A digitális tudatosság a biztonsági és az agilis szemléletmód aspetkutsai mentén[1]

Berényi Csaba

Óbudai Egyetem, Biztonságtudományi Doktori Iskola,
berenyi.csaba@uni-obuda.hu

Csiszárik-Kocsir Ágnes

Egyetemi docens, Óbudai Egyetem, Keleti Károly Gazdasági Kar,
kocsir.agnes@kgk.uni-obuda.hu

Absztarkt: A digitális korszak térhódításával párhuzamosan egyre növekszik az igény a digitális kompetenciákra. Ugyanakkor párhuzamosan megjelennek azok a fenyegetettségek, amelyek fokozzák a technológiától való félelmet. Az elmúlt évtizedekben a világ biztonsági kihívásai egyre inkább komplex és dinamikus jellegűvé váltak. A biztonság központi kérdései az emberi jólétnek és a társadalmi stabilitásnak. A biztonság elsősorban az emberi élet és vagyon védelmét szolgálja. A biztonság, összekapcsolódik a környezeti, közlekedési és munkahelyi biztonság kérdéseivel is. Kiterjed a digitális területekre, mint például a kiberbiztonság, valamint a fizikai védelemre és az emberi erőforrásokra. Az új technológiák térnyerése és egyre mélyebb integrációja forradalmasította a biztonsági paradigmákat, mely egyben új dimenziókat nyit meg a fenyegetések kezelésében és a védelmi stratégiák kialakításában is. A kutatás fókuszában a biztonságtudatosság és a digitális technológiákba vetett bizalom áll, melyek kritikus szerepet játszanak az egyének digitális életvitelében.

Kulcsszavak: kockázat, biztonság, védelem, fenyegetettség, digitalizáció

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

1

1 Bevezetés

Az internet és a digitális környezet számos kihívást és veszélyt hordoz magában, melyeket ismerni és ismertetni kell. Az online térben való sikeres helytálláshoz tudás és tudatosság kell, melyek segítenek az embereknek felismerni, megérteni és hatékonyan kezelni ezeket a kockázatokat.

Az online térben sok személyes információ kerülhet veszélybe, például a banki adatok, személyes azonosítók és egyéb személyes adatok, melyeket sokszor óvatlanul adunk a csalók, illetéktelenek kezébe. Ehhez sokszor elég egy rossz helyre kattintás, vagy akár a felhasználási feltételek szükséges elfogadása. A tudatosság segíthet az online veszélyek felismerésében és a védekezésben is, mivel napjainkban kiberbiztonsági fenyegetések, például a vírusok és rosszindulatú szoftverek terjedése szinte megállíthatatlan. Az online tudatosság segít az embereknek megérteni, hogyan működik a szociális média, és hogyan lehet biztonságosan kezelni az online kommunikációt. Ez magában foglalja a személyes információk megosztásának kockázatait és az online zaklatás elleni védekezést is, mely szintén nem újkeletű dolog. Nem szabad megfeledkezni a digitális lábnyom és az online hírnév csorbulásáról sem (Garai-Fodor, & Popovics, 2023; Garai-Fodor, 2023). Az internetnek köszönhetően rekord sebességgel terjednek az információk, sok esetben kitörölhetetlen módon, évekre, évtizedekre megőrizve azokat (hangok, képek, videók, bejegyzések formájában). Az online térben való túlzott időtöltés és az internetes tartalmak fogyasztásának hatása lehet az egyén pszichológiai és érzelmi állapotára. Ezen hatások csak tudatos hozzáállással csökkenthetők, egészséges mederben tartva az online tartalomfogyasztás mennyiségét. Mindezen tényezők tudatos felimerése, és a rájuk vonatkozó stratégia kialakítása segíthet az online térben való biztonság növelésén, a negatív hatások csökkentésén egyaránt.

A digitális tér és szereplés számos új kompetenciát, készséget hívott életre. Ilyen az agilitás, agilis gondolkodás is. Az agilitás, vagyis a gyors alkalmazkodóképesség és reagálóképesség, rendkívül fontos a digitális tudatosság szempontjából. A digitális környezet gyorsan változik és fejlődik (Varga et al, 2023), és az agilitás lehetővé teszi az egyének és szervezetek számára, hogy hatékonyan kezeljék és alkalmazkodjanak ezekhez a változásokhoz. Az új technológiák, alkalmazások és eszközök folyamatosan jelennek meg és kerülnek alkalmazásra az online térben. Az agilitás lehetővé teszi az emberek számára, hogy gyorsan megismerjék és alkalmazzák ezeket az újdonságokat, lépést tartva ezzel a technológiai fejlődéssel. A kiberbiztonsági kockázatok és fenyegetések folyamatosan jelen vannak, újabb és újabb alakot öltve. Az agilis hozzáállásnak köszönhetően új kiberbiztonsági veszélyekre is fókusz kerül. Az agilitás kulcsfontosságú szerepet játszik a digitális transzformáció során is. Azok, akik gyorsan tudnak alkalmazkodni az új digitális technológiákhoz és üzleti modellekhez, versenyelőnyhöz juthatnak a piacon, szervezeti oldalról jobban meg tudják szólítani és érteni a fogyasztókat és felhasználókat. Az agilitás a tanulási

készségben is megnyilvánul. A digitális tudatosság terén az agilis emberek hajlandóak folyamatosan tanulni az új technológiákról, digitális készségekről és biztonsági gyakorlatokról (Tick & Beke, 2021; Mai & Tick, 2021, Mizser et. al., 2022, Garai-Fodor et. al. 2022). Az agilitás tehát nemcsak a technológiai változásokra való gyors reagálás szempontjából fontos, hanem az egyéni és szervezeti fejlődés, innováció, és a digitális környezetben való sikeres működés szempontjából is.

2 Szakirodalmi áttekintés

Amikor a kockázatról, a biztonságról beszélünk, az emberek általában intuíciójuk alapján értik ezeket, és ez a megértés bizonyos szinten általános. Ennek következtében a kockázat, a biztonság és a védelem fogalmának vizsgálata azt mutatja, hogy nincs igazán általánosan elfogadott és széles körben használt szemantikai alap, amely alapján a biztonság- és védelemtudományban használnának. A kockázatot és a biztonságot gyakran ábrázolják ellentétként, ám egyre többen felismerik és értik meg, hogy ez csak részben igaz és nem felel meg a modernebb átfogóbb nézeteknek. Azonban, ha a szavak jelentését és a fogalmakat minden aspektusból, teljeskörűen megértsük könnyen beleütközhetünk szemantikai és ontológiai vitákba (Aven, 2009; 2010, 2014; Aven et al., 2011; Blokland & Reniers, 2020).

A tudósok által adott meghatározások főként kétféle megkülönböztetésre utalnak a biztonság tekintetében. A legtöbb kutatás és szakirodalom a biztonságról alapvetően a mérnöki szempontokra, például a tervezésre és a kockázatelemzési módszerekre összpontosít. Alapvetően a biztonság a veszélyekre és a nem szándékos vagy véletlen kockázatokra összpontosít. Másik megközelítés szerint rosszindulatú fenyegetésekre és szándékos kockázatokra összpontosít. (Ale, 2009; Smith & Brooks, 2012; Pièrre-Cambacédès & Bouissou, 2013).

Leveson a biztonságot „balesetek vagy veszteségek hiányaként" definiálta (Leveson, 2020). A mérnöki szakmában dolgozók pontos meghatározásokat alkalmaznak erre a fogalomra, míg mások, például a társadalomtudományok területén, kevésbé körültekintően használják, kidolgozatlan definíciókat használnak, és néha a helyi kontextustól függően változtatják meg a meghatározást. A biztonság fogalmát a balesetektől (veszteségektől) való mentességként kezdték el leírni és alkalmazni a védelmi iparban, ahol a rendszer érintettjei által meghatározottak szerint minden olyan nem kívánt vagy nem tervezett esemény veszteséget eredményez. A védelem a hidegháború végéig szorosan kapcsolódott az állambiztonsághoz és a külföldi államok által jelentett fenyegetések elleni védelemhez. Ez időszakban az ilyen jellegű biztonság főként az állami szervezetek és a katonai erők felelősségi körébe tartozott (Leveson, 2020; Engen et al., 2021).

A veszély jelzi és megelőzi a fenyegetettséget, amely káros a biztonságra, vagy ártó események potenciális megjelenésére, meglétére utal (Csiszárik-Kocsir et al, 2022). A fenyegetettség már konkrétabb, jelentheti az anyagi lét korlátozását vagy az arra gyakorolt nyomást. Ebből következik, hogy biztonságról akkor beszélhetünk, ha a fenyegetettség minimális szinten jelentkezik. A biztonság tehát a veszély hiányát, vagy az e veszéllyel szembeni védelmet jelenti (Ürmösi, 2013).

A biztonság egy sokrétű fogalom, amely magában foglalja a fizikai, digitális, személyes és társadalmi aspektusokat. A biztonság és a kockázatok fogalmával, projektszintű kezelésével számos szakirodalmi forrás foglalkozik (Blaskovics et al, 2023a; 2023b). Az egyén számára a biztonság azt jelenti, amikor a szociális tényezők (társadalmi kapcsolatok, gazdasági körülmények) zavartalanul tudják kifejteni hatásukat, és nem fenyegeti őket közvetlen kriminológiai veszély (Garai-Fodor et al, 2023; Garai-Fodor, 2022). Társadalmi kontextusban azt fejezi ki, amikor a különböző társadalmi rendszerek zavartalanul és szabályozottan működnek, és tevékenységüket semmilyen belső veszély nem befolyásolja. A társadalom külső dimenziójában azt értjük alatta, hogy más államok, szervezetek vagy csoportok nem jelentenek veszélyt a társadalom működésére. A biztonság már régóta fontos szempont a szervezetek számára is. Ez értelmezésben azt az állapotot jelenti, amikor a szervezet egyes elemei, azok kapcsolódása, illetőleg a struktúra egésze normalizált körülmények közt funkcionál (Ürmösi, 2013). A veszélyes technológiák és tevékenységek megjelenésével olyan ágazatokban, mint az energia, a vegyipar, a közlekedés, a vízügy és az egészségügy kulcsfontosságú a biztonság. A biztonság a politika, a szabályozás és az irányítás egyik központi fogalma lett (Leveson, 1995; Macrae, 2014).

A biztonság terén a veszélyeket és fenyegetéseket ma már egyre inkább úgy határozzák meg, hogy a modern társadalom rendszerszintű kockázataiként és kihívásaiként tekintenek rájuk. Ebben a komplex és összetett kontextusban a kockázatok nem csupán szigetelt események vagy jelenségek, hanem szorosan összefüggő rendszerek szerves részei, amelyek átfogó megközelítést és széleskörű együttműködést igényelnek a hatékony megelőzés, kezelés és reagálás érdekében. Az egyre fejlődő technológia, globalizáció és más társadalmi változások hatására a biztonság terén egyre összetettebb kihívásokkal kell szembenéznünk, amelyek megkövetelik az innovációt (Varga, 2023a; Varga, 2023b), az intelligens megoldásokat, és a változó környezeti feltételekhez szükséges folyamatos adaptációt (Kriaa et al., 2015, Skierka, 2018).

A biztonság közötti fogalmi különbségek sok összefüggésben tovább bővültek például a tudomány és a technológia által. A technológia egyre növekvő elterjedése és annak intenzív használata miatt emelkedik a technológiák által okozott károk kockázata is (Engen et al., 2021).

A biztonság és annak különféle részei összetett rendszert alkotnak, ami érinti a nemzetközi, nemzeti és szervezeti területeket is, ahol egymásra gyakorolt hatásuk egyre közvetlenebb és erőteljesebb. Minden biztonsági fogalom alapvető

elvárásaként fogalmazza meg a rendszer és az alrendszerek védelmét a sérülésekkel szemben, valamint azok sérülésmentes állapotát (Ürmösi, 2013). A rendszerek megnövekedett összekapcsolhatóságával együtt növekedett a nemkívánatos következmények kockázata is, mivel fennáll a szándékos károkozás következménye (Young & Leveson, 2014). A biztonságot gyakran rendszertulajdonságként definiálják, mely lehetővé teszi a rendszer számára küldetésének vagy kritikus funkcióinak - a fenyegetések által jelentett kockázatok ellenére történő – végrehajtását (Kissel, 2006).

Manapság szükség van a biztonság- és védelmi mérnöki megközelítések integrálására oly módon, hogy a hibás működés vagy rosszindulatú szándék okozta, ésszerűtlen károsodás kielégítő módon legyen kezelhető, melyhez sokszor rugalmas, agilis hozzáállás szükséges (Tóth – Csiszárik-Kocsir 2022a; 2022b; Dobos et al, 2022). A modern összekapcsolt biztonságkritikus rendszerek csak akkor tekinthetők biztonságosnak, ha azok külön részeiben is biztonságosak, ez azonban egy biztonságos és védett rendszer tervezését igényli. Az igénytervezés esetében minél korábban sikerül elérni a biztonság és a védelem integrációját, annál kevesebb iterációra van szükség az összehangoláshoz (Schmittner et al., 2015, Kriaa et al., 2015, Young & Leveson, 2013).

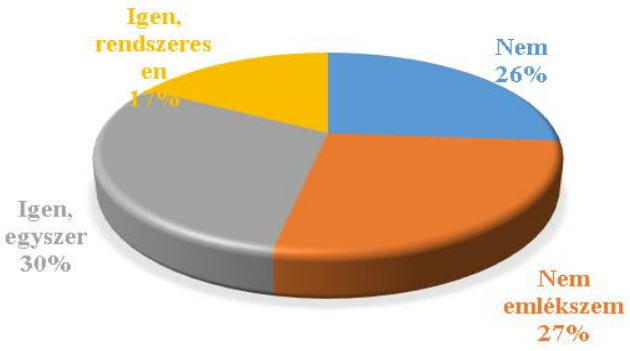
A valós életben a kritikus infrastruktúra védelme gyakran azon kritikus információs rendszerek vagy infrastruktúrák védelmét jelenti, amelyek az információs támadások vagy veszélyeztetések ellen vannak védve. A kritikus infrastruktúra védelme és a kritikus információs infrastruktúra védelme kapcsolódik más szakterületekhez is. Ezek közé tartozik például a működés folytonossága, a kormányzati tevékenység folytonossága, az információs tér biztonsága, valamint az információs és informatikai biztonság (Tokody et al., 2018). Az életünk ma már elképzelhetetlen a fizikai és a virtuális világ összekapcsolása nélkül. A kiber-fizikai rendszerek létrehozásával a számítástechnikai elemek bevezetése számos széles körű problémát vet fel, amelyek nem mindig kerülnek elő a hagyományos mérnöki gondolkodás során. A biztonság tradicionálisan az adat- vagy kommunikációbiztonság problémaként kerül kezelésre, és ezt informatikusoknak vagy számítógép-mérnököknek kell megoldaniuk (Haig, 2016; Babos, 2018).

A digitális eszközök és az internet adta lehetőségek már mindenütt jelen vannak a mai társadalomban. A digitális kultúra alapvető fontosságú a hatékony kommunikációhoz és a kapcsolatépítéshez. Az elmúlt években folyamatosan bővült a digitális technológiákból adódó kockázatok és sebezhetőségek listája azon hatásokkal kapcsolatban, amelyek kiberfenyegetéseket, függőségeket okozhatnak (Wilmer et al., 2017). A digitális eszközök biztonságos, etikus és megfelelő használata kulcsfontosságú, hogy aktívan részt vehessünk a társadalmi, szakmai és személyes kapcsolatokban. A digitális térben való részvétel nem csak egyéni szintű, hanem társadalmi szinten is megköveteli a felhasználók digitális jogainak védelméről, az információbiztonságról és az adatvédelemről történő gondoskodást. A biztonsági szolgáltatóknak a "klasszikus" biztonsági

módszereket, például a titkosítást, a személyazonosság-kezelési technikákat, az eszközhitelesítési mechanizmusokat, a digitális tanúsítványokat, a digitális aláírásokat és a vízjeleket új környezethez kell igazítaniuk. Mivel a különböző rendszerek elleni támadások egyre kifinomultabbak, a védekezések kidolgozása továbbra is kihívást jelent és folyamatos feladat marad. A biztonsági módszerek fejlesztésével alapvető elvárás, hogy azok megfelelő adatvédelmet biztosítsanak minden érintett számára (Ukil et al., 2011, Popescul & Genete, 2016).

3 Anyag és módszer

A jelen tanulmányunkban a különböző generációk biztonsághoz való hozzáállást mérjük fel egy olyan komplex, több témát vizsgáló kérdőív segítségével, mely a biztonságtudatosság, a jelenkor kihívásai mellett az alapkompetenciák (agilitás, tudatos internethasználat) mérésre is vállalkozik. A kutatás 2023 őszén zajlott le, és összesen 5067 értékelhető kérdőív alapján vonjuk le a következtetéseinket. A kérdőívet döntő többségében Z generációs (54,5%), valamint X (25,7%), és Y (19,9%) generációs válaszadók töltötték ki. A megkérdezést online hajtottuk végre. A méréshez egy négyfokozatú Likert-skálát használtunk, ahol az 1-es érték a feltett kérdés kapcsán mért teljes egyet nem értést, a 4-es érték pedig a nagyon erős, teljes egyetértést jelentette. Jelen tanulmányunkban bemutatott eredmények a válaszadók korábbi biztonsági oktatásban való részvétele alapján kerülnek bemutatásra. A minta összetételét az alábbi ábra mutatja:



1.ábra: A minta összetétele a válaszadók korábbi biztonságai oktatásban való részvétele alapján
Forrás: saját kutatás, 2023, N = 5067

4 Eredmények

Elsőként arra voltunk kíváncsiak, hogy hogyan értékelik a válaszadók a feltett állításokat. A kapott eredményeket az átlag és a szórás értéke alapján mutatjuk be. Az állítások a digitalizációra, és az online térre vonatkoztak, valamint az ott való szerepvállalásra, működésre. A kapott eredmények alapján látható, hogy a válaszadók gyakorlatilag az életünk részeként tekintenek a digitális térre. A digitális lehetőségek véleményük szerint jelentős mértékben át fogják írni a jövő munkaerőpiacát, amelyre már most láthatók az igencsak agresszíven előre törő kezdeményezéseket a mesterséges intelligencia képében. Mindemellett azt is igen magas átlagértékkel, közel három egész körüli átlaggal jellemezték a válaszadók, hogy a digitalizáció megkönnyíti az életünket. Önmagában igaz is ez az állítás, de itt jön be a képbe az a korábban már említett tudatossági dimenzió, amely annak veszélyeire hívja fel a figyelmet. A mesterséges intelligencia tekintetében is elég erőteljes volt a válaszadók egyetértése, hogy az is hatással lesz a jövő munkaerőpiacára. Összességében az látható, hogy a digitalizációt a válaszadók jó dolognak tekintik, és azt is látják, hogy milyen átalakulások előtt van a digitalizációs törekvéseknek köszönhetően a munkaerőpiac.

	Átlag	Szórás
A digitalizáció hasznos, mert megkönnyíti az életünket.	2,962	1,072
A digitális tartalmak érdekesebbek és szórakoztatóbbak számomra, mint a hagyományos kommunikáció.	2,390	1,101
Online térben jobban érzem magam, mint Offline térben.	2,183	1,145
Sokszor magabiztosabb vagyok az online térben, mint a valóságban.	2,322	1,164
Az online térben könnyebben megvalósíthatom álmaimat.	2,253	1,150
A digitalizáció jelentős mértékben meghatározza a jövő munkaerőpiacát.	2,984	1,159
A mesterséges intelligencia jelentős mértékben meghatározza a jövő munkaerőpiacát.	2,879	1,205

1.táblázat: A feltett állítások átlagértékei és szórásai
Forrás: saját kutatás, 2023, N = 5067

A továbbiakban megvizsgáltuk azt is, hogy a minta szegmentálásához használt kritériumok mentén, az egyes csoportok között hogyan változnak ezek az átlagértékek, kifejezettem a biztonságtudatosságra való felkészülés szempontjából. Az látható, hogy azok a válaszadók, akik rendszeresen vesznek részt biztonságtudatosságot növelő képzéseken egyértelműen látják a digitalizáció

előnyeit. Akik ilyen képzésen nem vettek részt, azok a legalacsonyabb átlagértékkel jellemezték ezt a kérdést. A digitális tartalmakra, azok szórakoztató jellegére vonatkozó állításokat azoknál láthatunk legmagasabb átlagértékkel jellemezve, akik eddig életükben csak egyszer vettek részt ilyen ismeretbővítő képzésen. Az online térben való magabiztosság, jólét szempontjából szintén ugyanez a csoport adott kiemelkedő, átlag feletti értéket az állításnak. Ez azért jelent problémát, mert egy alkalommal történő biztonság tudatosságot növelő oktatás nem tud elegendő információt adni ahhoz, hogy valaki biztonsággal tudjon működni az online térben. Itt mindenképpen szükséges az, hogy nagyobb teret adjunk az ilyen képzéseknek a hamis biztonságérzet elkerülése céljából. A továbbiakban a munkaerőpiacra, a mesterséges intelligencia munkát kiváltó szerepére vonatkozóan azoktól a válaszadóktól jött a legmagasabb értékelést, akik rendszeresen részt vesznek biztonság tudatosságot növelő képzésen. Ez az állítás, valamint a kapott eredmények azért érdekesek, mert akik ismerik a rendszer árnyoldalait, jobban, tudatosabban tudják használni azokat az eszközöket, amelyeket tényleg lehetőségként kínál a digitalizáció számunkra.

					95% Confidence Interval for Mean	
		Mean	Std. Deviation	Std. Error	Lower Bound	Upper Bound
A digitalizáció hasznos, mert megkönnyíti az életünket.	Nem	2,790	1,089	0,030	2,731	2,849
	Nem emlékszem	2,974	1,072	0,029	2,917	3,031
	Igen, egyszer	3,010	1,047	0,027	2,958	3,063
	Igen, rendszeresen	3,126	1,056	0,036	3,055	3,197
	Total	2,962	1,072	0,015	2,933	2,992
A digitális tartalmak érdekesebbek és szórakoztatóbbak számomra, mint a hagyományos kommunikáció.	Nem	2,416	1,098	0,030	2,357	2,476
	Nem emlékszem	2,318	1,106	0,030	2,259	2,377
	Igen, egyszer	2,446	1,096	0,028	2,390	2,501
	Igen, rendszeresen	2,362	1,099	0,038	2,288	2,436
	Total	2,390	1,101	0,015	2,359	2,420
Online térben jobban érzem magam, mint Offline térben.	Nem	2,238	1,156	0,032	2,176	2,300
	Nem emlékszem	2,054	1,125	0,030	1,994	2,113
	Igen, egyszer	2,276	1,143	0,029	2,219	2,334
	Igen, rendszeresen	2,135	1,142	0,039	2,058	2,212

	Total	2,183	1,145	0,016	2,151	2,214
Sokszor magabiztosabb vagyok az online térben, mint a valóságban.	Nem	2,369	1,172	0,032	2,306	2,432
	Nem emlékszem	2,256	1,162	0,031	2,194	2,318
	Igen, egyszer	2,398	1,162	0,030	2,339	2,456
	Igen, rendszeresen	2,221	1,147	0,039	2,144	2,298
	Total	2,322	1,164	0,016	2,290	2,354
Az online térben könnyebben megvalósíthatom álmaimat.	Nem	2,310	1,160	0,032	2,248	2,373
	Nem emlékszem	2,158	1,142	0,031	2,098	2,219
	Igen, egyszer	2,333	1,143	0,029	2,276	2,391
	Igen, rendszeresen	2,174	1,147	0,039	2,097	2,251
	Total	2,253	1,150	0,016	2,222	2,285
A digitalizáció jelentős mértékben meghatározza a jövő munkaerőpiacát.	Nem	2,819	1,165	0,032	2,757	2,882
	Nem emlékszem	2,947	1,181	0,032	2,884	3,010
	Igen, egyszer	3,033	1,120	0,029	2,977	3,089
	Igen, rendszeresen	3,214	1,139	0,039	3,137	3,291
	Total	2,984	1,159	0,016	2,952	3,016
A mesterséges intelligencia jelentős mértékben meghatározza a jövő munkaerőpiacát.	Nem	2,710	1,213	0,033	2,645	2,775
	Nem emlékszem	2,845	1,222	0,033	2,780	2,910
	Igen, egyszer	2,958	1,179	0,030	2,899	3,017
	Igen, rendszeresen	3,053	1,178	0,040	2,974	3,132
	Total	2,879	1,205	0,017	2,845	2,912

2.táblázat: A feltett állítások átlagértékei és szórásai
Forrás: saját kutatás, 2023, N = 5067

A biztonsági oktatásban való részvétel hatását a kérdések megítélésére varianciaanalízis segítségével vizsgáltuk meg. A (0,05 alatti) szignifikancia értékek alapján elmondható, hogy a digitális térben való tájékozódás, az ott való szereplés, a digitalizáció, mint eszköz munkaerő-piaci szereplését tekintve látható, hogy minden esetben hatás gyakorol rá a biztonság tudatosság, és az ehhez kapcsolódó képzés megléte.

		Sum of Squares	df	Mean Square	F	Sig.
A digitalizáció hasznos, mert megkönnyíti az életünket.	Between Groups	65,912	3	21,971	19,323	0,000
	Within Groups	5756,813	5063	1,137		
	Total	5822,725	5066			
A digitális tartalmak érdekesebbek és szórakoztatóbbak számomra, mint a hagyományos kommunikáció.	Between Groups	13,332	3	4,444	3,674	0,012
	Within Groups	6123,637	5063	1,209		
	Total	6136,970	5066			
Online térben jobban érzem magam, mint Offline térben.	Between Groups	42,078	3	14,026	10,763	0,000
	Within Groups	6598,060	5063	1,303		
	Total	6640,138	5066			
Sokszor magabiztosabb vagyok az online térben, mint a valóságban.	Between Groups	26,310	3	8,770	6,493	0,000
	Within Groups	6838,404	5063	1,351		
	Total	6864,714	5066			
Az online térben könnyebben megvalósíthatom álmaimat.	Between Groups	31,726	3	10,575	8,026	0,000
	Within Groups	6670,903	5063	1,318		
	Total	6702,629	5066			
A digitalizáció jelentős mértékben meghatározza a jövő munkaerőpiacát.	Between Groups	86,475	3	28,825	21,730	0,000
	Within Groups	6716,262	5063	1,327		
	Total	6802,737	5066			
A mesterséges	Between	74,678	3	24,893	17,303	0,000

intelligencia jelentős mértékben meghatározza a jövő munkaerőpiacát.	Groups					
	Within Groups	7283,678	5063	1,439		
	Total	7358,355	5066			

3.táblázat A feltett állítások átlagértékei és szórásai
Forrás: saját kutatás, 2023, N = 5067

Összefoglalás, következtetések

Összességében elmondható, hogy a digitális tudatosság napjainkban egy fontos kompetenciává nőtte ki magát. Míg korábban csak a klasszikus kompetencia készletből kellett válogatnunk a munkaerőpiac és a munkavállalás szempontjából, addig a 21. században ez kiegészült számos más tényezőkkel is. Megjelent az agilitás, mint a rugalmas hozzáállás alternatívája, és mint egy filozófia, amely a gyorsan változó világra képes választ adni. Emellett megjelent a tudatosság kérdése, amelyet korábban csak pénzügyi oldalról vizsgáltunk, de manapság most már inkább a digitális oldalát is nézni kell ennek a fogalomnak. Az új készségek és kompetenciák megjelenése új irányokat vet fel az oktatásban és a képzésben is. Fontossá vált az olyan képzések köre is, amelyek digitális tudatosságot, vagy csak önmagában véve az online térben való tudatos szerepvállalást erősítik. A kutatás alapján látható, hogy a válaszadók generációtól függetlenül nem zárkóznak el a digitális világban való szerepléstől, amit nem is tehetnek meg, hiszen az már az életünk részévé vált. Azonban látható, hogy akik kaptak bármiféle digitális tudatosságot növelő képzést, azok teljesen másképp látják a feltett állításokon keresztül vizsgált tényezőket. Ezért nagyon fontos, hogy a jövőben minél több teret adjunk az ilyen, és ehhez hasonló kezdeményezéseknek a megfelelő kompetenciákra fókuszálva annak érdekében, hogy a digitális tér hozta kockázatokat, és bizonytalansági faktorokat a lehető legminimálisabbra csökkentsük, és a lehető leghatékonyabban azonosítsuk és kezeljük.

Köszönetnyilvánítás

A 2021-1.2.4-TÉT-2021-00042 számú projekt a Kulturális és Innovációs Minisztérium Nemzeti Kutatási Fejlesztési és Innovációs Alapból nyújtott támogatásával, a 2021-1.2.4 TÉT pályázati program finanszírozásában valósult meg.

Irodalomjegyzék

[1] Ale, B. (2009). Risk: an introduction: the concepts of risk, danger and chance. Routledge.

[2] Aven, T. (2009). Safety is the antonym of risk for some perspectives of risk. Safety Science, 47(7), pp. 925-930.

[3] Aven, T. (2010). On how to define, understand and describe risk. Reliability Engineering & System Safety, 95(6), pp. 623-631.

[4] Aven, T. (2014). What is safety science?. Safety science, 67, pp. 15-20.

[5] Aven, T., Renn, O., & Rosa, E. A. (2011). On the ontological status of the concept of risk. Safety Science, 49(8-9), pp. 1074-1079.

[6] Babos, T. (2018). A Digitális Jólét Program biztonság-, védelem-és katonapolitikai relevanciái. HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA, 28(E-szám), 122.

[7] Blokland, P. J., & Reniers, G. L. (2020). The Concepts of Risk, Safety, and Security: A Fundamental Exploration and Understanding of Similarities and Differences. The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice, pp. 9-16.

[8] Csiszárik-Kocsir, Á. - Varga, J. - Garai-Fodor, M. (2022): External professional assistance for small and medium-sized enterprises to solving the challenges of the pandemic. In: Szakál, Anikó (szerk.) IEEE 20th Jubilee International Symposium on Intelligent Systems and Informatics (SISY 2022). Szabadka. Szerbia: IEEE (2022) 457 p. pp. 189-193.

[9] Engen, O. A. H., Gould, K. A. P., Kruke, B. I., Lindøe, P. H., Olsen, K. H., & Olsen, O. E. (2021). Perspektiver på samfunnssikkerhet.

[10] Garai-Fodor,M.,Varga, J., Csiszárik-Kocsir, Ág. (2022): Generation-specific perceptions of financial literacy and digital solutions. In: IEEE (szerk.) IEEE 20th Jubilee World Symposium on Applied Machine Intelligence and Informatics SAMI (2022) : Proceedings. Poprad, Szlovákia : IEEE (2022) 507 p. pp. 193-200. , 8 p.

[11] Haig, Zs. (2016). Katonai műszaki tudományok a 21. században. HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA, 26(1-2), pp. 115-116.

[12] Kissel, R. (2006). Glossary of Key Information Security Terms. Gaithersburg, MD, USA: U.S. Dept. of Commerce, National Institute of Standards and Technology

[13] Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., & Halgand, Y. (2015). A survey of approaches combining safety and security for industrial control systems. Reliability engineering & system safety, 139, pp. 156-178.

[14] Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., & Halgand, Y. (2015). A survey of approaches combining safety and security for industrial control systems. Reliability engineering & system safety, 139, pp. 156-178.

[15] Leveson, N. (2020). Safety and security are two sides of the same coin. The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice, pp. 17-27.

[16] Leveson, N. G. (1995). Safeware: system safety and computers. ACM.

[17] Macrae, C. (2014). Close calls: managing risk and resilience in airline flight safety. Springer.

[18] Mizser,Cs., Garai-Fodor, M., Csiszárik-Kocsir, Á. (2022): Key competences of young entrepreneurs in the world of digitalisation based on the results of a Hungarian questionnaire research. In: Szakál, Anikó (szerk.) IEEE 10th Jubilee International Conference on Computational Cybernetics and Cyber-Medical Systems ICCC 2022. Budapest, Magyarország : IEEE Hungary Section (2022) 401 p. pp. 281-286. , 6 p.

[19] Munk, S. (2008). Kritikus infrastruktúrák védelme információs támadások ellen. Hadtudomány XVIII.: (1-2.) pp. 95-106.

[20] Piètre-Cambacédès, L., & Bouissou, M. (2013). Cross-fertilization between safety and security engineering. Reliability Engineering & System Safety, 110, pp.110-126.

[21] Popescul, D., & Genete, L. D. (2016). Data security in smart cities: challenges and solutions. Informatica Economică, 20(1).

[22] Schmittner, C., Ma, Z., Schoitsch, E., & Gruber, T. (2015, April). A case study of fmvea and chassis as safety and security co-analysis method for automotive cyber-physical systems. In Proceedings of the 1st ACM Workshop on Cyber-Physical System Security pp. 69-80.

[23] Skierka, I. M. (2018, March). The governance of safety and security risks in connected healthcare. In Living in the Internet of Things: Cybersecurity of the IoT-2018, pp. 1-12 IET.

[24] Smith, C., & Brooks, D. J. (2012). Security science: The theory and practice of security. Butterworth-Heinemann.

[25] Tokody, D., Albini, A., Ady, L., Rajnai, Z., & Pongrácz, F. (2018). Safety and security through the design of autonomous intelligent vehicle systems and intelligent infrastructure in the smart city. Interdisciplinary Description of Complex Systems: INDECS, 16(3-A), pp. 384-396.

[26] Ukil, A., Sen, J., & Koilakonda, S. (2011) Embedded security for Internet of Things. In 2011 2nd National Conference on Emerging Trends and Applications in Computer Science pp. 1-6. IEEE.

[27] Ürmösi, K. (2013). A biztonság, a biztonság fogalma= The security, the concept of security. Hadtudományi Szemle, pp. 147-154.

[28] Varga, J. (2023a). SMEs as the innovation flagships - where are the real economic drivers? In: Szakál, Anikó (szerk.) IEEE 23rd International

Symposium on Computational Intelligence and Informatics (CINTI 2023): Proceedings. Danvers (MA), Amerikai Egyesült Államok: IEEE (2023) pp. 373-377.

[29] Varga, J. (2023b). Exploring the link between competitiveness and innovation In: Szakál, Anikó (szerk.) SISY 2023 IEEE 21st International Symposium on Intelligent Systems and Informatics Budapest. Magyarország: IEEE Hungary Section (2023) 663 p. pp. 229-233.

[30] Wilmer, H. H., Sherman, L. E., & Chein, J. M. (2017). Smartphones and cognition: A review of research exploring the links between mobile technology habits and cognitive functioning. Frontiers in psychology, 8, 605.

[31] Young, W., & Leveson, N. (2013, December). Systems thinking for safety and security. In Proceedings of the 29th Annual Computer Security Applications Conference, pp. 1-8

[32] Young, W., & Leveson, N. G. (2014). An integrated approach to safety and security based on systems theory. Communications of the ACM, 57(2), pp. 31-35.

[33] Garai-Fodor, M., & Popovics, A. (2023). Analysing the Role of Responsible Consumer Behaviour and Social Responsibility from a Generation Specific Perspective in the Light of Primary Findings. Acta Polytechnica Hungarica 20(3) pp. 121-134.

[34] Garai-Fodor, M. (2023). Digitalisation trends based on consumer research. IEEE 17th International Symposium on Applied Computational Intelligence and Informatics SACI 2023. Proceedings. Budapest. IEEE Hungary Section. 2023, pp. 349-352.

[35] Tick, A. & Beke, J. (2021). Online, Digital or Distance? – Spread of Narratives in ICT-supported Education. Journal Of Higher Education Theory And Practice, 21(6), pp. 15-31.

[36] Mai, P.T.& Tick, A. (2021). Cyber Security Awareness and Behavior of Youth in Smartphone Usage: A Comparative Study between University Students in Hungary and Vietnam. Acta Polytechnica Hungarica. 18(8) pp. 67-89.

[37] Garai-Fodor, M., Vasa, L., Jäckel, K. (2023). Characteristics of segments according to the preference system for job selection, opportunities for effective incentives in each employee group. Decision Making: Applications in Management and Engineering 6(2) pp. 557-580.

[38] Garai-Fodor, M. (2022). The Impact of the Coronavirus on Competence, from a Generation-Specific Perspective. Acta Polytechnica Hungarica. 19(8) pp. 111-125.

[39] Blaskovics, B., Maró, Z.M., Klimkó, G., Papp-Horváth, V. & Csiszárik-Kocsir, Á. (2023a). Differences between Public-Sector and Private-Sector Project Management Practices in Hungary from a Competency Point of View. Sustainability, 15(14) Paper: 11236

[40] Blaskovics, B., Czifra, J., Klimkó, G., & Szontágh, P. (2023b). Impact of the Applied Project Management Methodology on the Perceived Level of Creativity. Acta Polytechnica Hungarica, 20(3), pp. 101-120.

[41] Tóth, I.M. & Csiszárik-Kocsir, Á. (2022a). Assessing the agile approach to critical infrastructure in the light of primary research. In: Szakál, A. (ed.) 2022 IEEE 26th International Conference on Intelligent Engineering Systems (INES 2022) IEEE Hungary Section. pp. 207-211. ,

[42] Tóth, I.M. & Csiszárik-Kocsir, Á. (2022b). Teleworking and the home office – the digital possibilities in work organization. In: Szakál, A. (ed.) IEEE 10th Jubilee International Conference on Computational Cybernetics and Cyber-Medical Systems ICCC 2022, IEEE Hungary Section, pp. 277-280.

[43] Dobos, O., Tóth, I.M., Csiszárik-Kocsir, Á., Garai-Fodor, M. & Kremmer, L. (2022). How Generation Z managers think about the agility in a world of digitalization. In: IEEE (ed.) IEEE 20th Jubilee World Symposium on Applied Machine Intelligence and Informatics SAMI (2022) : Proceedings Poprad, pp. 207-212.

[44] Varga, J., Csiszárik-Kocsir, Á., Bíró, B.E:, Székely, K.K, Bíró, B.J., Garai-Fodor, M. (2023). Change Management Practices and the Impact of the Pandemic on Hungarian and Romanian SMEs. In: Szakál, Anikó (szerk.) IEEE 17th International Symposium on Applied Computational Intelligence and Informatics SACI 2023: Proceedings. Budapest, Magyarország: Óbudai Egyetem, IEEE Hungary Section (2023) 818 p. pp. 273-278.