Az IOTS-eszközök átfogó elemzése

Viktor Patrik

Egyetemi tanársegéd, Óbudai Egyetem Keleti Károly Gazdasági Kar, viktor.patrik@uni-obuda.hu

Garai-Fodor Mónika

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

Absztrakt: A gyors technológiai fejlődéssel jellemezhető korszakban az 5G hálózatok megjelenése átalakító ugrást jelent a távközlésben, és azt ígéri, hogy páratlan sebességével és csatlakoztathatóságával újradefiniálja digitális interakcióinkat. Ezt az áttörést azonban az informatikai biztonsággal kapcsolatos növekvő aggodalmak kísérik, amint arra az Óbudai Egyetemről Patrik Viktor és Fodor Monika által végzett átfogó kutatás is rávilágít. Tanulmányuk az IT-biztonsággal és az 5G hálózatokkal kapcsolatos árnyalt felfogásokat és attitűdöket vizsgálja a különböző generációs kohorszok körében, kvantitatív megközelítést alkalmazva egy szigorúan előre tesztelt, szabványosított kérdőív segítségével. A vizsgálat, amely 443 értékelhető kérdőívből gyűjtött betekintést, jelentős generációs különbségeket tár fel az informatikai biztonsági fenyegetések megértésében és az emberi tényezők hangsúlyozásában az informatikai biztonsági kereteken belül.

Kulcsszavak: 5G hálózat, IOT hógolyó, IOT

1 Bevezetés

A modern korban, amikor a digitális tájkép folyamatosan fejlődik, az ötödik generációs (5G) mobilhálózatok megjelenése jelentős előrelépést jelent a távközlési technológiában. Ez az előrelépés forradalmasítani ígéri a digitális világgal való interakcióinkat, és olyan példátlan sebességet és kapcsolódási lehetőségeket kínál, amelyek lehetővé teszik az innováció új hullámát a különböző ágazatokban. Mindezen változások új hullámot jelentenek a digitalizációs folyamatokban is (Varga – Csiszárik-Kocsir, 2023a; 2023b; Csiszárik-Kocsir, 2023; Csiszárik-Kocsir – Varga, 2023). Ezen izgalmas kilátások mellett azonban az 5G technológia bevezetése az informatikai biztonsággal kapcsolatos sürgető aggodalmakat is felvet.

Az Óbudai Egyetem Keleti Károly Gazdasági Karán Viktor Patrik és Fodor Monika által végzett kutatás ezeket az aggodalmakat járja körül, különös tekintettel a különböző generációs kohorszok informatikai biztonsággal és az 5G hálózatok megjelenésével kapcsolatos árnyalt felfogására és hozzáállására.

A tanulmány átfogó kvantitatív kutatási megközelítést alkalmaz, egy szigorúan előre tesztelt, szabványosított kérdőív segítségével gyűjti az adatokat a résztvevők sokszínű csoportjától.

A hólabda mintavételi technikát kihasználva a kutatóknak sikerült 341 kitöltött és értékelhető kérdőívet összegyűjteniük, ami gazdag adathalmazt biztosított az elemzéshez. A mélyreható vizsgálat eredményei azt mutatják, hogy a különböző generációk között jelentős különbségek vannak az informatikai biztonsági fenyegetésekről és az emberi tényezők informatikai biztonságban betöltött szerepéről való tudás szintjében. Továbbá nyilvánvaló, hogy az 5G hálózatok technológiai kifinomultsága ellenére a megkérdezett generációs csoportok körében a bizonytalanság érzése uralkodik e hálózatok biztonsági vonatkozásait illetően.

A hálózatok és a modern társadalom közötti bonyolult kapcsolat képezi azt a hátteret, amely előtt ez a kutatás zajlik. A hálózatok a legtágabb értelemben összekapcsolt világunk gerincét alkotják, megkönnyítve a zökkenőmentes információcserét és számtalan módon összekötve az egyéneket. Ez az összekapcsolhatóság gazdagítja életünket, lehetővé téve számunkra, hogy megosszuk tapasztalatainkat, támogatást keressünk, és eligazodjunk a digitális kor bonyolult viszonyai között. A hálózatoknak a mindennapi életünkbe való mindenre kiterjedő integrációja azonban sebezhetőségeket is rejt magában, így az IT-biztonság témája aktuálisabb, mint valaha.A kiberbiztonság kritikai vizsgálata ebben az összefüggésben rávilágít a terület dinamikus és folyamatosan fejlődő jellegére. Mivel a kiberfenyegetések egyre kifinomultabbá válnak, a kiberbiztonság sokrétű aspektusainak megértése - a hálózatbiztonságtól és az információbiztonságtól kezdve az operatív biztonságon át a végfelhasználók oktatásáig - létfontosságú. Ez az átfogó szemlélet hangsúlyozza a kiberbiztonság többrétegű megközelítésének fontosságát, amely nemcsak a technológiai megoldásokat, hanem az emberi viselkedés és cselekvés jelentőségét is hangsúlyozza a biztonságos digitális környezet fenntartásában.

Viktor és Fodor célja, hogy ezzel a kutatással rávilágítsanak arra a mélyreható hatásra, amelyet a hálózatok, különösen az 5G hálózatok gyakorolnak az életünkre. Feltárják az 5G technológia lehetséges előnyeit és kihívásait, megkérdőjelezve az egyéni magánéletre gyakorolt hatásait, a meglévő internetes szabályozás elégségességét és a kibertámadások megnövekedett kockázatát.A tanulmány megállapításai rámutatnak arra, hogy célzott oktatási kezdeményezésekre és szakpolitika-fejlesztésre van szükség az informatikai biztonságtudatosság és az 5G hálózatokkal kapcsolatos megítélés generációs eltéréseinek kezelése érdekében. Összefoglalva, mivel az 5G széles körű bevezetésének küszöbén állunk, Viktor és Fodor kutatása felbecsülhetetlen értékű

betekintést nyújt a generációs perspektívákba, amelyek az 5G korában az IT-biztonsággal kapcsolatos megértésünket és hozzáállásunkat alakítják. Rávilágít az átfogó kiberbiztonsági stratégiák kritikus szerepére és a technológiai intézkedéseken túlmutató biztonsági kultúra előmozdításának szükségességére, amely az emberközpontú megfontolások integrálásával navigál a digitális összekapcsolhatóság új korszakában jelentkező kihívások és lehetőségek között.

2 Irodalmi áttekintés

A kiberbiztonság jelentőségének mélyebb megértéséhez elengedhetetlen annak felismerése, hogy miért vált a modern társadalom nélkülözhetetlen részévé. (Al-Fuqaha,2015) Az internet és a digitális technológiák fejlődésével a kiberfenyegetések száma és összetettsége megnőtt. (Atzori & Morabito, 2010). A kiberbűnözők folyamatosan finomítják módszereiket, hogy céljaik elérése érdekében kihasználják az informatikai rendszerek sebezhetőségeit. (Bandyopadhyay & Sen,2011) Ebben a bevezetőben a kiberbiztonság alapvető fontosságával, valamint társadalmi és gazdasági hatásaival foglalkozunk. (Chen & Jin,2012). A digitális világ terjeszkedése és az online végzett tevékenységek növekedése jelentős előnyökkel járt a társadalom számára: könnyebb hozzáférést biztosít az információkhoz, javul a kommunikáció, bővülnek az üzleti és oktatási lehetőségek. Nem utolsó sorban javítva a gazdasági szereplők innovációs potenciálját is (Varga, 2023a; Varga 2023b). Ezek az előnyök azonban új kockázatokat is jelentettek. Da & Li,2014). Az adatok és személyes információk online tárolása, valamint az informatikai rendszerektől való növekvő függőség a kiberbűnözők elsődleges célpontjává tette ezeket a rendszereket. (Elkhodr & Cheung,2013) A kiberbiztonság elsődleges célja az információk és az informatikai infrastruktúra elleni jogosulatlan hozzáférés vagy támadások elleni védelem biztosítása. (Gubbi et al,2023) Ez magában foglalja az adatvédelmi intézkedéseket, a hálózati biztonsági protokollokat, a szoftverek és operációs rendszerek rendszeres frissítését, valamint a felhasználók biztonságos online viselkedésre való nevelését. (Hsu & Lin,2016) A kiberbiztonság nem csupán technológiai kérdés; szélesebb körű társadalmi és gazdasági vonatkozásai vannak.(Jing et al.,2014) Az informatikai rendszerek elleni sikeres támadások nemcsak az érintett szervezetekre, hanem ügyfeleikre és a társadalom egészére is negatív hatással lehetnek. (Lin et al.,2017) Fontos megjegyezni, hogy a kiberbiztonság nem csupán a technológia és az infrastruktúra védelméről szól; az emberi tényező is döntő szerepet játszik. (Lu & Cecil,2016) A kiberbiztonsági incidensek jelentős része emberi hiba vagy hanyagság miatt következik be, például gyenge jelszavak használata, gyanús mellékletek megnyitása vagy a szoftverfrissítések elhanyagolása miatt. (Miorandi,2012) Ezért a kiberbiztonsági oktatás és tudatosság minden szinten - az egyénektől a nagyvállalatokig -

létfontosságú a kiberfenyegetések elleni védekezésben. (Perera et al.,2016) A kiberbiztonsági oktatás és tudatosság minden szinten - az egyénektől a nagyvállalatokig - létfontosságú a kiberfenyegetések elleni védekezésben. (Perera et al,2016). A kiberbiztonság azokat a gyakorlatokat, technológiákat és folyamatokat foglalja magában, amelyek célja a számítógépek, hálózatok, programok és adatok védelme a támadásoktól, károktól vagy jogosulatlan hozzáféréstől. Napjaink összekapcsolt világában a kiberbiztonság a nemzetbiztonság, a vállalatirányítás és a magánélet kritikus eleme. (Razzaque et al.,2016) A kiberbiztonság fogalma széleskörű, az érzékeny személyes adatok védelmétől kezdve a kritikus nemzeti infrastruktúra integritásának biztosításáig mindent lefed. Alapvetően a kiberbiztonság az információs technológia (IT) külső és belső fenyegetésekkel szembeni védelméről szól. (Sicari et al., 2015) A technológia gyors fejlődése, valamint a kibertámadók egyre kifinomultabbá válása dinamikus és folyamatosan fejlődő területté teszi a kiberbiztonságot. Ez magában foglalja a fizikai biztonsági intézkedések, a digitális biztosítékok és a jogszabályi megfelelési protokollok kombinációját az információs eszközök védelme érdekében. (Singh & Sharma, 2017)

2.1 A kiberbiztonság kulcsfontosságú területei

A kiberbiztonság több kulcsfontosságú területre bontható, amelyek mindegyike a digitális és fizikai világ különböző aspektusainak védelmére összpontosít:

Hálózati biztonság: Ez a terület az adatátvitel során az adatok integritásának, bizalmas jellegének és rendelkezésre állásának védelmére összpontosít. A hálózati biztonsági intézkedések közé tartoznak a tűzfalak, a titkosítás, a behatolásjelző rendszerek és a biztonságos aljzatréteg (SSL) protokollok. (Stankovic,2014)

Információbiztonság: A kiberbiztonsággal gyakran felcserélhetően használt információbiztonság kifejezetten az adatok integritásának, bizalmas jellegének és rendelkezésre állásának védelmére vonatkozik, függetlenül azok formájától (elektronikus vagy fizikai). Az intézkedések közé tartozik az adattitkosítás, a felhasználói hitelesítés és a hozzáférés-ellenőrző rendszerek.

Alkalmazásbiztonság: Ez magában foglalja a szoftverek és eszközök védelmét a fenyegetésekkel szemben. Az alkalmazásbiztonság magában foglalja az alkalmazások fejlesztési szakaszában hozott intézkedéseket, beleértve a kód felülvizsgálatát, a biztonsági tesztelést és az alkalmazás tűzfalakat.

Operatív biztonság (OpSec): Az OpSec az adatvagyont kezelő és védő műveletekkel és folyamatokkal foglalkozik. Ide tartoznak az adatok kezelésére és tárolására vonatkozó irányelvek, a felhasználói jogosultságok, valamint az adatvesztés vagy -rongálódás esetén alkalmazandó adat-visszaállítási tervek. (sundmaeker et al., 2010)

Végfelhasználói oktatás: Felismerve, hogy az emberi hiba jelentős biztonsági kockázatot jelent, ez a terület a felhasználók oktatására összpontosít a biztonság megsértésének megelőzését szolgáló legjobb gyakorlatokról. A képzés olyan témákat érinthet, mint az adathalászattal kapcsolatos tudatosság, az erős jelszavak fontossága és a biztonságos internetezési szokások.Ahogy a kiberfenyegetések fejlődnek, úgy fejlődnek az ellenük való küzdelem stratégiái és technológiái is. A mesterséges intelligencia (AI) és a gépi tanulás egyre inkább beépül a kiberbiztonsági megoldásokba, hogy hatékonyabban lehessen előrejelezni, azonosítani és reagálni a fenyegetésekre. A blokklánc technológia decentralizált és átlátható jellegével új lehetőségeket kínál a tranzakciók és a kommunikáció biztosítására. (Whitmore & Da,2015) Emellett a tárgyak internete (IoT) lehetőségeket és kihívásokat is jelent a kiberbiztonság számára, mivel a csatlakoztatott eszközök elterjedése növeli a kiberbűnözők támadási felületét. A robusztus kiberbiztonsági stratégia létfontosságú a kiberfenyegetések széles skálája elleni védelemhez, beleértve a rosszindulatú szoftvereket, a zsarolóvírusokat, az adathalász-támadásokat és a fejlett tartós fenyegetéseket (APT-k). Egy ilyen stratégia többrétegű megközelítést igényel, amely nemcsak a technológiára összpontosít, hanem a szervezeti, emberi és szabályozási szempontokkal is foglalkozik. (Xu & Li,2014) Ez magában foglalja a folyamatos nyomon követést, a biztonsági protokollok rendszeres frissítését, az incidensekre való reagálás tervezését, valamint a személyzet és az érdekeltek folyamatos oktatását. Összefoglalva, a kiberbiztonság összetett és alapvető fontosságú terület, amely hatással van az egyénekre, a szervezetekre és a nemzetekre. A technológia fejlődésével és a kiberfenyegetések kifinomultabbá válásával a kiberbiztonság jelentősége tovább nő. A kiberbiztonság alapvető elemeinek és kulcsfontosságú területeinek megértésével az egyének és a szervezetek jobban fel tudnak készülni és meg tudják védeni magukat a kiberfenyegetések folyamatosan változó tájképével szemben. (Zanella et al.,2014)

2.2 Gazdasági és társadalmi hatások

A kiberbiztonsági incidensek gazdasági hatásai több dimenzióban jelentkeznek. A vállalkozások közvetlen pénzügyi veszteségei az adatlopás, a zsarolóprogramok által okozott adatvesztés vagy a működési leállások miatt keletkezhetnek. A kibertámadásokat követően szükséges helyreállítási folyamatok, valamint a biztonsági intézkedések megerősítése jelentős költségekkel járhatnak.(A kiberbiztonsági incidensek hosszú távú gazdasági hatásai is jelentősek lehetnek. A vállalat hírnevének sérülése, az ügyfelek bizalmának elvesztése és a piaci pozíció elvesztése hosszú távon befolyásolhatja a vállalkozások gazdasági teljesítményét. Az ügyfelek adatbiztonságának megsértése jogi következményekhez és bírságokhoz vezethet, ami tovább növeli a vállalatok költségeit. (Zhang et al.,2014)

A kiberbiztonsági incidensek társadalmi hatásai is sokrétűek. Egyéni szinten az adatbiztonsági és adatvédelmi incidensek súlyosan érinthetik a személyes életet, például amikor személyes és pénzügyi információk illetéktelen kezekbe kerülnek. (Csiszárik et al.,2021) Ez az online szolgáltatásokba és a digitális gazdaságba vetett bizalom elvesztéséhez vezethet, ami korlátozza az új technológiák elfogadását és a digitális gazdaság fejlődését. (csiszárik,2022) A társadalmi hatások azonban sokkal messzebbre terjednek. A kritikus infrastruktúrák, például az energiaágazat, a közlekedés és az egészségügyi szolgáltatások elleni kibertámadások közvetlen veszélyt jelenthetnek a közbiztonságra és a közjólétre. (csiszárik,2023) A kiberbiztonsági incidensekből eredő káosz és bizonytalanság társadalmi feszültségeket okozhat, ami hosszú távon alááshatja a társadalmi kohéziót és a kormányzati intézményekbe és a digitális infrastruktúrába vetett bizalmat. A kiberbiztonság gazdasági és társadalmi hatásai rávilágítanak annak fontosságára, hogy a kiberbiztonságot ne csak technológiai kihívásként, hanem összetett társadalmi és gazdasági kérdésként kezeljük.(Csiszárik, 2022) A hatékony kiberbiztonsági stratégiák kidolgozása és a kiberbiztonsági kultúra megerősítése elengedhetetlen a digitális kor kihívásainak kezeléséhez, amelynek célja a gazdasági és társadalmi stabilitás megőrzése a folyamatosan változó digitális környezetben. (Csiszárik,2021)

3 Módszertan

Ez a tanulmány túlmutat a hagyományos másodlagos elemzéseken, elsődleges adatgyűjtési módszerekre támaszkodik, és kvantitatív megközelítést alkalmaz. A hólabda mintavételi módszerekkel végzett online felmérésekből gyűjtött adatok - a hallgatóinkkal mint kezdeti kohorszal kezdve - lehetővé tették, hogy 443 értékelhető kérdőívből gyűjtsünk válaszokat, amelyek kizárólag zárt kérdéseket tartalmaztak nominális és skálamérésekkel. A kérdőív feleletválasztós és skála-alapú kérdéseket tartalmazott, beleértve Likert-skálákat és szemantikus differenciálskálákat.

A szabványosított kérdőív 24 különböző témakört fedett le, az általános IT-biztonsági kérdésektől kezdve az 5G hálózatok IT-biztonsági szempontból történő értékeléséig, valamint az IT-ismeretekre és a szociodemográfiai információkra vonatkozóan. A kvantitatív elemzés leíró statisztikákat, kétváltozós és többváltozós elemzéseket tartalmazott az SPSS 26.1 szoftver segítségével. Az elemzés a mérési szinteken is feltárta a kapcsolatokat a varianciaelemzés, különösen az ANOVA segítségével, amely megkönnyítette az átlagok összehasonlítását több csoporton keresztül. A szignifikanciaszint (sig <= 0,025) vezérelte az összefüggések meghatározását. Az ANOVA-eredményekben talált szignifikáns kapcsolatokból levezetett korrelációs elemzések további betekintést nyújtottak a vizsgált hipotézisekbe. A kvantitatív kutatási szakasz elsődleges

fókusza a következő hipotézisek alapos vizsgálata volt: H1: Az informatikai biztonság megítélése generáció-specifikus elemeket tartalmaz. H1/a) Az informatikai támadások ismerete generáció-specifikus jellemzőket rejt magában. H1/b) Az emberi tényezők IT-biztonságban betöltött szerepének megítélése generáció-specifikus tulajdonságokat testesít meg. H2: Az a meggyőződés, hogy az 5G hálózatok sebezhetőbbek az informatikai támadásokkal szemben, szintén generáció-specifikus jellemzőket tartalmaz. A hipotézisekkel kapcsolatos eredményeket és a szignifikáns kapcsolatokat részletesen tárgyaljuk. Emellett a tanulmány értelmezéseket és további megfigyeléseket kínál, amelyek kibővítik a kutatás tematikus körét. Figyelemre méltó, hogy az X és Z generáció mutatta a legnagyobb érzékenységet az IT-biztonság területén, ezzel bizonyítva az IT-biztonsági elvek és gyakorlatok mélyreható megértését. Az informatikai támadásokkal kapcsolatos ismeretek jelentőségét a különböző generációk között az X generáció 143 fővel, átlagosan 4,42, szórás 0,94; az Y generáció 72 fővel, átlagosan 3,7, szórás 1,12; a Z generáció 237 fővel, átlagosan 4,4, szórás 0,54; és a Baby Boom generáció 50 fővel, átlagosan 4,2, szórás 0,15 bizonyította. Az emberi tényezők szerepének vizsgálata az IT-biztonságban generációs szempontból további jelentős különbségeket tárt fel, megerősítve a H1/b hipotézist.

Az X generáció kiemelkedett az emberi tényezők fontosságának magasra értékelésével az IT-biztonságban. Fokozott tudatosságuk és az emberi viselkedés és cselekedetek biztonságot garantáló kulcsszerepének felismerése alátámasztja e területre vonatkozó egyedi álláspontjukat. Ez a megállapítás kiemeli, hogy az X generáció az emberi tényezőre mint az informatikai biztonsági intézkedések hatékonyságának kritikus meghatározó tényezőjére helyezi a hangsúlyt. Az X generációval kapcsolatos megfigyelések rávilágítanak a pusztán technológiai megközelítéseken túlmutató összetettségre és árnyalatokra, hangsúlyozva az emberi tényezők átfogó megértésének fontosságát a robusztus IT biztonsági stratégiák kidolgozásában. Továbbá ez a felismerés jelentős hatással van az IT-biztonsági oktatási kezdeményezések fejlesztésére és végrehajtására. Felismerve az X generáció fokozott tudatosságát, a szervezetek és oktatási intézmények úgy alakíthatják ki erőfeszítéseiket, hogy foglalkozzanak ezzel a sajátos generációs szemlélettel, és kihasználják azt. Oktatási programok ez a felismerés jelentős hatással van az IT-biztonsági oktatási kezdeményezések fejlesztésére és végrehajtására. Felismerve az X generáció fokozott tudatosságát, a szervezetek és oktatási intézmények úgy alakíthatják ki erőfeszítéseiket, hogy ezt a sajátos generációs perspektívát kezeljék és kihasználják. Oktatási programok Ez a felismerés jelentős hatással van az IT-biztonsági oktatási kezdeményezések fejlesztésére és végrehajtására. Felismerve az X generáció fokozott tudatosságát, a szervezetek és oktatási intézmények úgy alakíthatják ki erőfeszítéseiket, hogy ezt a sajátos generációs perspektívát célozzák meg és használják ki. Oktatási programok Oktatási programok Ez a felismerés jelentős hatással van az IT-biztonsági oktatási kezdeményezések kidolgozására és végrehajtására. Felismerve az X generáció fokozott tudatosságát, a szervezetek és az oktatási intézmények úgy alakíthatják ki erőfeszítéseiket, hogy ezt a sajátos generációs perspektívát

célozzák meg és használják ki. Oktatási programok Oktatási programok Ez a felismerés jelentős hatással van az IT-biztonsági oktatási kezdeményezések fejlesztésére és végrehajtására. Felismerve az X generáció fokozott tudatosságát, a szervezetek és az oktatási intézmények úgy alakíthatják ki erőfeszítéseiket, hogy ezt a sajátos generációs perspektívát célozzák meg és használják ki. Oktatási programok, hogy az X generáció az emberi tényezőre helyezi a hangsúlyt, mint az IT biztonsági intézkedések hatékonyságának kritikus meghatározó tényezőjére. Felismerve az X generáció fokozott tudatosságát, a szervezetek és oktatási intézmények úgy alakíthatják ki erőfeszítéseiket, hogy ezt a sajátos generációs perspektívát célozzák meg és használják ki. Oktatási programok Oktatási programok Ez a felismerés jelentős hatással van az IT-biztonsági oktatási kezdeményezések kidolgozására és végrehajtására. Felismerve az X generáció fokozott tudatosságát, a szervezetek és az oktatási intézmények úgy alakíthatják ki erőfeszítéseiket, hogy ezt a sajátos generációs perspektívát célozzák meg és használják ki. Oktatási programok Oktatási programok Ez a felismerés jelentős hatással van az IT-biztonsági oktatási kezdeményezések fejlesztésére és végrehajtására. Felismerve az X generáció fokozott tudatosságát, a szervezetek és az oktatási intézmények úgy alakíthatják ki erőfeszítéseiket, hogy ezt a sajátos generációs perspektívát célozzák meg és használják ki. Oktatási programok, hogy az X generáció az emberi tényezőre helyezi a hangsúlyt, mint az IT biztonsági intézkedések hatékonyságának kritikus meghatározó tényezőjére. Ez a felismerés továbbá jelentős hatással van az informatikai biztonsági oktatási kezdeményezések kidolgozására és végrehajtására. Felismerve az X generáció fokozott tudatosságát, a szervezetek és oktatási intézmények úgy alakíthatják ki erőfeszítéseiket, hogy ezzel a sajátos generációs szemlélettel foglalkozzanak, és kihasználják azt. Oktatási programok ez a felismerés jelentős hatással van az IT-biztonsági oktatási kezdeményezések fejlesztésére és végrehajtására. Felismerve az X generáció fokozott tudatosságát, a szervezetek és oktatási intézmények úgy alakíthatják ki erőfeszítéseiket, hogy ezt a sajátos generációs perspektívát kezeljék és kihasználják.

	N	Mean*	Std. Deviation	significance
Generation X	143	3,33	1,04	0,1
Generation Y	72	3,322	9,17	
Generation Z	237	3,64	0,92	
Baby boom generation	50	3,56	1,08	
Total	443			
1= strongly disagree, 5= strongly agree; analysis of variance; One Way Anova, Post Hoc Test				

1. táblázat

Elemzésünket folytatva mélyebb vizsgálatot végeztünk annak megállapítására, hogy a különböző generációk rendelkeznek-e egyedi nézőpontokkal az emberi tényezők IT-biztonságra gyakorolt hatásáról. E kiegészítő elemzés eredményei meggyőző bizonyítékot szolgáltatnak a különböző generációk közötti jelentős különbségekre, így alátámasztva a H1/ b hipotézist.

Jelentős, hogy az X generáció az a csoport, amely a legnagyobb jelentőséget tulajdonítja az emberi tényezőknek az IT-biztonságon belül.

	N	Mean*	Std. Deviation	significance
Generation X	143	3,33	1,04	0,1
Generation Y	72	3,322	9,17	
Generation Z	237	3,64	0,92	
Baby boom generation	50	3,56	1,08	
Total	443			
1= strongly disagree, 5= strongly agree; analysis of variance; One Way Anova, Post Hoc Test				

2. táblázat

Az emberi viselkedés és cselekedetek biztonság fenntartásában játszott döntő szerepének fokozott tudatossága és elismerése kiemeli az IT-menedzsment e

létfontosságú aspektusával kapcsolatos sajátos nézőpontjukat. Ez az eredmény azt sugallja, hogy az X generáció egyértelműen hangsúlyozza az emberi tényezőt, mint az IT biztonsági stratégiák hatékonyságának kulcsfontosságú tényezőjét.

Folytatva a vizsgálatot, mélyebbre merültünk a vizsgálatban, hogy megállapítsuk, vajon a különböző generációs kohorszok rendelkeznek-e egyedi nézőpontokkal az emberi tényezők IT-biztonságra gyakorolt hatásáról. Ez a további elemzés meggyőző bizonyítékokat hozott, amelyek rávilágítottak a generációk közötti jelentős különbségekre, és így alátámasztották a H1/b hipotézist. Különösen az X generáció volt az a csoport, amely a legnagyobb jelentőséget tulajdonítja az emberi tényezőknek az informatikai biztonság területén. Az emberi viselkedésnek és cselekvéseknek a digitális környezetek védelmében játszott döntő szerepének fokozott tudatossága és elismerése kiemeli az IT-irányítás e lényeges aspektusához való sajátos hozzáállásukat. Ez a megfigyelés arra utal, hogy az X generáció az emberi tényezőt az informatikai biztonsági intézkedések hatékonyságának fokozásában alapvető kulcsként hangsúlyozza. Ezt kibővítve minden egyes generáció egyedülálló módon járul hozzá az IT-biztonságról folytatott szélesebb körű párbeszédhez, túllépve a technológiai tényezők egyszerű felismerésén, és kiemelve annak szükségességét, hogy a szilárd IT-biztonsági stratégiák kialakításába integrálni kell az emberi elemek átfogó megértését. Ez a felismerés mélyreható következményekkel jár az IT-biztonsági oktatási kezdeményezések megfogalmazására és végrehajtására. Az X generáció IT-biztonsággal kapcsolatos fokozott tudatosságának felismerésével a szervezetek és az oktatási intézmények olyan helyzetbe kerülnek, hogy stratégiáikat úgy alakíthatják ki, hogy bevonják és kihasználják ezt a sajátos generációs nézőpontot.

Az oktatási programok ezután az informatikai biztonságban játszó emberi dinamika mélyebb megértésére összpontosíthatnak, hangsúlyozva a felhasználói viselkedést, a döntéshozatali folyamatokat és a szervezeteken belüli erős biztonsági kultúra kialakítását.Az informatikai biztonság emberi tényezőinek megítélését befolyásoló generációs különbségek pontosabb megértése elmélyíti az informatikai biztonsági kihívások és megoldások széles skálájának megértését. Rávilágít arra, hogy nemcsak a technológiai védekezés fejlesztése, hanem egy olyan átfogó megközelítés előmozdítása is kritikus fontosságú, amely az emberi szempontokat zökkenőmentesen beépíti az IT-biztonsági stratégiák szövetébe. Az egyre összetettebb és összekapcsolt digitális világban tett utazásunk során e generációs felismerések elismerése és hasznosítása kulcsfontosságú a hatékony és rugalmas IT-biztonsági keretrendszerek létrehozásához, amelyek képesek alkalmazkodni a digitális korszak változó fenyegetéseihez és lehetőségeihez.

3.1 A generáció-specifikus kiber biztonság

Külön vizsgálatunkban arra összpontosítottunk, hogy megértsük, hogyan vélekednek az 5G hálózatokról informatikai biztonsági szempontból, miközben

azt is vizsgáltuk, hogy a különböző korcsoportok között lehetnek-e különbségek a véleményekben. Eredményeink azt mutatták, hogy az 5G hálózatok megítélése nem különbözik jelentősen az egyes generációk között, ami arra a következtetésre vezetett, hogy a H2 hipotézis (szignifikancia >= 0,05) nem igazolódott. Ennek ellenére az átlagos válaszok elemzése érdekes mintázatot mutatott: az Y generációs csoport mutatta a legnagyobb szkepticizmust az 5G technológia bevezetésével szemben. Ez az óvatos hozzáállás valószínűleg számos kérdésből fakad, például a magánélet és az adatvédelemmel kapcsolatos aggodalmakból, vagy a technológia fejlődési sebességével kapcsolatos nyugtalanságból.

	N	Mean*	Std. Deviation	significance
Generation X	143	2,81	0,97	0,05
Generation Y	72	2,72	0,76	
Generation Z	237	2,21	1,11	
Baby boom generation	50	2,32	1,03	
Total	443	2,41	1,06	
1= strongly disagree, 5= strongly agree; analysis of variance; One Way Anova, Post Hoc Test				

3. táblázat

Ha mélyebben megvizsgáljuk, hogy az Y generáció miért lehet különösen óvatos az 5G-vel kapcsolatban, akkor konkrét félelmeket és aggodalmakat fedezhetünk fel az új technológiával kapcsolatban. Ezek a meglátások aztán felhasználhatók az e demográfiai csoport félelmeinek mérséklésére irányuló, személyre szabott oktatási erőfeszítésekhez vagy célzott kommunikációs stratégiákhoz. Továbbá az Y generáció szkepticizmusának felismerése rávilágít arra, hogy az új technológiák bevezetésekor egyértelmű kommunikációra és erős kockázatkezelési stratégiákra van szükség. Az aggodalmak proaktív kezelése, valamint a bizalom és a nyitottság légkörének ápolása megkönnyítheti az átmenetet, és segíthet az olyan innovációk szélesebb körű elfogadásában, mint az 5G, minden korcsoportban. Bár az 5G hálózatok általános értékelésében nem találtak jelentős generációs különbségeket, az Y generáció érezhető szkepticizmusa lehetőséget kínál az alaposabb vizsgálatra és a célzott fellépésre az 5G technológia iránti bizalom és elfogadás fokozása érdekében a különböző lakossági szegmensekben. A tanulmányban az 5G IT-biztonságra gyakorolt hatásának vizsgálata a bizonytalanság uralkodó érzését tárta fel, ami a kohorszok között osztott érzést tükrözi. Ez az ambivalencia rámutat azokra az összetett és többrétegű kihívásokra, amelyeket az 5G technológia

integrálása a meglévő informatikai keretrendszerek számára jelent. Ez a kutatás kritikus kérdéseket vet fel a további vizsgálathoz. Például az egyes generációknak az 5G biztonsági következményeivel kapcsolatos konkrét aggodalmainak és aggályainak pontosabb megértése segíthet a célzott kockázatcsökkentési stratégiák kialakításában. Emellett a különböző korcsoportok kockázatérzékelésének és elfogadásának eltéréseinek feltárása betekintést nyújthat a biztonsági aggályok kommunikációjának és megoldásának leghatékonyabb módjaiba, ahogy az 5G egyre szélesebb körben elterjed. Továbbá annak vizsgálata, hogy az oktatási és tudatosságnövelési erőfeszítések hogyan alakíthatják az 5G biztonságával kapcsolatos attitűdöket, az egyes korcsoportokra szabott, hatásosabb kiberbiztonsági képzési programok kidolgozásához vezethet. A technológiai ismeretek és az 5G biztonságával kapcsolatos nézetek közötti kapcsolat feltárása rávilágíthat a digitális írástudás javításának és a biztonságos technológiahasználat generációkon átívelő ösztönzésének módjaira is.

4 Eredmények

A dokumentumban az 5G hálózat kialakulásáról és annak az informatikai biztonságra gyakorolt várható hatásáról szóló átfogó elemzés alapján több ajánlás is megfogalmazható. Ezek az ajánlások az IT-biztonsági tudatosság generáció-specifikus árnyalataival, az 5G hálózatok megítélésével, valamint ezen eredményeknek a szakpolitikára, az oktatásra és a szervezeti stratégiákra gyakorolt tágabb következményeivel foglalkoznak. Az oktatás hozzáigazítása a generációs igényekhez: Olyan IT-biztonsági oktatási programok kidolgozása és végrehajtása, amelyek a különböző generációk egyedi igényeihez és tudásszintjéhez igazodnak. Mivel az X és Z generáció magasabb szintű tudatosságot mutat az IT-biztonsági kérdésekkel kapcsolatban, az oktatási kezdeményezések ennek a tudásnak az elmélyítésére és kiterjesztésére összpontosíthatnának, hogy lefedjék az újonnan megjelenő fenyegetéseket, beleértve az 5G hálózatokkal kapcsolatosakat is. Az emberi tényezők jobb megértése: Mivel az X generáció jelentős jelentőséget tulajdonít az emberi tényezőknek az IT-biztonságban, lehetőség nyílik olyan oktatási és képzési programok kialakítására, amelyek hangsúlyozzák az emberi viselkedés szerepét, a döntéshozatali folyamatokat és a szervezeteken belüli erős biztonsági kultúra kialakítását. Az 5G biztonsági bizonytalanságok kezelése: Mivel az 5G hálózatokkal kapcsolatban minden generációban bizonytalanság uralkodik, az oktatási erőfeszítéseknek az 5G technológia demisztifikálására is törekedniük kell. Ezek közé kell tartoznia az 5G biztonsági jellemzőiről, a lehetséges kockázatokról, valamint arról, hogy az egyének és a szervezetek hogyan csökkenthetik ezeket a kockázatokat. Nemzedékeket figyelembe vevő politikák kidolgozása: A politikai döntéshozóknak a szabályozás kialakításakor figyelembe kell venniük az informatikai biztonságtudatosság és az 5G hálózatokkal kapcsolatos felfogás generációs különbségeit. Az átláthatóságot

ösztönző, a magánéletet védő és az 5G-hálózatok biztonságát garantáló politikák kulcsfontosságúak lesznek az összes generációs kohorsz aggodalmainak kezelésében. Az 5G biztonsági szabványok megerősítése: Tekintettel az 5G technológiában rejlő átalakító potenciálra, a szabályozó testületeknek szorosan együtt kell működniük az iparági érdekeltekkel annak érdekében, hogy szilárd biztonsági szabványokat és gyakorlatokat dolgozzanak ki az 5G telepítésére és használatára vonatkozóan. Ezeknek a szabványoknak foglalkozniuk kell az 5G által támasztott egyedi biztonsági kihívásokkal, beleértve a kiterjedt összekapcsolhatóságot és az általa kezelt hatalmas adatmennyiséget. A biztonság kultúrájának támogatása: A szervezeteknek olyan kultúrát kell kialakítaniuk, amely az IT-biztonságot kollektív felelősségként értékeli. Ez magában foglalja a rendszeres képzést, a tudatosságnövelő kampányokat és a biztonságos viselkedés fontosságának egyértelmű hangsúlyozását a szervezet minden szintjén. A generációs szempontok beépítése az IT-biztonsági stratégiákba: A munkaerőn belül a generációs dinamika megértésével a szervezetek jobban hozzáigazíthatják IT-biztonsági stratégiáikat. Ez magában foglalhatja olyan kommunikációs és képzési megközelítések elfogadását, amelyek a különböző korcsoportok számára rezonálnak, vagy az egyes generációk egyedi perspektíváinak kihasználását az általános biztonsági helyzet megerősítése érdekében.Felkészülés az 5G integrációra: Ahogy a szervezetek az 5G technológia bevezetésére készülnek, fel kell készülniük a jelenlegi IT-biztonsági kereteik felmérésével és a lehetséges hiányosságok azonosításával. Ez magában foglalja az IoT-eszközök biztonságának értékelését, az érzékeny adatok titkosításának biztosítását, valamint a személyzet képzését az 5G technológiával kapcsolatos kockázatokról és legjobb gyakorlatokról. Vizsgálja meg a mögöttes aggodalmakat és attitűdöket: További kvalitatív kutatások, például fókuszcsoportok vagy interjúk mélyebb betekintést nyújthatnak a különböző generációk 5G technológiával kapcsolatos konkrét aggodalmaiba és attitűdjeibe. Ez alapján célzottabb beavatkozásokra lehet támaszkodni.Az oktatás szerepének feltárása a felfogás alakításában: A jövőbeni tanulmányoknak meg kell vizsgálniuk, hogy az oktatási és tudatosságnövelő erőfeszítések hogyan befolyásolhatják az 5G biztonságával kapcsolatos generációs attitűdöket, ami a különböző korcsoportokra szabott, hatékonyabb kiberbiztonsági oktatási programok kidolgozásához vezethet. Összefoglalva, az informatikai biztonsággal és az 5G hálózatokkal kapcsolatos felfogások és ismeretek generációs árnyaltságának kezelése többoldalú megközelítést igényel, amely magában foglalja a személyre szabott oktatási kezdeményezéseket, az inkluzív szakpolitika-fejlesztést és a stratégiai szervezeti erőfeszítéseket. E generációs különbségek felismerésével és kihasználásával az érdekelt felek biztonságosabb és tájékozottabb digitális környezetet teremthetnek az 5G technológia elfogadásának további terjedésével párhuzamosan.

Összefoglalás

A budapesti Óbudai Egyetem kutatói az 5G hálózatok megjelenésének és az informatikai biztonságra gyakorolt hatásának átfogó vizsgálata során az informatikai biztonsággal és az 5G technológia megjelenésével kapcsolatos generációs felfogást és ismereteket vizsgálták. A vizsgálat, amelyet az a hipotézis vezérelt, hogy a generációs árnyalatok jelentősen befolyásolják az informatikai biztonsággal kapcsolatos észleléseket és az 5G hálózatokkal kapcsolatos attitűdöket, kvantitatív kutatási módszertant használt, és egy szabványosított kérdőív segítségével 443 résztvevő adatait gyűjtötte össze. Ez a folyamat az informatikai biztonsági fenyegetések és az emberi tényezők informatikai biztonságban betöltött szerepének megértése terén a különböző generációk között éleslátó eltéréseket tárt fel, miközben az 5G hálózatokkal kapcsolatos bizonytalanság érzése is egységes volt az összes megkérdezett csoportban. A tanulmány megállapította, hogy az informatikai biztonsági fenyegetésekkel kapcsolatos ismeretek és az emberi tényezők fontossága az informatikai biztonság biztosításában jelentősen eltér a különböző generációk között, az X és Z generációk pedig fokozott tudatosságot mutatnak az informatikai biztonsági kérdésekkel kapcsolatban. Ez a megállapítás hangsúlyozza annak szükségességét, hogy az IT-biztonsági oktatási programokat úgy kell testre szabni, hogy azok hatékonyan foglalkozzanak a generációk eltérő megértési szintjeivel, biztosítva az ismeretek és a kockázatcsökkentési stratégiák széles körű és hatékony terjesztését. A kutatás kiemelte továbbá, hogy az X generáció különös hangsúlyt fektet az emberi tényezők jelentőségére az IT-biztonság területén. Ennek a generációnak a fokozott tudatossága és annak elismerése, hogy az emberi viselkedés és cselekedetek kulcsfontosságú szerepet játszanak a biztonság fenntartásában, aláhúzza annak szükségességét, hogy az emberközpontú megfontolásokat integráló, szilárd IT-biztonsági kultúra kialakítására irányuló erőfeszítéseket prioritásként kezeljük.

A kutatók várakozásaival ellentétben az 5G hálózatok vizsgálata informatikai biztonsági szempontból nem tárt fel jelentős generációs eltéréseket az értékelésekben. Ehelyett a bizonytalanság uralkodó érzése volt nyilvánvaló a résztvevők körében, ami arra utal, hogy fokozott kommunikációs és oktatási erőfeszítésekre van szükség az 5G technológiával kapcsolatos tisztázásra és tájékoztatásra, mivel annak elfogadása tovább növekszik. A tanulmánynak az informatikai biztonsággal és az 5G hálózatokkal kapcsolatos generációs attitűdökkel kapcsolatos megállapításai jelentős következményekkel járnak a célzott oktatási kezdeményezések, a szakpolitika-alkotás és a szervezeti stratégiák kidolgozására. A különböző generációk eltérő nézőpontjainak és tudásszintjeinek felismerésével és kihasználásával az érdekeltek elősegíthetik egy biztonságosabb és tájékozottabb digitális környezet kialakítását, amely elősegíti az 5G technológia sikeres integrációját. Az elemzésből levezetett ajánlások a különböző generációk sajátos igényeihez és tudásszintjéhez igazított informatikai biztonsági oktatási programok kidolgozását szorgalmazzák. Mivel az X- és Z-generáció tagjai jobban

tisztában vannak az informatikai biztonsági kérdésekkel, az oktatási kezdeményezések elmélyíthetik ezt a megértést, és kiterjeszthetik azt az újonnan megjelenő fenyegetésekre, beleértve az 5G hálózatokhoz kapcsolódó fenyegetéseket is. A tanulmány olyan oktatási és képzési programokat is szorgalmaz, amelyek hangsúlyozzák az emberi viselkedés, a döntéshozatali folyamatok fontosságát és a szervezeteken belüli erős biztonsági kultúra ápolását. Az 5G technológiát övező bizonytalanságokkal foglalkozva a kutatás egyértelmű kommunikációt javasol az 5G biztonsági jellemzőiről, a potenciális kockázatokról és a mérséklési stratégiákról, hogy minden generációs kohorszban enyhítsék az aggodalmakat. Összefoglalva, a kutatás kiemeli annak fontosságát, hogy sokoldalú megközelítést alkalmazzunk az informatikai biztonsággal és az 5G hálózatokkal kapcsolatos felfogások és ismeretek generációs árnyalatait illetően. A személyre szabott oktatási kezdeményezések, az inkluzív szakpolitika-fejlesztés és a stratégiai szervezeti erőfeszítések révén az érdekeltek eligazodhatnak az 5G technológia bevezetése által jelentett kihívások és lehetőségek között, biztosítva a biztonságos és tájékozott átmenetet a digitális összekapcsolhatóság következő korszakába.

Hivatkozások

[1] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials, 17(4), pp. 2347-2376. https://doi.org/10.1109/COMST.2015.2444095

[2] Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A Survey. Computer Networks, 54(15), pp. 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

[3] Bandyopadhyay, D., & Sen, J. (2011). Internet of Things: Applications and Challenges in Technology and Standardization. Wireless Personal Communications, 58(1), 49-69. https://doi.org/10.1007/s11277-011-0288-5

[4] Chen, J., & Jin, X. (2012). Research on Key Technology and Applications for Internet of Things. Physics Procedia, 33, pp. 561-566. https://doi.org/10.1016/j.phpro.2012.05.108

[5] Csiszárik-Kocsir, Á. (2021). Customer Preferences in Bank Selection before and after the Pandemic in the Light of Financial Culture and Awareness. Acta Polytechnica Hungarica 18(11) pp. 151-169.

[6] Csiszárik-Kocsir, Á. (2022). The Present and Future of Banking and New Financial Players in the Digital Space of the 21st Century. Acta Polytechnica Hungarica 19(8) pp. 143-160.

[7] Csiszárik-Kocsir, Á. (2023). The Purposes and Motivations of Savings Accumulation based on Generational Affiliation, Financial Education and Financial Literacy. Acta Polytechnica Hungarica, 20(3).

[8] Csiszárik-Kocsir, Á. (2023). Digital presence and awareness through the content consumption habits of different generations. In: Szakál, Anikó (szerk.) SISY 2023 IEEE 21st International Symposium on Intelligent Systems and Informatics, Budapest, Magyarország : IEEE Hungary Section, pp. 191-195.

[9] Csiszárik-Kocsir, Á., Varga, J. 2023. The advancing role of digitalisation through the example of the Perlmutter project from the user side. In: Szakál, Anikó (szerk.) IEEE 17th International Symposium on Applied Computational Intelligence and Informatics SACI 2023 : Proceedings Budapest, Magyarország : Óbudai Egyetem, IEEE Hungary Section, pp. 327-332.

[10] Csiszárik-Kocsir, Á., Garai-Fodor, M., & Varga, J. (2021). What has Become Important during the Pandemic?–Reassessing Preferences and Purchasing Habits as an Aftermath of the Coronavirus Epidemic through the Eyes of Different Generations. Acta Polytechnica Hungarica, 18(11), 49-74..

[11] Csiszárik-Kocsir, Á., Garai-Fodor, M., & Varga, J. (2022). Generation-specific analysis of the pandemic's impact on financial culture. In: IEEE (ed.) IEEE 20th Jubilee World Symposium on Applied Machine Intelligence and Informatics SAMI (2022) : Proceedings, IEEE, pp. 201-205.

[12] Csiszárik-Kocsir, Á., Garai-Fodor, M., & Varga, J. (2022). Preference system for the choice of savings in a generation-specific approach of the financial culture before and after the coronavirus pandemic. In: Szakál, Anikó (ed.) IEEE 10th Jubilee International Conference on Computational Cybernetics and Cyber-Medical Systems ICCC 2022, pp. 287-291.

[13] Da Xu, L., He, W., & Li, S. (2014). Internet of Things in Industries: A Survey. IEEE Transactions on Industrial Informatics, 10(4), pp. 2233-2243. https://doi.org/10.1109/TII.2014.2300753

[14] Elkhodr, M., Shahrestani, S., & Cheung, H. (2013). The Internet of Things: New Interoperability, Management and Security Challenges. arXiv preprint arXiv:1307.2340.

[15] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. Future Generation Computer Systems, 29(7), pp. 1645-1660. https://doi.org/10.1016/j.future.2013.01.010

[16] Hsu, C. W., & Lin, Y. H. (2016). An Empirical Examination of Consumer Adoption of Internet of Things Services: Network Externalities and Concern for Information Privacy Perspectives. Computers in Human Behavior, 62, pp. 516-527. https://doi.org/10.1016/j.chb.2016.04.023

[17] Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: Perspectives and Challenges. Wireless Networks, 20(8), pp. 2481-2501. https://doi.org/10.1007/s11276-014-0761-7

[18] Ju, J., Kim, M. S., & Ahn, J. H. (2016). Prototyping Business Models for IoT Service. Procedia Computer Science, 91, pp. 882-890. https://doi.org/10.1016/j.procs.2016.07.088

[19] Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. In 2012 10th International Conference on Frontiers of Information Technology (pp. 257-260). IEEE. https://doi.org/10.1109/FIT.2012.53

[20] Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, Investments, and Challenges for Enterprises. Business Horizons, 58(4), pp. 431-440. https://doi.org/10.1016/j.bushor.2015.03.008

[21] Li, S., Xu, L. D., & Zhao, S. (2015). The Internet of Things: A Survey. Information Systems Frontiers, 17(2), pp. 243-259. https://doi.org/10.1007/s10796-014-9492-7

[22] Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. IEEE Internet of Things Journal, 4(5), pp. 1125-1142. https://doi.org/10.1109/JIOT.2017.2683200

[23] Lu, Y., & Cecil, J. (2016). An Internet of Things (IoT)-based Collaborative Framework for Advanced Manufacturing. The International Journal of Advanced Manufacturing Technology, 84(1-4), pp. 1141-1152. https://doi.org/10.1007/s00170-015-7772-0

[24] Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of Things: Vision, Applications and Research Challenges. Ad Hoc Networks, 10(7), 1497-1516. https://doi.org/10.1016/j.adhoc.2012.02.016

[25] Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Context Aware Computing for The Internet of Things: A Survey. IEEE Communications Surveys & Tutorials, 16(1), pp. 414-454. https://doi.org/10.1109/SURV.2013.042313.00197

[26] Razzaque, M. A., Milojevic-Jevric, M., Palade, A., & Clarke, S. (2016). Middleware for Internet of Things: A Survey. IEEE Internet of Things Journal, 3(1), pp. 70-95. https://doi.org/10.1109/JIOT.2015.2498900

[27] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, Privacy and Trust in Internet of Things: The Road Ahead. Computer Networks, 76, pp. 146-164. https://doi.org/10.1016/j.comnet.2014.11.008

[28] Singh, S., Rajan, R., & Sharma, P. K. (2017). Security for Wireless Sensor Network-Based Smart Home. International Journal of Advanced Research

in Computer Science, 8(9), pp. 398-402. https://doi.org/10.26483/ijarcs.v8i9.4964

[29] Stankovic, J. A. (2014). Research Directions for the Internet of Things. IEEE Internet of Things Journal, 1(1), pp. 3-9. https://doi.org/10.1109/JIOT.2014.2312291

[30] Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S. (2010). Vision and Challenges for Realising the Internet of Things. Cluster of European Research Projects on the Internet of Things, European Commission. https://doi.org/10.2759/26127

[31] Varga, J. (2023a): 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.

[32] Varga, J. (2023b): The potential benefits of innovation as seen by some domestic businesses. In: Szakál, Anikó (szerk.) SISY 2023 IEEE 21st International Symposium on Intelligent Systems and Informatics. Budapest, Magyarország: IEEE Hungary Section (2023). 663 p. pp. 223-228.

[33] Varga, J., Csiszárik-Kocsir, Á. (2023a). Exploring the use of digital tools in a technology and change-driven world in Hungary and Poland in the light of the pandemic. In: Szakál, Anikó (szerk.) SISY 2023 IEEE 21st International Symposium on Intelligent Systems and Informatics, Budapest, Magyarország : IEEE Hungary Section, pp. 243-247.

[34] Varga, J., Csiszárik-Kocsir, Á. 2023b. Perception of innovation and innovative projects at user level through the example of the Atala Prism project. In: Szakál, Anikó (szerk.) IEEE 17th International Symposium on Applied Computational Intelligence and Informatics SACI 2023 : Proceedings Budapest, Magyarország : Óbudai Egyetem, IEEE Hungary Section pp. 321-326.

[35] Vermesan, O., & Friess, P. (Eds.). (2014). Internet of Things - From Research and Innovation to Market Deployment. River Publishers.

[36] Wang, S., Wan, J., Zhang, D., Li, D., & Zhang, C. (2016). Towards Smart Factory for Industry 4.0: A Self-Organized Multi-Agent System with Big Data Based Feedback and Coordination. Computer Networks, 101, pp. 158-168. https://doi.org/10.1016/j.comnet.2015.12.017

[37] Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The Internet of Things—A Survey of Topics and Trends. Information Systems Frontiers, 17(2), pp. 261-274. https://doi.org/10.1007/s10796-014-9489-2

[38] Xu, L. D., He, W., & Li, S. (2014). Internet of Things in Industries: A Survey. IEEE Transactions on Industrial Informatics, 10(4), pp. 2233-2243. https://doi.org/10.1109/TII.2014.2300753

[39] Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of Things for Smart Cities. IEEE Internet of Things Journal, 1(1), pp. 22-32. https://doi.org/10.1109/JIOT.2014.2306328

[40] Zhang, Y., Xiao, Y., Ma, X., Vasilakos, A. V., Yang, H., & Liu, C. (2014). A Survey of Security and Privacy Issues in Cloud Computing. IEEE Communications Surveys & Tutorials, 15(2), pp. 843-859. https://doi.org/10.1109/SURV.2013.082713.00285