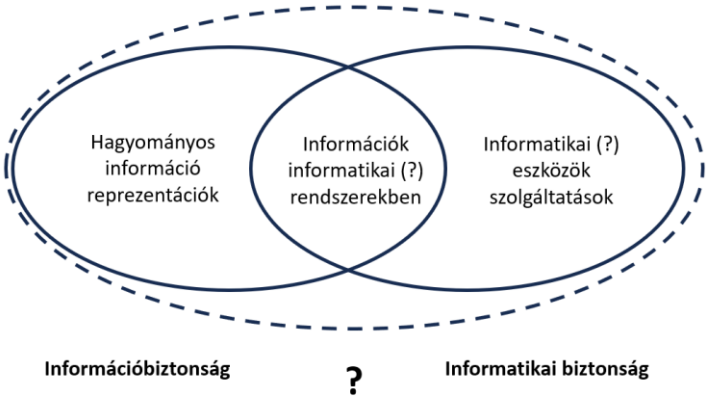
Az információbiztonság szó az (értelemmel bíró) adattal, azaz az információval kapcsolatos biztonságot, védelmet sugallja. Minden információ adat, viszont fordítva ez már nem igaz, tehát nem nevezhetünk minden adatot információnak. Kizárólag akkor tekinthető az adat információnak, ha megfelelő kontextusba kerül. Erre egy példa az alábbi számsor: 19340414. Ez egy jelentés nélküli adat. Ha eláruljuk, hogy a számsor egy születési dátum, akkor már értelmezhető lesz, és információvá válik (Vágány, 2023).

Munk (2008) az információbiztonságot személyi-, dokumentum- és elektronikus információvédelemre bontotta, míg Gémes (2017) személyi-, fizikai- és dokumentum biztonsági részeket említett.

Muha (2008) megállapítása szerint még a szakemberek körében is gyakran tévesen használják az informatikai biztonság és az információbiztonság fogalmakat. Ez a pontatlanság elsősorban arra vezethető vissza, hogy az angol nyelvben az „information security" kifejezés egyaránt utalhat az informatikai védelemre, az információk biztonságára, illetve azok védelmére. Az információbiztonság olyan tevékenységek összességére utal, amelyek célja a szóban, írásban, rajzban,

valamint kommunikációs, informatikai és egyéb elektronikus rendszerekben (vagy bármilyen más formában) kezelt adatok védelme.

Az informatikai biztonság az információbiztonságnál szűkebb, mivel elsősorban az informatikai rendszerekben kezelt és tárolt adatok, valamint a rendszereknek a védelmét foglalja magában. Az információk biztonságának biztosítása viszont nem lehetséges az azokat tároló és feldolgozó rendszerek megfelelő védelme nélkül. (Muha, 2008)



2. ábra. **Információbiztonság vs. informatikai biztonság**

Forrás: Munk (2008) alapján, saját szerkesztés

Az Information Systems Audit and Control Association (ISACA) magyar szakkifejezés-gyűjtemény (2013) szerint az információbiztonság „biztosítja, hogy a vállalaton belül az információ védve van jogosulatlan felhasználók felé való közzététel (bizalmasság), helytelen módosítás (sértetlenség), és a szükség szerinti hozzáférhetőség elvesztése (rendelkezésre állás) ellen." (ISACA, p. 108)

A 2024. évi LXIX. törvény az elektronikus információs rendszer biztonságáról a következőképpen rendelkezik: „az elektronikus információs rendszerek azon képessége, hogy adott bizonyossággal ellenálljanak minden olyan eseménynek, amely veszélyeztetheti a rajtuk tárolt, továbbított vagy kezelt adatok vagy az említett hálózati és információs rendszerek által kínált vagy azokon keresztül

elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát". (I. fejezet 4. § 25.)

A bizalmasság (confidentiality), sértetlenség (integrity) és rendelkezésre állást (availability) a szakirodalomban CIA-elvként hivatkozzák. Az információbiztonság tehát az információ bizalmasságának, sértetlenségének és rendelkezésére állásának megőrzését jelenti.

A CIA (confidentiality, integrity, availability) elemeiből a bizalmasság és sértetlenség volt az, amit elsőként azonosítottak az információ védendő tulajdonságai közül. A későbbiekben még egy tulajdonság, a rendelkezésre állás is kapcsolódott Munk (2008) szerint.

A 2024. évi LXIX. törvény az alábbi definíciókat adja a bizalmasságra, sértetlenségre és rendelkezésre állásra:

„bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról." (I. fejezet 4. § 13.)

„sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik, azaz hiteles, valamint a származás ellenőrizhetőségét, bizonyosságát, azaz letagadhatatlanságát is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható." (I. fejezet 4. § 86.)

„rendelkezésre állás*:* annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek." (I. fejezet 4. § 84.)

Napjainkban az információbiztonsági tudatosság kialakítása égetően fontossá vált. A szervezetek és a magánszemélyek egyaránt folyamatosan ki vannak téve a

világhálón megjelenő rosszindulatú kiberfenyegetéseknek és -támadásoknak. (Schaik et al., 2017, Vágány, 2024)

Életünk szinte minden területét érinti a digitalizáció, amely ezzel párhuzamosan újabb és újabb kihívások elé állítja az információbiztonsági szakembereket a hétköznapi internetfelhasználókkal együtt. Az egyre növekvő digitális transzformációval (amelyet a mesterséges intelligencia használata is gyorsíthat), párhuzamosan nő a személyes adatok gyűjtésével, tárolásával és feldolgozásával kapcsolatos nem feltétlen alaptalan aggodalom is. (Drljača & Latinović, 2017, Liu, 2020)

Az adatvédelem kiemelt jelentőséggel bír, nemcsak a magánélet védelme, hanem az internet és a közösségi média töretlen térnyerése miatt is, amelyek elősegítik az adatok megosztását, valamint azok begyűjtését is. Az információ egyre fontosabb szerepet tölt be a döntéshozatalban, azonban ez újabb kockázatokat is jelent: a döntéshozók sokszor az információ értékét a magánélet védelme elé helyezik, ami a személyes adatokkal kapcsolatos jogok sérelméhez vezethet. (Darwin & Nkongolo, 2023).

A spamek, azaz a kéretlen levelek terjedése, az illetéktelen hozzáférés vagy az adatszivárgás mind a felhasználói személyes adatokra, mind pedig az állami infrastruktúra digitális adataira nézve komoly veszélyt jelenthetnek. Az érzékeny adatok (például az egészségügyi információk) fokozottan ki vannak téve különféle fenyegetéseknek, ami még inkább ráirányítja a figyelmet a magánélet védelmének kiemelt fontosságára. (Nazarov et al., 2021, Pereira et al., 2020) A felhasználók gyakran nincsenek tisztában az adatfeldolgozás módjával (és annak következményeivel). A jelenlegi helyzet alapvető kérdéseket vet fel az adatgyűjtés, az adathasználat és az egyéni jogok közötti egyensúly megteremtése kapcsán. Ezért elengedhetetlen olyan megközelítést kialakítani, amely a technológiai fejlődés mellett az etikai szempontokat, a társadalmi elvárásokat is figyelembe veszi, elősegítve az átláthatóságot, a nyilvános párbeszédet az adatkezelés jövőjéről. (Métayer et al., 2015, Christen et al., 2019, Hand, 2018, Helbing, 2013)

Az adatok gyűjtéséhez és felhasználásához kapcsolódó aggodalmak különösen az adatvédelem, az átláthatóság és az elszámoltathatóság területein jelennek meg, rámutatva arra, hogy a digitális jogok védelme emberi jogi szempontjából is kiemelt jelentőségű. A személyes adatok kiterjedt gyűjtése és elemzése könnyen ütközhet a magánélethez, illetve az adatvédelemhez fűződő jogokkal, különösen a digitális környezetben, ahol szinte minden tranzakció és interakció rögzítésre kerül, tárolódik, vagy profilalkotási célokra hasznosul. (Shehu & Shehu, 2023, Rooy & Bus, 2010, Weydner-Volkmann, 2023). A mesterséges intelligencia által vezérelt rendszerek újabb kihívásokat jelentenek, mivel ezek a rendszerek képesek lehetnek az emberi viselkedés előrejelzésére és befolyásolására. Ez súlyos etikai és társadalmi következményekkel járhat, ha mindez az egyének tudta és beleegyezése nélkül történik. (Larsson, 2018).

A kialakult helyzet megköveteli minden résztvevőtől, hogy mélyebb szinten értsék és tudatosan kezeljék az információbiztonság kérdéseit, annak érdekében, hogy a digitális ökoszisztéma integritása fenntartható legyen és a felmerülő kihívásokra hatékony válaszok születhessenek. (Shehu & Shehu, 2023).

Információbiztonság-tudatosság

Az információbiztonság-tudatosságnak az egyén szintjén is legalább annyira fontosnak kellene lennie, mint a gazdálkodó szervezetek esetén, mivel hétről hétre hallhatunk a médiában kibertámadásokról és biztonsági incidensekről.

Kevin Mitnick és szerzőtársa (2003) szerint csupán technológiai védelmi intézkedésekkel nem lehet kivédeni az ilyen jellegű támadásokat. Több, a témával foglalkozó szakember is hangsúlyozza a munkavállalók megfelelő tudatossági képzését.

Az ISACA (2013) szerint a tudatosság definíciója: „Megismerni, figyelembe venni, tudatában lenni és jól tájékozottnak lenni egy meghatározott témáról, amely magába foglalja a téma ismeretét és megértését, valamint az ennek megfelelő cselekvést." (ISACA (2013), p. 260)

Tarján (2020) hozzáteszi, hogy a definíció valaminek a tudásáról („tudatában van") és megértéséről beszél, tehát megkülönbözteti a betanítást (training) és a képzést (education). A betanítással azt tanuljuk meg, hogy mit és hogyan kell végrehajtani, a képzéssel pedig az az információ kerül átadásra, hogy mi az értelme az adott intézkedésnek, és a tennivaló egyéb kontextusára is rávilágít. A tudatosság pedig azt feltételezi, hogy a szabályok nem csak azért kerülnek követésre, mert ismerik őket, hanem azért is, mert megértették, hogy miért fontos úgy cselekedni, ahogy ezt előírták.

Kovács és Krasznay (2010) egy Magyarország elleni elképzelt kiberbiztonsági támadás forgatókönyvét mutatta be. 2017-ben egy új cikket írtak a témában, amiben arra voltak kíváncsiak, hogy az eltelt években hozott, a védelemmel összefüggő lépések, jogszabályok elegendők lehetnek-e a megfelelő védelem megteremtésében. Több következtetésre jutottak, és kiemelték az információbiztonság-tudatosság növelésének fontosságát.

Kruger (2006) úgy véli, hogy az információbiztonság-tudatosságnak dinamikus folyamatként kell működnie, mivel a kockázatok is folyamatosan változnak. A munkavállalók tudása csak akkor maradhat naprakész, ha a tudatosságnövelő program nem alkalmi jellegű, hanem a vállalati kultúrába szervesen beépül. Schlienger és Teufel (2003) tanulmányára hivatkozva Kruger (2006) – utalva a program folytonosságára –, úgy gondolja, hogy azon szervezetek esetén, ahol ezek az információbiztonság-tudatosság növelését célzó programok nem állnak meg a „tudatossá válásnál" (become aware) vagy a „tudatosnak maradásnál" (stay aware) hanem elérik a „tudatosnak lenni" (be aware) szintjét, ott gyökeresen megváltozik a biztonsági kultúra.

Illésy és munkatársai (2014) kutatásukban a közigazgatásban dolgozók információbiztonság-tudatosságát vizsgálták, melynek célja a hazai közigazgatás információbiztonsági szintjének megismerése volt. Az információbiztonság képzés előkészítésekor azt tapasztalták, hogy a közigazgatásban dolgozók esetén a tudás meglehetősen heterogén. A megkérdezett szakemberek olyan képzési

formát tartottak elfogadhatónak, amelynek tartalma szorosan kapcsolódik a mindennapi munkavégzéshez. Emellett azt is hangsúlyozták, hogy nem csupán az informatikai vagy a jogi ismeretekre kellene fókuszálni a képzéseknél, hanem a biztonságtudatos gondolkodásmód kialakítása lenne a fontos.

Wilson és Hash (2003) megállapította, hogy a biztonsági tudatosság programban a szervezet minden alkalmazottját szükséges bevonni, a vezetői példamutatás (valamint támogatás) ennél is kiemelkedően fontos.

Lee szerzőtársaival (2003) szerint az információbiztonság-tudatosság nemcsak a fenyegetések felismerését, hanem az ezekkel szembeni sebezhetőség tudatosítását is jelenti. A veszélyek ismerete nem elegendő ahhoz, hogy a felhasználók megtegyék a szükséges (és helyes) intézkedéseket. Véleményük szerint a felhasználók csak akkor cselekszenek, ha tudatosul bennük az, hogy az ilyen (negatív) eseményben személyesen ők is érintettek lehetnek.

Jacobs és szerzőtársai (2022) az amerikai kormányzat biztonságtudatossági programjainak hatékonyságának mérésével foglalkoztak. Rámutattak arra, hogy az alkalmazottak biztonságos viselkedését valóban fejleszthetik a biztonságtudatossági képzések, mivel segítenek megfelelően reagálni a problémákra, így elősegíthetik a szervezet biztonsági helyzetét. A kutatás arra is rámutatott, hogy a szervezetek a programok hatékonyságának pontos mérésében nehézségekbe ütköznek. Gyakran a képzés elvégzésének arányára támaszkodnak a tényleges viselkedésváltozás helyett

A szerzők szerint a holisztikus értékeléshez elengedhetetlen többfélre mérőeszköz együttes alkalmazása, mint a képzési témákhoz kapcsolódó biztonsági incidensek száma és jellege, a felhasználók által kezdeményezett incidensek jelentése, az adathalász teszteknél tapasztalt kattintási arány, a releváns tartalmak megtekintése, valamint az érintettek körében végzett interjúk vagy kérdőíves visszajelzések.

A SANS arra a következtetésre jutott, hogy azok a szervezetek, amelyek saját képzési programjukat más szervezetekéhez viszonyítva értékelik, jellemzően nagyobb vezetői támogatásban részesülnek, ami az eredményességre is hatással

van. Az információbiztonság-tudatosság fejlettségét értékelő ötfokozatú modell, a Security Awareness Maturity Model megfelelő lehet az ilyen típusú összehasonlításhoz.

Az ötlépcsős modellt Lance Spitzner nevéhez kötik; kialakítása több szervezet együttműködésén és konszenzusán alapult. A modell támpontot nyújt a szervezetek számára információbiztonság-tudatossági programjuk érettségi szintjének értékeléséhez. Spitzner értelmezésében az első szintet, a program hiánya jellemzi a szervezetnél (Non-existent). Az ilyen szervezeteknél semmilyen törekvés sincs az információbiztonsági képzésre, a munkavállalók nincsennek tisztában azzal, hogy célpontjai lehetnek az humánalapú támadásoknak.

A második, a megfelelőségközpontú szint (Compliance-focused). Spitzner szerint a legtöbb szervezet ezen a szinten helyezkedik el. Bár a képzések megtörténnek (évente vagy ad-hoc jelleggel) a különböző követelmények miatt (pl. audit), de nincs valós célja a munkavállalók viselkedésének megváltoztatására. Emiatt ugyanolyan védtelenek a szervezetnél dolgozók a támadásokkal szemben, mint ahol semmilyen tudatossági program sincs.

A harmadik szint a tudatosság és a viselkedésváltozás előmozdítását (Promoting awareness & behavior change) célozza. Ezen a szinten már cél a munkavállalói viselkedés megváltoztatása, valamint a kockázat csökkentése is. A szervezet azonosítja azokat a képzési témákat, amelyek a legnagyobb hatással vannak a szervezet küldetésének támogatására. Spitzner szerint az ilyen szervezetek dolgozói ismerik a szervezet folyamatait és szabályait, valamint képesek felismerni és megelőzi, valamint jelenteni a biztonsági incidenseket.

A negyedik szint a hosszú távú fenntarthatóság és kultúraváltás (Long-term sustainment & culture change) szintje. A program célja itt már nem csak a tudatosság és a viselkedésváltozás támogatása, hanem ezek beépítése a szervezeti kultúrába. A képzési anyagok ezért évente felülvizsgálatra kerülnek, hogy a program naprakész maradhasson.

A modell legmagasabb szintje a mérőszámokra épülő stratégiai keretrendszer (Strategic metrics framework) szintje. A tudatosságnövelő programhoz mérőszámokat rendelnek, amelyek lehetővé teszik az előrehaladás nyomon követését és a program hatásának (pl. viselkedés változás) mérését (SANS, 2023) Az információbiztonsági kockázatokat – a különböző kontrollok alkalmazása mellett –, tudatosító képzésekkel is csökkenthetjük.

A mesterséges intelligencia technológia robbanásszerű fejlődése (amely nagyrészt a hatalmas adatmennyiségek gyűjtésén alapul) új kihívásokat és dimenziókat nyitott meg az információbiztonság területén, különösen az adatvédelem és a biztonság jelentőségével kapcsolatban. (Huang, 2023) A mesterséges intelligencia rendszerek komplexitása, az algoritmusok felhasználói szempontból való átláthatatlansága megnehezíti az esetleges hibák felismerését és szükség szerinti korrekcióját, ami súlyos következményekkel járhat mind az egyének, mind a társadalom szintjén. (Naik et al., 2022, Latham & Goltz, 2019) Ezen kihívások kezelése érdekében alapvető fontosságú az átfogó szabályozási keretek és az etikai irányelvek kidolgozása, amelyek egyensúlyt teremthetnek a technológiai innováció és az alapvető emberi jogok, különösen a magánélet védelme között (Pusztahelyi, 2021). Ez különösen igaz azon döntéshozatali rendszerek esetében, amelyek jelentős mértékben támaszkodnak a mesterséges intelligenciára, mivel ezek érdemben befolyásolhatják az egyéni autonómiát, illetve hosszabb távon a társadalmi értékrend alakulását is. Fontos, hogy az AI-rendszerek tervezése és alkalmazása során is kiemelt figyelmet fordítsanak az adatvédelem és a magánélet alapelveinek érvényesítésére, hogy minimalizálható legyen a visszaélések kockázata, és az egyének megfelelő kontrollt gyakorolhassanak saját adataik felett. (Hernández, 2024, Al-Zahrani, 2024). Ez magában foglalja az etikai kockázati tényezők és mechanizmusok azonosítását a mesterséges intelligencia döntéshozatali folyamataiban, valamint egy emberközpontú megközelítés érvényesítését ezen rendszerek tervezésénél (Guan et al., 2022, Calvano et al., 2025). A mesterséges intelligencia etikai vonatkozásai – mint például az adatok

torzítása, a diszkrimináció vagy az átláthatóság hiánya – komoly aggályokat vetnek fel, különösen abban az esetben, ha az AI-rendszerek szakmai döntések meghozatalában vesznek részt, vagy teljes mértékben átveszik ezt a szerepet, ezáltal elmosva a felelősségi határokat az érintett szereplők között. (Kubaisi, 2024, Olorunfemi et al., 2024).

A mesterséges intelligencia nem csupán technológiai eszköz, hanem egy olyan formáló tényező, amely társadalmi szinten is jelentős előnyöket kínál: hozzájárul a költségek és kockázatok csökkentéséhez, növeli a folyamatok konzisztenciáját és megbízhatóságát, valamint innovatív megoldásokat kínál az összetett problémák kezelésére. (Hermann, 2021).

Számos területen használnak már ma is mesterséges intelligenciát. Gondoljunk csak a bankok, a webáruházak vagy egyéb szolgáltatók chatbotjaira, melyek fontos láncszemeivé váltak a kapcsolattartásnak és információszerzésnek.

A banki szektorban a chatbotok már ma is valós idejű szolgáltatásokat nyújtanak, lehetővé téve az ügyfelek mélyebb megismerését és a kapcsolat javítására irányuló stratégiák kidolgozását (Cordero et al., 2022). A technológia fejlődésével a chatbotok egyre kifinomultabbá válnak, és már ma is képesek egyre komplexebb feladatok elvégzésére is, mint például az ügyfélszolgálati interakciók széles körének kezelésére, valamint a felhasználói igények proaktív azonosítására és kiszolgálására (Radziwill & Benton, 2017, Alboqami, 2023).

A chatbotok és az emberek közötti interakciók vizsgálata során megfigyelhető, hogy a felhasználók gyakran hasonló módon reagálnak a mesterséges intelligenciával működő rendszerekre, mint az emberekre, ami új kutatási irányokat nyithat meg a mesterséges intelligencia és az emberi viselkedés közötti kapcsolat mélyebb megértésében (Lou et al., 2021). Ez a jelenség rávilágít az antropomorf jegyek, mint például az empátia, a társas jelenlét és a személyiség chatbotokba történő integrálásának fontosságára. Ezek jelentős szerepet játszanak az emberi interakciók szimulálásában és a felhasználói elkötelezettség erősítésében (Cox et al., 2023).

Miközben a mesterséges intelligencia alapú megoldások alkalmasak a repetitív feladatok automatizálására, a fejlettebb rendszerek – mint a gondolkodó AI, amely az adatelemzésen alapuló döntéshozatalt teszi lehetővé, illetve az érző AI, amely az emberi érzelmek felismerésére és az interakciók finomhangolására alkalmas – összetettebb feladatok ellátására is használhatók. (Huang & Rust, 2020).

Ez pedig jelentős információbiztonsági veszélyt is magában hordozhat, és új kutatási lehetőségeket nyithat meg a tudományos világ számára.

A következőkben ismertetett empirikus kutatás a mesterséges intelligencia információbiztonságra gyakorolt hatásaival még nem foglalkozik, azt egy következő kutatásban fogjuk megvizsgálni.

Módszertan

Jelen tanulmány egy folyamatban lévő kutatás részeredményeit ismerteti. Ennek keretében egy kvantitatív kutatás legfontosabb megállapításai kerülnek bemutatásra. A kvantitatív kutatás keretében egy információbiztonság-tudatossággal kapcsolatos kérdőív került összeállításra, melyet online tölthettek ki a válaszadók. A mintavétel hólabda módszer segítségével történt.

A kérdőív döntően zárt kérdésekből állt. A kérdőív összeállításánál figyelembe kellett venni, hogy a kutatásba különböző informatikai háttérrel rendelkező válaszadó fog részt venni, ezért a kérdések összeállításánál a lehető legegyszerűbb megfogalmazásra törekedtünk.

A kérdőív publikálása előtt 20 fővel próba lekérdezést végeztünk, hogy megbizonyosodjunk a kérdéseink közérthetőségéről. A folyamat során világossá vált, hogy a szakszavakat a megkérdezettek közül többen nem értették, például a „kártékony kód elleni védelem" helyett a „vírusirtó" kifejezés került a végleges kérdőívbe, valamint a kétfaktoros azonosításhoz is magyarázatot kellett elhelyezni, mert bár a kifejezést nem, de magát a megoldást több válaszadó is ismerte és használja.

A Google Formsban készített kérdőívet 2023. szeptember 14-től október 28-ig lehetett kitölteni. A felmérésbe elsősorban gazdálkodó szervezetnél dolgozó munkavállalók kerültek bevonásra.

A tanulmányban a következő kutatási kérdésre keressük a választ:

K1: Mi jellemzi a magyar embereket információbiztonság-tudatosság szempontjából?

A kutatási kérdés mellett három hipotézis is megfogalmazásra került:

H1: A 30 évnél fiatalabbak információbiztonsági szempontból tudatosabbak, mint az idősebbek.

H2: KKV-k esetén az információbiztonság kevésbé hangsúlyos, mint a nagyvállalatoknál.

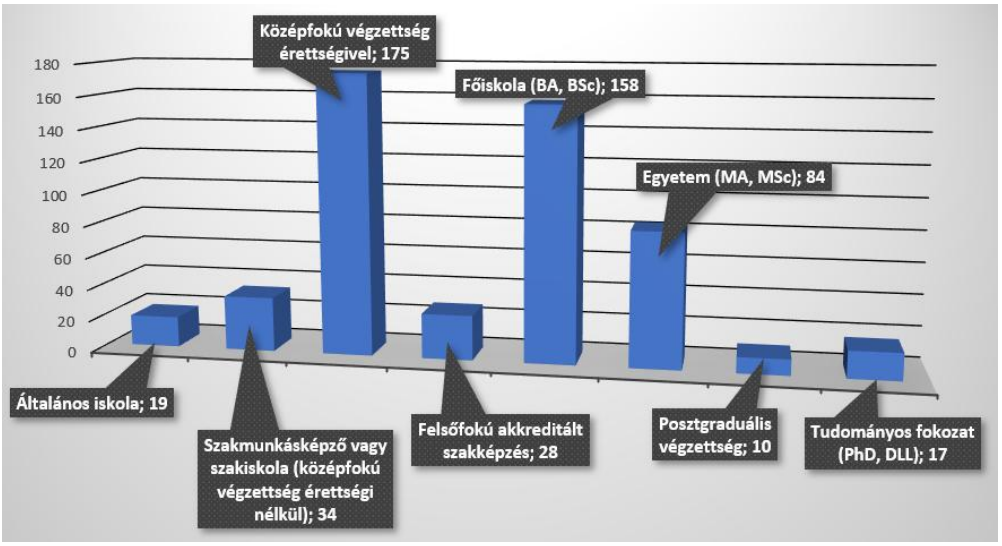
H3: Az iskolai végzettséggel nő az információbiztonság-tudatosság.

Az eredmények az SPSS 24 verziójával kerültek elemzésre.

EREDMÉNYEK

A kérdőívet 525 fő töltötte ki. 399 nő, illetve 126 férfi. A legtöbben (33,3%) érettségivel rendelkeznek, de jelentős számú válasz (30,1%) érkezett főiskolai (BA/BSc) végzettséggel rendelkezőktől is. Egyetemi végzettséggel (MA/MSc) 16 százalék, tudományos fokozattal (PhD, DLL) pedig 3,2 százalék rendelkezik (3. ábra).

A felsőfokú, valamint a doktori fokozattal rendelkező kitöltők felülreprezentáltak, ami a hólabda módszer sajátosságából ered. Az adatgyűjtés folyamán nem volt cél, hogy a kérdőív reprezentatív legyen, a megállapítások kizárólag erre a mintára vonatkoznak, és nem általánosíthatóak.



3. ábra. **A válaszadók iskola végzettségének megoszlása (fő)**
Forrás: saját szerkesztés

A kérdőív kitöltésének nem volt feltétele az informatikai végzettség. A válaszadók 23,2 százaléka (122 fő) állította azt magáról, hogy rendelkezik ilyen végzettséggel. Akik megjelölték, hogy rendelkeznek informatikai végzettséggel, azok egy szabadszöveges mezőben megadhatták végzettségük típusát. A kérdésre válaszolók közül a legtöbb (42 fő) ECDL (European Computer Driving Licence) végzettséggel rendelkeztek.

A kérdőív eredménye alapján a válaszadók 71,4 százaléka beosztottként dolgozik, 10,7 százalékuk döntéshozó, a többiek (17,9 százalék) nem dolgoznak.

A munkahellyel rendelkező válaszadók száma tehát 431 fő lett. Ebből 39,9 százalék (172 fő) dolgozik nagyvállalatnál, a válaszadók többsége (60,1 százalék) pedig a KKV-szektorban dolgozik.

307 fő magyar tulajdonú-, 97-en multinacionális-, míg 27 válaszadó vegyes tulajdonú vállalatnál dolgozik. 270-en adták azt a választ, hogy profitorientált vállalkozásnál dolgoznak, míg 101-en nem válaszoltak erre a kérdésre (60 fő pedig nonprofit vállalkozás munkavállalója).

A demográfiai és munkahelyi adatok bemutatás után térjünk át a hipotézis vizsgálatra!

H1: A 30 évnél fiatalabbak információbiztonsági szempontból tudatosabbak, mint az idősebbek.

A kérdőívre érkezett adatok vizsgálatánál – a hipotézisnek megfelelően – először arra voltam kíváncsi, hogy van-e összefüggés a 30 év alatti és az annál idősebb korosztály információbiztonság-tudatossága között. (A válaszadók 36,2 százaléka volt 30 éves vagy annál fiatalabb.)

A kereszttábla elemzés (2. táblázat) a következő eredményeket hozta:

2. táblázat. **Khi-négyzet próba az első hipotézisnél**

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	30,966[a]	2	*,000*
Likelihood Ratio	32,363	2	,000
Linear-by-Linear Association	30,414	1	,000
N of Valid Cases	525		

[a]: 0 cells (0,0%) have expected count less than 5. The minimum expected count is 34,02.

Forrás: saját kutatás, a kérdőív adatai alapján

Az adatok alapján megállapítható, hogy van összefüggés a két változó között (a Khi-négyzethez tartozó p érték kisebb, mint 0,05)

3. táblázat. **A két változó közötti kapcsolat erősségének vizsgálata a Cramer V értéke alapján az első hipotézisnél**

		Value	Approximate Significance
Nominal by Nominal	**Phi**	,243	,000
	Cramer's V	*,243*	,000
N of Valid Cases		525	

Forrás: saját kutatás, a kérdőív adatai alapján

A Cramer V értéke alapján a kapcsolat erőssége közepes.

Megállapítható tehát, hogy közepes erősségű összefüggés van az életkor és az információbiztonság-tudatosság között, tehát a mintában szereplő 30 év alatti válaszadók kevésbé tudatosak, mint az idősebbek, így az első hipotézisemet el kell vetnem.

H2: KKV-k esetén az információbiztonság kevésbé hangsúlyos, mint a nagyvállalatoknál.

A hipotézis vizsgálathoz először meg kell nézni, hogy alakult a mintában a mikro-, kis- és középvállalkozásoknál (KKV-knál), valamint a nagyvállalatnál dolgozók összetétele.

4. táblázat. **A dolgozói összetétel vizsgálata**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	**1,00 KKV**	259	49,3	*60,1*	60,1
	2,00 Nagyvállalat	172	32,8	*39,9*	100,0
	Total	431	82,1	100,0	
Missing System		94	17,9		
Total		525	100,0		

Forrás: saját kutatás, a kérdőív adatai alapján

Ahogyan azt már fentebb említettük, az elemzésbe bevont válaszok száma 431 fő (94 fő jelölte, hogy jelenleg nem rendelkezik munkahellyel). A munkahellyel rendelkező válaszadók 60,1 százaléka dolgozik KKV-knál, 39,9 százalékuk pedig nagyvállalatnál.

Három kérdés segítségével vizsgáltam az információbiztonság megjelenésének hangsúlyát az elemzés során:

- Szokott-e információbiztonsággal kapcsolatban tájékoztatást, értesítést kapni a munkahelyén (pl. hírlevél, adathalász figyelmeztetés stb.)?
- Van-e információbiztonsággal kapcsolatos oktatás, képzés a munkahelyén?

– Van-e a munkahelyén információbiztonsággal foglalkozó részleg, vagy munkatárs?

A válaszok alapján, adatredukciós eljárással (index) három típust azonosítottam (5. táblázat):

1. Az információbiztonságot nagy hangsúllyal kezelő vállalkozások, ahol van információbiztonsággal foglalkozó részleg, tájékoztatás és oktatás is (35,7%).
2. Az információbiztonsággal valamilyen formában foglalkozó vállalkozások (35,7%).
3. Információbiztonsági részleggel nem rendelkező és a témában tájékoztatást vagy oktatást sem végző vállalkozás (28,5%).

5. táblázat **Az információbiztonság hangsúlya a vállalkozásnál (három kategóriába sorolva)**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	**1,00 A munkahelyemen hangsúlyosan kezelik az információbiztonság kérdését**	154	29,3	*35,7*	35,7
	2,00 A munkahelyemen van néhány kezdeményezés az információbiztonsággal kapcsolatban	154	29,3	*35,7*	71,5
	3,00 A munkahelyemen nincs információbiztonsági osztály, képzés vagy hírlevél	123	23,4	*28,5*	100,0
	Total	431	82,1	100,0	
Missing System		94	17,9		
Total		525	100,0		

Forrás: saját kutatás, a kérdőív adatai alapján

Ezt követően ismét kereszttábla segítségével vizsgáltam a második szakmai hipotézisemet, mely szerint a KKV-k esetén az információbiztonság kevésbé hangsúlyos, mint a nagyvállalatoknál.

6. táblázat. **Khi-négyzet próba eredménye a második hipotézisnél**

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	92,176[a]	2	*,000*
Likelihood Ratio	95,046	2	,000
Linear-by-Linear Association	84,326	1	,000
N of Valid Cases	431		

[a]: 0 cells (0,0%) have expected count less than 5. The minimum expected count is 49,09.

Forrás: saját kutatás, a kérdőív adatai alapján

A kereszttábla elemzés alapján megállapítható, hogy a Khi-négyzethez tartozó p érték (6. táblázat) ismét kisebb, mint 0,05, ezért a két változó között összefüggés van. A Cramer V (7. táblázat) erős kapcsolatot mutat a két változó között (0,462).

7. táblázat. **A két változó közötti kapcsolat erősségének vizsgálata a Cramer V értéke alapján a második hipotézisnél**

		Value	Approximate Significance
Nominal by Nominal	**Phi**	,462	,000
	Cramer's V	*,462*	,000
N of Valid Cases		431	

Forrás: saját kutatás, a kérdőív adatai alapján

H3: Az iskolai végzettséggel nő az információbiztonság-tudatosság

A harmadik hipotézisnél azt feltételeztem, hogy a magasabb iskolai végzettséggel rendelkezők jobban odafigyelnek az információbiztonságra, tehát az információbiztonság-tudatosság szintjük magasabb.

A válaszadóimat – adatredukciós eljárás segítségével – négy csoportba osztottam:

- érettségivel nem rendelkezőkre (10,1 százalék),
- érettségizettekre (33,3 százalék),

- felsőfokú végzettségűekre (51,4 százalék), valamint
- posztgraduális és doktori fokozattal rendelkezőkre (5,1 százalék).

Ezt követően kereszttábla elemzést végeztem (8. és 9. táblázat), melyek alapján több megállapítás is tehető a mintában szereplő válaszadókra.

***8. táblázat.* Khi-négyzet próba eredménye a harmadik hipotézisnél**

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	29,424[a]	6	*,000*
Likelihood Ratio	31,416	6	,000
Linear-by-Linear Association	14,424	1	,000
N of Valid Cases	525		

[a]: 0 cells (0,0%) have expected count less than 5. The minimum expected count is 8,43.

Forrás: saját kutatás, a kérdőív adatai alapján

A Khi-négyzethez tartozó p érték ismét kisebb, mint 0,05, ezért a két változó között összefüggés van. Az összefüggés erőssége (Cramer V) azonban gyenge kapcsolatot mutat (0,167).

***9. táblázat.* A két változó közötti kapcsolat erősségének vizsgálata a Cramer V értéke alapján a harmadik hipotézisnél**

		Value	Approximate Significance
Nominal by Nominal	**Phi**	,237	,000
	Cramer's V	*,167*	,000
N of Valid Cases		525	

Forrás: saját kutatás, a kérdőív adatai alapján

A végzettséggel növekszik az információbiztonság-tudatosság, ám ez a növekedés nem folytonos (az érettségivel nem rendelkezők inkább tudatosak, mint az érettségivel rendelkezők), a többi esetben azonban a végzettség növekedésével a tudatosság szintje is folyamatosan növekszik. Az elemzés alapján ezt a hipotézist elfogadom.

A hipotézis vizsgálatot követően térjünk át a kutatási kérdés megválaszolására! A kutatási kérdés a következő volt: Mi jellemzi a magyar embereket információbiztonság-tudatosság szempontjából?
A válaszadók tudatosságának a mérésére egy tudatosság indexet képeztem a következő állításokra adott válaszok alapján:

1. A közösségi oldalamra szívesen töltök fel fényképeket magamról.
2. Mindenhol ugyanazt a jelszót használom.
3. A jelszavaimat egy helyen tárolom (pl. Word dokumentum, telefon, notesz, jelszókezelő stb.).
4. A jelszavaimat jól látható/elérhető helyen tárolom.
5. Szívesen töltök le és telepítek programokat a számítógépemre.
6. Szívesen töltök le és telepítek alkalmazásokat a mobiltelefonomra.

Az állítások válaszadóra való jellemző vonását egy 5 fokú Likert-skálán lehetett értékelni, ahol az egyes érték jelentette azt, hogy az adott állítás egyáltalán nem jellemző a kitöltőre, míg az ötös érték azt mutatta, hogy az állítást teljesen magáénak érzi a válaszadó.
Az elemzés első lépéseként megvizsgáltam, hogy azonos irányba mutatnak-e a válaszok. Ezt követően meghatároztam, hogy melyik válasz számít tudatosnak, és mivel az elemzés szempontjából lényeges, hogy egy irányba álljanak a változók (tehát az egyes érték azt mutassa, hogy kevésbé tudatos, az ötös pedig, hogy nagyon tudatos), ezért elvégeztem a szükséges átalakításokat. Ezt követően előállítottam a tudatosság indexet.

A tudatosság indexből egy három kategóriás változót hoztam létre (10. táblázat).

10. táblázat. **A tudatossági index három kategóriája**

		Frequency	Percent	Cumulative Percent
Valid	**1,00 Kevésbé tudatos**	94	17,9	17,9
	2,00 Közepesen tudatos	289	55,0	73,0
	3,00 Tudatos	142	27,0	100,0
	Total	525	100,0	

Forrás: saját kutatás, a kérdőív adatai alapján

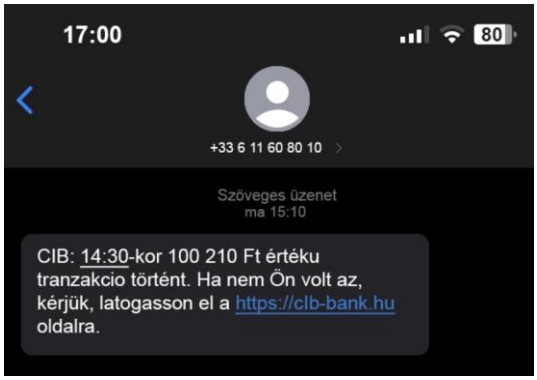
Az eredmények alapján a mintában szereplő válaszadók 17,9 százaléka kevésbé tudatos. Ez nem csak a közösségi médiában történő jelenlétet, információk, fényképek megosztását jelenti, hanem a jelszóhasználati szokásokat, illetve az alkalmazások, programok telepítését is. 27 százalékuk a válaszok alapján viszont tudatosnak tekinthető.

Ezt követően kereszttábla elemzés segítségével elvégeztem kutatási kérdésem vizsgálatát.

Bár nem szerepelt a kutatási kérdések között, kíváncsi voltam az átveréses támadásokkal kapcsolatos eredményekre is. Megvizsgáltam az internetes és telefonos csalásokkal kapcsolatos válaszadói immunitást, hiszen az elmúlt időszakban gyakran szereplő téma volt a médiában is.

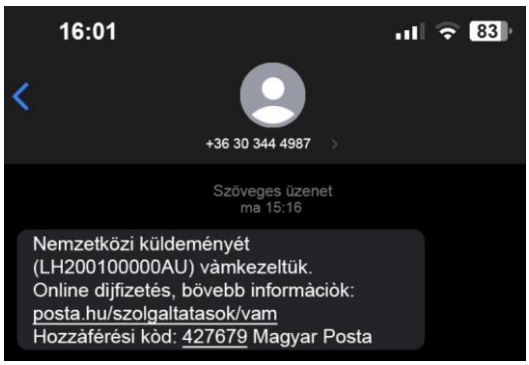
Az internetes és telefonos csalásokkal kapcsolatban négy kérdést fogalmaztam meg és a teljes mintára (525 fő) vizsgáltam, mert fontosnak tartottam a munkavállalói tudatosság mellett egy általános kép megismerését is.

Az alábbi SMS-t kapja a bankjától. Mit tesz?



4. ábra. **A kérdőívhez készített ábra (adathalász SMS-üzenet)**
Forrás: saját szerkesztés

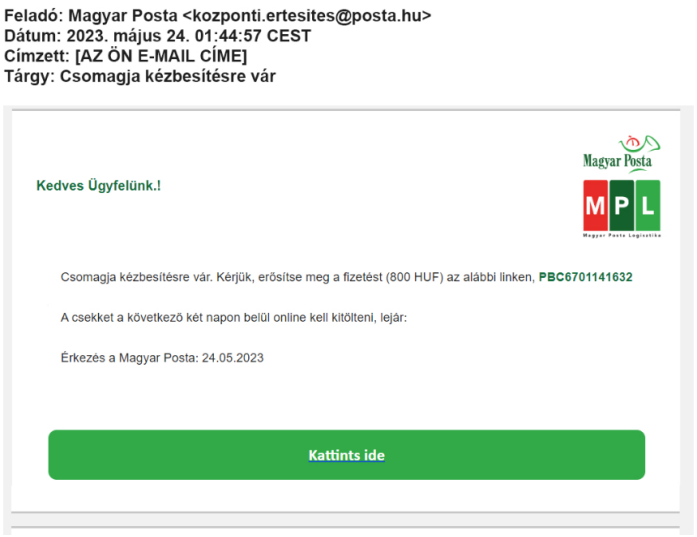
Nemzetközi csomagot vár. Telefonjára az alábbi SMS érkezik. Mit tesz?



5. ábra. **A kérdőívhez készített ábra (valódi SMS-üzenet)**
Forrás: saját szerkesztés

Telefonhívást kap. A hívó fél banki alkalmazottként mutatkozik be, egy gyanús tranzakcióval kapcsolatban keresi és ehhez a bankkártyaadatait kéri. Ebben az esetben mit tesz?

Nemzetközi csomagot vár. A képen látható e-mailt kapja. Mit tesz?



***6. ábra.* A kérdőívhez készített ábra (adathalász e-mail)**

Forrás: saját szerkesztés

A kérdőívben az erre vonatkozó kérdések a klasszikusnak mondható adathalász módszereket tartalmazta, ezekre kérdeztem rá én is. Fontosnak tartom megjegyezni, hogy a 5. ábrán található SMS-képen nem adathalász SMS szerepel, mégis a válaszadók 74,1%-a (tehát a válaszadók kétharmada) gyanúsnak vélte azt. Első lépésként megnéztem, hogy a kérdésekre melyik volt a jó válasz. Ezt követően négy csoportot képeztem aszerint, hogy ki és mennyi helyes választ adott. Ezt foglaltam össze a 11. táblázatban.

***11. táblázat* A helyesen megválaszolt kérdések aránya**

Helyesen megválaszolt kérdések	Százalék
3 kérdést rontott	2%
2 kérdést rontott	16%
1 kérdést rontott	69%
Minden kérdést helyesen megválaszolt	13%

Forrás: saját kutatás, a kérdőív adatai alapján

Döntő többségében (69 százalék) a válaszadók csak egy kérdést rontottak el, és nem volt olyan a kérdőív kitöltői között, aki az összes kérdést elrontotta volna.

Az eredmények rávilágítottak arra, hogy a válaszadók egyre tájékozottabbak az internetes és telefonos csalások terén, ám fontos tudatosítani, hogy a csalók újabb és újabb módszereket találnak ki, ezért minden esetben fenntartásokkal kezeljük a személyes adatainkat bekérő SMS-eket, telefonhívásokat vagy email-eket.

KÖVETKEZTETÉS

A vizsgálat eredményei alapján több megállapítás tehető az információbiztonsági tudatosság alakulásával kapcsolatban. A fiatalabb korosztály (30 év alattiak) esetében a várt tudatosabb hozzáállás nem igazolódott, a statisztikai elemzések alapján a 30 év feletti korcsoport mutatott magasabb tudatossági szintet. A vállalati méret és a biztonságtudatosság közötti kapcsolat viszont markáns: a nagyvállalatoknál dolgozók körében az információbiztonság hangsúlyosabban jelenik meg, amit a rendszeres képzések, tájékoztatások és dedikált szervezeti egységek is tükröznek. Ezzel szemben a KKV-szektorban jelentős a lemaradás, ami kockázatot jelenthet mind a szervezeti működés, mind a munkavállalói adatok biztonsága szempontjából. Az iskolai végzettség és az információbiztonsági tudatosság között ugyan kimutatható összefüggés, de az erőssége gyenge, így önmagában nem tekinthető meghatározó tényezőnek. Ezek a megállapítások rámutatnak arra, hogy az információbiztonság nem csupán technológiai, hanem társadalmi és szervezeti kérdés is, mely komplex megközelítést igényel.

A KUTATÁS KORLÁTAI

A kutatás során alkalmazott hólabda módszer nem biztosít reprezentativitást, így az eredmények a teljes magyar munkavállalói populációra nem vonhatóak le, csak a mintában szereplő válaszadókra általánosíthatóak. A kérdőív önkitöltős jellege torzíthatja az adatok megbízhatóságát, különösen az önbevalláson alapuló tudatossági szintek esetében. A válaszadók között felülreprezentáltak voltak a felsőfokú végzettségűek, mely szintén torzíthatja a mintát, valamint a kérdések

egyszerűsített megfogalmazása miatt bizonyos technológiai finomságok kimaradhattak a válaszokból.

ÖSSZEFOGLALÁS

A tanulmány arra a kérdésre kereste a választ, hogy a különböző társadalmi és szervezeti tényezők miként befolyásolják az információbiztonsági tudatosság szintjét a hazai munkavállalók körében. Az empirikus kutatás alapján megállapítható, hogy a nagyvállalati környezet és az idősebb korcsoport kedvezőbb információbiztonsági attitűdöket mutat, míg a KKV-k és a fiatalabb válaszadók esetében nagyobb kockázatok azonosíthatók. Az iskolai végzettség szerepe ugyan mérsékelt, de nem elhanyagolható. A kutatás hozzájárulhat a biztonságtudatos gondolkodás elterjesztéséhez, különösen a KKV-szektor fejlesztési stratégiáiban. A mesterséges intelligencia térnyerése és információbiztonsági vonatkozásai – különösen az AI-rendszerek átláthatósága, etikai kérdései és döntéshozatali szerepe – szorosan kapcsolódnak a vizsgált témakörhöz. Ezek részletes elemzése ugyanakkor meghaladta jelen tanulmány kereteit, és egy következő tanulmány központi vizsgálati irányát képezi majd.

FELHASZNÁLT FORRÁSOK

1. 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információ-biztonságáról. (2013). https://mkogy.jogtar.hu/jogszabaly?docid=a1300050.TV
2. 2024. évi LXIX. törvény Magyarország kiberbiztonságáról. (2024). https://mkogy.jogtar.hu/jogszabaly?docid=A2400069.TV
3. Ackoff, R. (1989). From Data to Wisdom. *Journal of Applied Systems Analysis,* 16, 3-9. University of Lancaster.
4. Alboqami, H. (2023). Factors Affecting Consumers Adoption of AI-Based Chatbots: The Role of Anthropomorphism. *American Journal of*

Industrial and Business Management, 13(4), 195. https://doi.org/10.4236/ajibm.2023.134014

5. Al-Zahrani, A. M. (2024). Unveiling the shadows: Beyond the hype of AI in education. *Heliyon*, 10(9). https://doi.org/10.1016/j.heliyon.2024.e30696
6. Calvano, M., Curci, A., Desolda, G., Esposito, A., Lanzilotti, R., & Piccinno, A. (2025). *Building Symbiotic AI: Reviewing the AI Act for a Human-Centred*, Principle-Based Framework. https://doi.org/10.48550/ARXIV.2501.08046
7. Christen, M., Blumer, H., Hauser, C., & Huppenbauer, M. (2019). *The Ethics of Big Data Applications in the Consumer Sector*. In Springer eBooks (p. 161). Springer Nature. https://doi.org/10.1007/978-3-030-11821-1_10
8. Copeland, B. J (szerk.) (2004): *The Essential Turing Seminal Writingsin Computing, Logic, Philosophy, Artificial Intelligence, and Artificial Life plus The Secrets of Enigma*. Oxford University Press
9. Cordero, J., Barba-Guamán, L., & Guamán, F. (2022). Use of chatbots for customer service in MSMEs. *Applied Computing and Informatics*. https://doi.org/10.1108/aci-06-2022-0148
10. Cox, S. R., Lee, Y., & Ooi, W. T. (2023). *Comparing How a Chatbot References User Utterances from Previous Chatting Sessions: An Investigation of Users' Privacy Concerns and Perceptions*. 105. https://doi.org/10.1145/3623809.3623875
11. Darwin, V., & Nkongolo, M. (2023). Data Protection for Data Privacy-A South African Problem? *arXiv* (Cornell University). https://doi.org/10.48550/arxiv.2306.09934
12. Davenport, T. H., & Prusak, L. (2001). *Tudásmenedzsment*. Kossuth Kiadó
13. *Digital Economy and Society Index (DESI)*. (2022) Európai Bizottság. https://digital-strategy.ec.europa.eu/hu/library/digital-economy-and-society-index-desi-2022 (utolsó hozzáférés: 2025.06.30.)

14. Drljača, D., & Latinović, B. (2017). *Audit in public administration's information systems – External or internal?* IOP Conference Series Materials Science and Engineering, 200, 12026. https://doi.org/10.1088/1757-899x/200/1/012026
15. Gémes Cs. (2017. december). Az információbiztonság alapkérdései, *Hadmérnök*, 12(4), 128-137.
16. Guan, H., Dong, L., & Zhao, A. (2022). Ethical Risk Factors and Mechanisms in Artificial Intelligence Decision Making. *Behavioral Sciences,* 12(9), 343. https://doi.org/10.3390/bs12090343
17. Hand, D. J. (2018). Aspects of Data Ethics in a Changing World: Where Are We Now? [Review of Aspects of Data Ethics in a Changing World: Where Are We Now?]. *Big Data*, 6(3), 176. Mary Ann Liebert, Inc. https://doi.org/10.1089/big.2018.0083
18. Helbing, D. (2013). From Technology-Driven Society to Socially Oriented Technology. The Future of Information Society -- Alternatives to Surveillance. arXiv (Cornell University). https://doi.org/10.48550/arxiv.1307.2397
19. Hermann, E. (2021). Leveraging Artificial Intelligence in Marketing for Social Good—An Ethical Perspective. *Journal of Business Ethics*, 179(1), 43. https://doi.org/10.1007/s10551-021-04843-y
20. Hernández, E. (2024). Towards an Ethical and Inclusive Implementation of Artificial Intelligence in Organizations: A Multidimensional Framework. *arXiv* (Cornell University). https://doi.org/10.48550/arxiv.2405.01697
21. Huang, L. (2023). Ethics of Artificial Intelligence in Education: Student Privacy and Data Protection. *Science Insights Education Frontiers*, 16(2), 2577. https://doi.org/10.15354/sief.23.re202

22. Huang, M., & Rust, R. T. (2020). A strategic framework for artificial intelligence in marketing. *Journal of the Academy of Marketing Science*, 49(1), 30. https://doi.org/10.1007/s11747-020-00749-9
23. Illésy M., Nemeslaki A., & Som Z. (2014). Elektronikus információbiztonság tudatosság a magyar közigazgatásban. *Információs Társadalom*, XIV, 1. szám. 52-73.
24. ISACA. (2013). *ISACA magyar szakkifejezés-gyűjtemény*.
25. Jacobs J., Haney J., & Furman S. (2022). *Measuring the Effectiveness of U.S. Government Security Awareness Programs: A Mixed-Methods Study* (Short Paper). Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022) 8th Workshop on Security Information Workers (WSIW 2022).
26. Koltay T. (2008. augusztus). A bölcsesség hierarchiája: az adat-, információ-, tudás-, bölcsességhierarchia reprezentációi, *Tudományos és Műszaki Tájékoztatás*, 55(8), 2008.
27. Kovács L., & Krasznay Cs. (2010). Digitális Mohács. *Nemzet és biztonság*, 3., 44-56.
28. Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computer & Security*, 25, 289-296, Elsevier BV. https://doi.org/10.1016/j.cose.2006.02.008
29. Kubaisi, A. A. S. H. A. (2024). Ethics of Artificial Intelligence a Purposeful and Foundational Study in Light of the Sunnah of Prophet Muhammad. *Religions*, 15(11), 1300. https://doi.org/10.3390/rel15111300
30. Larsson, S. (2018). Algorithmic governance and the need for consumer empowerment in data-driven markets. *Internet Policy Review*, 7(2). https://doi.org/10.14763/2018.2.791
31. Latham, A., & Goltz, N. (2019). *A Survey of the General Public's Views on the Ethics of Using AI in Education*. In Lecture notes in computer science (p.

194). Springer Science+Business Media. https://doi.org/10.1007/978-3-030-23204-7_17

32. Lee, R.-W., Choi, S.-H., & Hu, S.-H. (2023). Effect of temporal distance and goal type on predictions of future information security: Focus on moderation of self-efficacy and social responsibility. *Acta Psychologica*, 238. Elsevier BV. https://doi.org/10.1016/j.actpsy.2023.103990
33. Liu, F. (2020). A Statistical Overview on Data Privacy. *arXiv* (Cornell University). https://doi.org/10.48550/arxiv.2007.00765
34. Lou, C., Kang, H., & Tse, C. H. (2021). Bots vs. humans: how schema congruity, contingency-based interactivity, and sympathy influence consumer perceptions and patronage intentions. *International Journal of Advertising*, 41(4), 655. https://doi.org/10.1080/02650487.2021.1951510
35. Métayer, D. L., Danezis, G., Hansen, M., Hoepman, J.-H., Tirtea, R., Schiffner, S., & Domingo-Ferrer, J. (2015). Privacy and Data Protection by Design - from policy to engineering. *arXiv* (Cornell University). https://doi.org/10.48550/arxiv.1501.03726
36. Mitnick, K.D., & Simon, W. L. (2003). *The Art of Deception: Controlling the Human Element of Security*. Wiley Publishing.
37. Muha L. (2008). Az informatikai biztonság egy lehetséges rendszertana. *Bolyai szemle*, 17(4), 137-156.
38. Munk S. (2008). Információbiztonság vs. informatikai biztonság. *Hadmérnök*, 1-21.
39. Naik, N., Hameed, B. M. Z., Shetty, D. K., Swain, D., Shah, M., Paul, R., Aggarwal, K., Ibrahim, S., Patil, V., Smriti, K., Shetty, S., Prasad, B., Chłosta, P., & Somani, B. (2022). Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility? [Review of Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility?]. *Frontiers in Surgery*, 9. Frontiers Media. https://doi.org/10.3389/fsurg.2022.862322

40. Nazarov, A., Nazarov, D., & Kovtun D. (2021). *Information security of territorial stability.* E3S Web of Conferences, 291, 3018. https://doi.org/10.1051/e3sconf/202129103018
41. Olorunfemi, O. L., Amoo, O. O., Atadoga, A., Fayayola, O. A., Abrahams, T. O., & Shoetan, P. O. (2024). Towards A Conceptual Framework For Ethical Ai Development In *It Systems. Computer Science & IT Research Journal,* 5(3), 616. https://doi.org/10.51594/csitrj.v5i3.910
42. Pereira, F., Correia, R., Pinho, P., Lopes, S. I., & Carvalho, N. B. (2020). Challenges in Resource-Constrained IoT Devices: Energy and Communication as Critical Success Factors for Future IoT Deployment [Review of Challenges in Resource-Constrained IoT Devices: Energy and Communication as Critical Success Factors for Future IoT Deployment]. *Sensors*, 20(22), 6420. Multidisciplinary Digital Publishing Institute. https://doi.org/10.3390/s20226420
43. Pusztahelyi, R. (2021). Towards a European AI liability system. *Multidiszciplináris Tudományok,* 11(5), 317. https://doi.org/10.35925/j.multi.2021.5.35
44. Radziwill, N., & Benton, M. C. (2017). Evaluating Quality of Chatbots and Intelligent Conversational Agents. *arXiv* (Cornell University). https://doi.org/10.48550/arxiv.1704.04579
45. Rooy, D. V., & Bus, J. C. P. (2010). Trust and privacy in the future internet—a research perspective. Identity in the Information *Society*, 3(2), 397. https://doi.org/10.1007/s12394-010-0058-7
46. Rowley, J. (2007). The wisdom hierarchy: representations of the DIKW hierarchy. *Journal of Information Science*, 33 (2), 163-180.
47. SANS (2023). *Security Awareness Report, Managing Human Risk*., [Éves jelentés].
48. Schaik, P. van, Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour.

Computers in Human Behavior, 75, 547. https://doi.org/10.1016/j.chb.2017.05.038

49. Schlienger, T., & Teufel S. (2003). Information security culture - From analysis to change. *South African Computer Journal*, 46–52
50. Shehu, V. P., & Shehu, V. (2023). Human rights in the technology era – Protection of data rights. Deleted Journal, 7(2), 1. https://doi.org/10.2478/ejels-2023-0001
51. T.S. Eliot*, The Rock* (Faber & Faber, London, 1934)
52. Tarján G. (2020). *Az információbiztonsági tudatosság érettségi szintjének mérése szervezetekben* [Doktori értekezés]. Budapesti Corvinus Egyetem
53. Vágány P. (2023). *A leggyengébb láncszem vagy az utolsó védvonal? – Információbiztonság tudatosság gazdálkodó szervezeteknél*, METU, 2023 (diplomadolgozat)
54. Vágány, P. (2024). Ne legyen áldozat! Néhány gondolat az információbiztonságról. *Mezőgazdasági Technika*, 2024 április, pp 38-40
55. Weydner-Volkmann, S. (2023). Using Open, Public Data for Security Provision: Ethical Perspectives on Risk-Based Border Checks in the EU. *European Journal for Security Research*, 8, 25. https://doi.org/10.1007/s41125-023-00092-4
56. Wilson, M., & Hash, J. (2003). *Building an Information Technology Security Awareness and Training Program*. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-50
57. Zeleny, M. (1987). Management support systems: Towards integrated knowledge management*, Human Systems Management*, 7(1), 59–70.

ISSN 2630-886X

18 57

BGE