ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS

FEHÉR-POLGÁR PÁL

Biztonsági stratégia kialakításának lehetőségei saját tulajdonú mobileszközök munkacélú használatára

Témavezető: Prof. Dr. Michelberger Pál

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2026. március 19.

Nyilvános védés teljes bizottsága:

Elnök:

Prof. Dr. Pokorádi László

Titkár:

Dr. Szilágyi Győző

Tagok:

Dr. habil. Tóth András

Dr. Varga Péter János

Dr. habil. Farkas Tibor

Bírálók:

Prof. Dr. habil. Kiss Gábor

Dr. Jobbágy Szabolcs

Nyilvános védés időpontja:

2026.

D12) Nyilatkozat a munka önállóságáról, irodalmi források megfelelő módon történt idézéséről

NYILATKOZAT

A MUNKA ÖNÁLLÓSÁGÁRÓL, IRODALMI FORRÁSOK MEGFELELŐ MÓDON TÖRTÉNT IDÉZÉSÉRŐL

Alulírott Fehér-Polgár Pál kijelentem, hogy a Biztonsági stratégia kialakításának lehetőségei saját tulajdonú mobileszközök munkacélú használatára című benyújtott doktori értekezést magam készítettem, és abban csak az irodalmi hivatkozások listáján megadott forrásokat használtam fel. Minden olyan részt, amelyet szó szerint, vagy azonos tartalomban, de átfogalmazva más forrásból átvettem, a forrás megadásával egyértelműen megjelöltem.

Budapest, 2026. március 19.

Fehér-Polgár P.

aláírás

Tartalomjegyzék

BEVEZETÉS

Az elmúlt két évtized digitális technológiai fejlődése alapvetően átalakította a munkavégzés, a kommunikáció és az információkezelés kereteit. A mobileszközök – különösen az okostelefonok és táblagépek – mára nem csupán kiegészítő eszközei, hanem meghatározó infrastruktúrái a mindennapi életnek, a civil szervezeti működésnek és egyre inkább a katonai, honvédelmi és kritikus infrastruktúrákat működtető rendszerek információs architektúrájának is. Az információkhoz való folyamatos hozzáférés, az állandó online jelenlét és a helyfüggetlen munkavégzés lehetősége olyan új működési modellt eredményezett, amelyben a munka és a magánélet határai egyre inkább elmosódnak. Ezzel párhuzamosan a szervezetek – ideértve a magas biztonsági követelményű intézményeket is – egyre inkább digitális, hálózatközpontú működési struktúrákra támaszkodnak.

A kétezres évek elején megjelenő okostelefonok nemcsak az internet szinte bárhonnan történő elérését tették lehetővé, hanem a „bárhonnan”, „bármikor” történő munkavégzést is. A mobileszközök teljesítménye, kapacitása és funkcionalitása folyamatosan növekedett, miközben méretük és relatív költségük csökkent. A mobil távközlési hálózatok sávszélessége és lefedettsége ugyancsak jelentős fejlődésen ment keresztül, ami a szervezeti rendszerek távoli elérését technikailag rutinszerűvé tette. A vállalati működés szempontjából a mobileszközök alkalmazása mára megkerülhetetlenné vált [1] [2].

Ugyanez a tendencia figyelhető meg a védelmi és honvédelmi szektorban is, ahol a hálózatközpontú hadviselési és irányítási modellek az információ gyors, decentralizált és mobil hozzáférésére épülnek. A digitális eszközök integrációja a katonai kommunikációs rendszerekbe, logisztikai folyamatokba és vezetésirányítási struktúrákba olyan új működési logikát eredményez, amelyben a mobil hozzáférés nem csupán kényelmi, hanem operatív jelentőségű tényezővé válik.

A technológiai fejlődéssel párhuzamosan azonban új típusú információbiztonsági kihívások is megjelentek. Bár az erős titkosítási és hitelesítési megoldások elterjedtek, ezek önmagukban nem garantálnak teljes körű védelmet. A mobileszközök kommunikációja során számos metaadat kerül továbbításra – például földrajzi koordináták, hálózati kapcsolatok, mozgásra vonatkozó adatok –, amelyek érzékeny információkat hordozhatnak. A rádióalapú kommunikáció (például Bluetooth) lehallgatása, illetve a mobil adatforgalom monitorozása sok esetben nehezen kontrollálható [3] [4] [5].

Katonai és nemzetbiztonsági kontextusban a metaadatok különösen kritikus jelentőséggel bírnak. Egy látszólag ártalmatlan helyinformáció, hálózati mintázat vagy kommunikációs időzítés operatív következtetések levonását teheti lehetővé. A mobileszközökből származó adatok aggregálása akár személyi állomány mozgására, infrastruktúra elhelyezkedésére vagy műveleti aktivitásra vonatkozó mintázatokat is kirajzolhat. Ennek következtében a mobileszközök használata nem pusztán informatikai kérdés, hanem stratégiai kockázati tényező is lehet.

E folyamat egyik meghatározó jelensége a BYOD (Bring Your Own Device), amely a saját tulajdonú mobileszközök munkacélú használatát jelenti. A BYOD keretében a munkavállalók nem vállalati tulajdonú eszközeiken keresztül férnek hozzá vállalati erőforrásokhoz – például adatbázisokhoz, irányítási rendszerekhez vagy felhőszolgáltatásokhoz. Ez a gyakorlat jelentős rugalmasságot és hatékonyságnövekedést eredményezhet, ugyanakkor új típusú kockázati struktúrát is létrehoz.

Bár a BYOD elsősorban vállalati kontextusban terjedt el, a civil–katonai technológiai konvergencia következtében a saját tulajdonú vagy részben kontrollált eszközök használata a védelmi szektor számára is releváns kérdéssé vált. A digitális ökoszisztéma egységesülése, a felhőszolgáltatások és mobil alkalmazások elterjedése olyan technológiai környezetet teremtett, amelyben a szervezeti és magáneszközök közötti határvonal elmosódik. Ez a jelenség különösen érzékeny a magas biztonsági követelményű rendszerekben.

A BYOD egyik sajátossága, hogy a vállalati és magánhasználat egyazon eszközön, egyazon technológiai környezetben valósul meg. A munkavállaló ugyanarról az eszközről fér hozzá közösségi alkalmazásokhoz, személyes adatokhoz és vállalati rendszerekhez. Ez a kevert használati modell az információbiztonsági kontroll szempontjából különösen érzékeny helyzetet teremt. A vállalati adatokhoz való hozzáférés szabályozása és felügyelete így nem csupán technológiai kérdés, hanem szervezeti és humán tényezőkkel is összefügg.

A biztonsági szakirodalomban gyakran idézett megállapítás szerint „a leggyengébb láncszem az ember” [6] [7] [8] [9]. A technológiai védelem hatékonysága jelentős mértékben függ a felhasználók döntéseitől, tudatosságától és kockázatvállalási attitűdjétől. Ez a megállapítás különösen érvényes olyan rendszerekben, ahol a biztonsági sérülékenység stratégiai vagy akár nemzetbiztonsági következményekkel járhat. Katonai és kritikus infrastruktúrák esetében az egyéni döntések rendszerszintű hatással bírhatnak, így a humán tényező nem pusztán kiegészítő elem, hanem a biztonsági architektúra strukturális komponense [10].

A BYOD tehát olyan szervezeti – és bizonyos kontextusokban stratégiai jelentőségű – döntési dilemma, amelyben a technológiai infrastruktúra, a szabályozási környezet és az egyéni döntéshozatali mechanizmusok egyaránt szerepet játszanak. A vállalatok jelentős része ugyan alkalmazza a BYOD megoldásokat, ám gyakran hiányzik a tudatos, stratégiai szintű döntés és a strukturált kockázatkezelési megközelítés. A kockázatok azonosítása, rendszerezése és kezelése sok esetben ad hoc módon történik.

KUTATÁSI KÉRDÉSEK ÉS HIPOTÉZISEK

A disszertáció kiindulópontja az a feltételezés, hogy a BYOD nem kizárólag informatikai vagy technológiai kérdés, hanem döntéselméleti, viselkedéstudományi és rendszerelméleti szempontból is vizsgálandó jelenség. A vállalati és – tágabb értelemben – szervezeti kockázatok jelentős része nem pusztán a technikai sebezhetőségből, hanem a felhasználói döntésekből ered. A technológiai és humán dimenzió kölcsönhatásának megértése ezért kulcsfontosságú a biztonsági rendszerek tervezésében.

A BYOD jelenség információbiztonsági vizsgálata a szakirodalomban elsősorban technológiai és szabályozási perspektívából jelenik meg. A kutatások jelentős része a mobileszközök sérülékenységeire, a hálózati fenyegetésekre, valamint a szervezeti kontrollmechanizmusokra fókuszál. Ugyanakkor lényegesen kevesebb figyelem irányul arra, hogy a felhasználói döntések, a kockázatészlelés és az egyéni kockázatvállalási attitűdök miként befolyásolják a BYOD-környezetben megjelenő biztonsági kockázatokat. Különösen hiányzik annak empirikus vizsgálata, hogy az IT-biztonsági döntések milyen viszonyban állnak az általános, doménspecifikus kockázatvállalási mintázatokkal.

A jelen disszertáció e kutatási résre reagálva a BYOD jelenséget a technológiai, szervezeti és humán tényezők integrált vizsgálatán keresztül elemzi, különös tekintettel az IT-biztonsági kockázatvállalási hajlandóság mérhetőségére és szerkezeti sajátosságaira.

A kockázat fogalmának alkalmazása során a dolgozat Renn [11], [12] kockázatklasszifikációs megközelítésére támaszkodik, amely lehetővé teszi a különböző kockázati dimenziók rendszerezett kezelését. A BYOD esetében a kockázatok több szinten jelennek meg: technikai, adatvédelmi, szervezeti és humán tényezők dimenzióiban. E dimenziók integrált kezelése különösen fontos olyan rendszerekben, ahol a működési folyamatosság és az információbiztonság stratégiai jelentőségű.

A humán tényező vizsgálatához a disszertáció a Weber, Blais és Betz által kidolgozott Domain-Specific Risk-Attitude Scale (DOSPERT), illetve annak továbbfejlesztett változata [13] által kínált keretre támaszkodik. A DOSPERT megközelítés lehetővé teszi a kockázatvállalási hajlandóság doménspecifikus mérését, elkülönítve az észlelt haszon, az észlelt kockázat és a cselekvési valószínűség dimenzióit. A BYOD és az IT-biztonsági kontextus esetében különösen releváns annak vizsgálata, hogy a felhasználói döntések milyen súlyozási struktúra mentén alakulnak ki: a kockázatészlelés vagy az észlelt előnyök dominálják-e a döntési folyamatot.

A kutatás célkitűzései

A jelen doktori kutatás átfogó célja a saját tulajdonú mobileszközök munkacélú használatából (BYOD) fakadó információbiztonsági kihívások újszerű, szocio-technikai megközelítésű vizsgálata. Bár a technológiai védelmi vonalak elengedhetetlenek, a rendszer legkritikusabb pontja maga a felhasználó és az ő döntési mechanizmusa. Ennek megértése és a vállalati stratégiába történő integrálása érdekében az alábbi öt, egymásra épülő kutatási célt fogalmaztam meg:

- **C1: Az IT-biztonsági kockázatvállalás mint önálló, doménspecifikus konstrukció azonosítása és mérési kereteinek validálása**

  Az általános kockázatvállalási hajlandóságot vizsgáló modellek (mint például a DOS-PERT) hagyományosan pénzügyi, egészségügyi, etikai, szociális és rekreációs doméneket különítenek el. Kutatásom elsődleges célja annak tudományos igazolása, hogy az infokommunikációs technológiák térnyerésével az IT-biztonsági kockázatvállalás egy ezektől jól elkülöníthető, önálló doménként jelenik meg az egyének kognitív térképén. Célom továbbá feltárni, hogy ez a specifikus IT-kockázatvállalási hajlandóság milyen mértékben magyarázható olyan alapvető demográfiai és egyéni változókkal, mint az életkor vagy a nem, ezáltal megteremtve a felhasználói viselkedés mérésének és előrejelzésének alapjait.

- **C2: Az IT-biztonsági kockázatok percepciós helyzetének meghatározása és rendszerezése a BYOD-környezetben**

  Nem elegendő pusztán azonosítani az IT-biztonságot, mint önálló területet; vizsgálni kell annak szubjektív súlyát is a felhasználók értékrendjében. Második célkitűzésem a BYOD modell alkalmazása során felmerülő specifikus kockázatok (adatvesztés, jogosulatlan hozzáférés, eszközök kompromittálódása stb.) strukturált rendszerezése, valamint annak feltárása, hogy a felhasználók a mindennapi életük során megélt egyéb (pl. pénzügyi vagy egészségügyi) fenyegetettségekhez képest hová pozicionálják a kibertérből érkező veszélyeket. Ennek megértése elengedhetetlen a megfelelő fókuszú vállalati figyelemfelhívó és oktatási programok, biztonságtudatosság kialakításához.

- **C3: A szubjektív kockázatpercepció és a biztonságtudatos felhasználói viselkedés közötti összefüggések feltárása**

  A szakirodalom gyakran feltételezi, hogy a magasabb fenyegetettség-érzet automatikusan óvatosabb magatartást eredményez. Harmadik kutatási célom ennek az összefüggésnek az empirikus vizsgálata a mobil okoseszközök vállalati környezetben történő használata során. Meg vizsgálom, hogy a felismert és észlelt kockázatok (szubjektív percepció) milyen irányban és mértékben alakíthatóak tényleges, mérhető biztonságtudatos viselkedéssé (például képernyőzár használata, nyilvános hálózatok kerülése). Célom azonosítani azokat a tényezőket, amelyek erősítik, vagy éppen gátolják ezt az átmenetet.

- **C4: A technikai biztonságtudatosság és a szervezeti kockázatvállalás ellentmondásainak (biztonságtudatossági paradoxon) elemzése**

  A szervezeti IT-biztonsági incidensek jelentős része nem az ismeretek hiányából, hanem a túlzott magabiztosságból fakad. Negyedik célom a „biztonságtudatossági paradoxon" jelenségének mélyreható elemzése a BYOD kontextusában. Ennek során azt vizsgálom, hogy a magasabb szintű technikai kompetenciák és a fejlett biztonsági ismeretek hogyan és miért vezethetnek – a kontroll illúzióján keresztül – magasabb szervezeti kockázatvállaláshoz. E jelenség feltárása rávilágít arra, hogy a puszta technikai oktatás önmagában miért nem elégséges a biztonsági incidensek elkerüléséhez.

- **C5: A haszon-domináns döntési mechanizmusok feltárása és a BYOD döntéstámogató stratégiai alapjainak kidolgozása**

  A BYOD modell terjedésének alapvető motorja a felhasználói és szervezeti előnyök maximalizálása. Ötödik célkitűzésem annak bizonyítása, hogy az IT-biztonsági és eszközhasználati döntések során a felhasználók kognitív mérlegelésében súlyos aszimmetria figyelhető meg: az észlelt haszon (pl. kényelem, rugalmasság, produktivitás) sokkal erősebben dominálja a viselkedést, mint az észlelt kockázat. Eredményeimre támaszkodva egy olyan döntéstámogató és stratégiai keretrendszer alapjainak kidolgozását tűztem ki célul, amely a tiltáson alapuló, tisztán technológiai (hard) megközelítés helyett a viselkedésalapú, a haszon-kockázat aszimmetriát menedzselni képes (soft) elemeket is integrálja a vállalati biztonsági szabályozásba.

E kutatási kérdések alapján a következő hipotéziseket fogalmazom meg:

- H1: A DOSPERT eredeti doménjei nem képesek szignifikáns mértékben előre jelezni az IT-biztonsági kockázati kérdésekre adott válaszokat.
- H2: Az IT-biztonsági domén észlelt kockázati szintje nem a legmagasabb a vizsgált kockázati domének között.
- H3: A különböző szakok hallgatói között szignifikáns különbség mutatható ki az IT-biztonsági kockázatok észlelésében.
- H4: Az IT-biztonsági kockázatok magasabb észlelése pozitív kapcsolatban áll a biztonságtudatos viselkedési gyakorlatok alkalmazásával.
- H5: A technikai biztonságtudatosság egyes formái együtt járhatnak BYOD-kontextusban magasabb szervezeti kockázatvállalási hajlandósággal.
- H6: Az IT-biztonsági döntésekben az észlelt haszon standardizált regressziós súlya szignifikánsan meghaladja az észlelt kockázat abszolút értékű regressziós súlyát.
- H7: Az észlelt haszon–kockázat súlyozási aszimmetriája nem kizárólag IT-biztonsági sajátosság, más doménekben is kimutatható.
- H8: Az életkor az általános kockázatvállalási dimenziók kontrollálása mellett szignifikáns magyarázóerővel bír az IT-biztonsági kockázatvállalás tekintetében.
- H9: A nem az általános kockázatvállalási dimenziók kontrollálása mellett is szignifikáns kapcsolatban áll az IT-biztonsági kockázatvállalással.

A DOKTORI ÉRTEKEZÉSBEN HASZNÁLT LEGFONTOSABB FOGALMAK ÉS KIFEJEZÉSEK ÉRTELMEZÉSE

Disszertációmban a saját tulajdonú mobileszközök munkacélú használatának információbiztonságát elemzem és fogalmazok meg eredményeket és javaslatokat. E témában használt legfontosabb fogalmakat ebben az alfejezetben definiálom röviden, később a dolgozat érdemi pontjaiban részletesebben is bemutatom ezeket.

Alapfogalmak és technológiai környezet

BYOD, BYOD eszközök (Bring Your Own Device, eszközök): A disszertációban a BYOD eszközök alatt olyan, a munkavállalók saját tulajdonában álló, mobileszközöket értek, melyek bár teljes értékű számítógépes képességekkel bírnak, a mindennapokban mégsem úgy tekintenek rájuk. Olyan hordozható eszközök, mint táblagépek, tabletek, okostelefonok, PDA-k stb., de a laptopokat, ultrahordozható laptopokat, számítógépeket nem sorolom ide. Ezen eszközök kényelmes, folyamatos használatból fakadó óvatlanság és az eszközök valós tudása közötti ellentmondás az, ami kiemelt biztonsági kockázatot jelent a vállalatok számára [14] [15] [16].

BYOD kockázat: A BYOD kockázat azt a komplex biztonsági fenyegetést jelenti, amely abból fakad, hogy a munkavállalók a saját tulajdonú mobileszközeiket (például okostelefonokat, tableteket) használják vállalati feladatok elvégzésére. Ebből adódóan az üzleti adatok és a vállalati folyamatok a magánhasználat szférájával ugyanazon az eszközön, azonos felhasználói rutinok mentén keverednek, így a szervezet elveszíti a közvetlen ellenőrzést az információs környezete felett. A veszélyt tovább súlyosbítja az a felhasználói óvatlanság is, amely a megszokott és kényelmes használatból ered: az emberek hajlamosak elfelejteni, hogy ezek a készülékek valójában mekkora számítástechnikai tudással rendelkeznek. A BYOD kockázat tehát nem csupán egy technikai vagy informatikai sebezhetőség, hanem a technológiai, a szervezeti kontrollhoz kötődő és a humán tényezők (felhasználói viselkedés) közös kölcsönhatásából kialakuló veszélyforrás [12] [17].

Kockázatelemzés BYOD környezetben: A kockázatelemzés az a folyamat, amikor a vállalat feltérképezi a saját okoseszközök munkacélú használatából (BYOD) eredő veszélyeket, felismerve, hogy a technikai sebezhetőségek mellett legalább ekkora problémát jelent a dolgozók kényelemszeretete és óvatlansága [17] [12] [18].

Kockázatértékelés BYOD környezetben: A kockázatértékelés során azt mérik fel, hogy ezek a veszélyek mekkora valós fenyegetést jelentenek a cég számára, itt azonban komoly kihívást

jelent, hogy a felhasználók a hamis biztonságérzetük miatt („velem úgysem történik meg”) jellemzően nagyon alulbecsülik a digitális veszélyeket [19] [20].

Kockázatkezelés: az a stratégiai válaszlépés, amellyel a szervezet megpróbálja kivédeni ezeket a fenyegetéseket: technológiai védelemmel (például az eszközök távoli felügyeletével), szigorúbb szabályozásokkal és – ami a legfontosabb – a munkavállalók biztonságtudatosságának célzott fejlesztésével [21] [22].

MDM (Mobile Device Management): Mobileszköz-menedzsment; olyan szoftveres megoldás, amely lehetővé teszi a szervezetek számára a mobileszközök távoli felügyeletét, konfigurálását és biztonsági szabályozását [23].

Shadow IT (Árnyékinformatika): A szervezet által nem jóváhagyott vagy nem kontrollált informatikai eszközök, szoftverek és szolgáltatások használata a munkavállalók részéről [24] [25].

Kockázat- és döntéselméleti fogalmak

Észlelt és valós kockázat (Perceived and objective risk): A szubjektív (egyéni tapasztalatokon, félelmeken alapuló) és az objektív (statisztikailag mérhető, technikai) kockázati szint közötti különbség [26].

DOSPERT-skála (Domain-Specific Risk-Attitude Scale): A kockázatvállalási hajlandóság mérésére szolgáló módszertan, amely különböző életterületeken (doméneken), úgy mint; pénzügyi, egészségi, szabadidős, etikai és társas helyzetek, méri a kockázatvállalási hajlandóság attitűdjeit [13] [27].

Humán és társadalmi dimenziók

Biztonságtudatosság (Safety Consciousness): Az egyén ismereteinek és hozzáállásának összessége, amely meghatározza, mennyire ismeri fel és kezeli a biztonsági fenyegetéseket [28] [29] [30].

Biztonsági kultúra (Security culture): A szervezet tagjai által vallott értékek, normák és hiedelmek, amelyek befolyásolják az információbiztonsággal kapcsolatos viselkedést [31] [32].

Biztonsági attitűd (Security attitude)**:** A biztonsági attitűd az egyén ismereteinek, tapasztalatainak és személyes beállítottságának az összessége, amely meghatározza, hogy a mindennapi eszközhasználat során mennyire ismeri fel és hogyan kezeli a digitális fenyegetéseket. Ennek egyik legfontosabb jellemzője, hogy nem pusztán a szakmai tudáson múlik: a kutatás rámutat,

hogy önmagában a magas informatikai képzettség sem garantálja feltétlenül az óvatos viselkedést. A mindennapi döntéseket ugyanis sok esetben a kényelem, az azonnali megoldásokra való törekvés és a megszokott rutinok erősebben befolyásolják, mint a racionálisan felmérhető technikai kockázatok. A biztonsági attitűd tehát egy egyedi, helyzetfüggő emberi gondolkodásmód, amelyben az értékrend és az egyéni felelősségérzet dönti el, hogy a felhasználó pajzsként védi a rendszert, vagy éppen ő maga válik a leggyengébb láncszemmé [8] [7] [10].

Specifikus biztonsági kockázatok a BYOD-ban

Metaadat-kitettség (Metadata leakage, Metadata disclosure): A kommunikáció során keletkező kiegészítő adatok (helyszín, időpont, hálózati adatok), amelyek aggregálva érzékeny információkat árulhatnak el [33] [34].

Adatszivárgás (Data Leakage): Vállalati adatok nem szándékos vagy jogosulatlan kikerülése a magánszférába vagy külső felekhez (pl. felhő-szinkronizáció vagy másolás révén) [34].

Rendszerfeltörés (Rootolás / Jailbreak): Az operációs rendszer gyártói korlátozásainak eltávolítása, ami növeli a funkcionalitást, de súlyosan veszélyezteti az eszköz biztonsági integritását.

1 A BYOD HUMÁN ÉS DÖNTÉSELMÉLETI DIMENZIÓJA

1.1 Az új generáció

A disszertáció empirikus vizsgálata egyetemi hallgatók körében valósult meg, mivel ők a jelen és a közeljövő munkavállalói. Digitális eszközhasználati rutinjaik, információtechnológiai attitűdjeik és információbiztonsághoz való viszonyuk már a jelenben is, a jövőben pedig még inkább meghatározó tényezői lehetnek a szervezetek információbiztonsági gyakorlatának. A BYOD jelenség megértése és a kapcsolódó kockázatok kezelése ezért nem választható el attól a társadalmi és technológiai környezettől, amelyben az Y és Z generáció – gyakran „digitális bennszülött" generációként – szocializálódott.

A millenniumiak, „ezredfordulósok", illetve a digitális bennszülöttek megnevezés alatt általában az Y és Z generációt értjük, amelynek tagjai a technológiai fejlődést nem külső, később elsajátított eszközként, hanem természetes, mindennapi környezetként tapasztalták meg. E generációk technikai és csoportmunka-képességei, gyors alkalmazkodása és nyitottsága új igényeket fogalmazott meg az oktatásban és a munka világában is. A BYOD és a hozzá kapcsolódó információbiztonsági kérdések szempontjából mindez azért releváns, mert a technológiai természetesség egyfelől támogatja a gyors adaptációt és a produktivitást, másfelől azonban a kockázatok észlelésének és tudatos kezelésének csökkenéséhez is vezethet. Amennyiben a szervezeti információbiztonságot humán tényezőként is vizsgáljuk, indokolt áttekinteni azokat a generációs sajátosságokat, amelyek a digitális eszközhasználat, a döntési rutinok és a biztonságtudatosság szempontjából kiemelten fontosak.

1.1.1 Az új generáció általános jellemzői

Az új generációk értékrendjét és jellegzetességeit több kutatás is vizsgálta, célként tűzve ki a domináns tulajdonságok és viselkedési mintázatok azonosítását [35]. A szakirodalom a generációs különbségek mellett több olyan pszichológiai és társadalmi jelenséget is azonosít, amely a digitális technológiákkal kapcsolatos döntésekben – így az információbiztonsági döntésekben is – releváns lehet.

Sebesség és azonnaliság.

Az Y és Z generáció tagjait gyakran nevezik digitális bennszülötteknek, mivel belenőttek a technológiai környezetbe és könnyedén használják az információtechnológia vívmányait [36] [37]. Információigény esetén a hagyományos források helyett jellemzően online keresést alkalmaznak, és gyors, azonnal rendelkezésre álló válaszokat várnak. A közösségi médiaplatformok

valós idejű működése megerősíti az azonnali reakció, az időnyomás és a folyamatos információáramlás élményét. E jellegzetesség információbiztonsági szempontból azért lényeges, mert az azonnali haszon (kényelem, gyors hozzáférés) könnyen domináns motivációvá válhat olyan döntési helyzetekben, ahol a kockázatok késleltetetten vagy absztrakt módon jelennek meg.

A személyes kapcsolatok átalakulása és a folyamatos online jelenlét

Az online közösségek a kapcsolattartás mintázatait is átalakították. A folyamatos online jelenlét elvárássá válhat, a közösségi felületeken való megjelenés pedig a társas beágyazottság egyik indikátora lehet. Ennek következményeként az offline állapot akár hiányérzetet vagy társas kizártság-élményt is kiválthat. A jelenség a digitális környezetben megvalósuló döntésekre is hatással van: a gyors kommunikáció és az állandó elérhetőség a BYOD környezetben is könnyen kialakíthatja azt a normát, hogy a munkavállaló mindig elérhető, és a munkavégzés technikailag (és sokszor kulturálisan) „mindig lehetséges”.

Szabadság, mobilitás, digitális nomád jelleg

Az Y és Z generációra jellemző lehet a mobilitás iránti igény és az a törekvés, hogy a munkavégzés időben és térben kevésbé kötött legyen. A fejlett technológiának és az elterjedt internetkapcsolatnak köszönhetően a munkavégzés sok esetben akár utazás közben, külső helyszíneken, vagy nem hagyományos munkakörnyezetben is megvalósítható [38]. E jelenség közvetlenül kapcsolódik a BYOD-hoz, mivel a saját eszközök munkacélú használata tipikusan azt az igényt elégíti ki, hogy a szervezeti erőforrások hozzáférhetők legyenek a klasszikus szervezeti infrastruktúrán kívül is. A mobilitás ugyanakkor információbiztonsági kockázati tényező is lehet, mivel változatos hálózati környezetek, heterogén alkalmazások és a kontrollálhatóság csökkenése társulhat hozzá.

Egyediség és individualizmus

A digitális térben az identitásképzés és az önmegjelenítés tudatos, sok esetben teljesítmény- és elismerés-orientált formában jelenhet meg [39]. A közösségi médiában mért visszajelzések („like”, elérés, követők) a társas összehasonlítás új terepét teremthetik meg. A jelenség közvetlen információbiztonsági kapcsolata abban ragadható meg, hogy a digitális eszközök és alkalmazások intenzív használata növeli a felhasználói rutinok stabilitását, és a kényelmi szempontok könnyen háttérbe szoríthatják a biztonságtudatos viselkedést.

Egyszerűség és egyszerűsítés

A kép- és rövidvideómegosztó platformok elterjedése a digitális kommunikációt rövidebb, gyorsabban fogyasztható tartalmak irányába tolhatja. Ezzel párhuzamosan a hosszabb, komplex információk feldolgozása és az elmélyült figyelem gyakorlata csökkenhet. Biztonsági kontextusban mindez azért releváns, mert a szervezeti szabályzatok, információbiztonsági előírások és kockázatkommunikáció gyakran hosszabb, összetett szövegeken keresztül történik. Ha a felhasználók preferenciái az egyszerű, gyorsan értelmezhető üzenetek felé tolódnak, akkor a biztonsági oktatás és kockázatkommunikáció hatékonyságát is ehhez kell igazítani.

Biztonság és a csoporthoz tartozás igénye

A biztonság igénye ebben a generációs kontextusban nem feltétlenül a kockázat elkerülésével azonos, hanem sokszor a megbízható közösségekhez és márkákhoz való kötődés formájában jelenhet meg. A társas támogatás és a megerősítés igénye – különösen a kortárscsoport felől – hangsúlyos lehet [40]. Ennek információbiztonsági implikációja, hogy a normakövetés és a biztonsági viselkedés gyakran társas mintázatokhoz kötődik: a felhasználó nemcsak egyéni racionalitás alapján dönt, hanem a közösségi normákhoz való illeszkedés mentén is.

Divat, trendkövetés

A gyors információáramlás miatt a trendek és új technológiák átvétele felgyorsulhat; a csoportokon belüli „újítók” (influencerek) szerepe hangsúlyos lehet [35] [41]. A szervezeti IT-környezetben ez azt eredményezheti, hogy a felhasználók a szervezet által támogatott megoldások mellett alternatív alkalmazásokat és csatornákat keresnek, ha azok „korszerűbbnek” vagy kényelmesebbnek tűnnek.

FoMo (fear of missing out) – a valamiből való kimaradástól való félelem

Az Y és Z generáció számára sajátos jelenség lehet a FoMo, azaz attól való szorongás, hogy mások valamilyen élményben vagy közösségi eseményben vesznek részt, miközben az érintett abból kimarad [42]. A FoMo a közösségi médián keresztül állandósuló összehasonlítás és jelenlétkényszer miatt hosszabb távon is befolyásolhatja a digitális eszközhasználati mintázatokat. Biztonsági szempontból a FoMo közvetetten növelheti a folyamatos csatlakozás, gyors reagálás és az azonnali hozzáférés iránti igényt – ez pedig olyan döntési környezetet hozhat létre, ahol az észlelt haszon (elérhetőség, kényelem) felülírja a kockázatészlelésből fakadó óvatosságot.

A szakirodalom az Y generációs hallgatók oktatási preferenciáit is vizsgálta: gyakran előnyben részesítik a gyakorlatias tanulást, a csoportmunkát és a technológia használatát [43] [44]. Vizuális tanulóknak is nevezik őket, akik gyors és könnyen elérhető megoldásokat várnak [45]. Információszerzésben jellemzően online platformokra támaszkodnak, és sok esetben jelentős bizalmat helyeznek online társaikra [46]. Ezt erősítheti, hogy számukra a technológia használata „könnyed" és „természetes" [37]. A technológia természetessége azonban – információbiztonsági nézőpontból – kettős: a magas használati kompetencia nem azonos a magas biztonságtudatossággal, és a rutinszerű, gyors döntések növelhetik a kockázatokkal járó cselekvések valószínűségét.

Az Y generációs egyetemi hallgatókat gyakran úgy nevezett technológiai „multitasker"-ekként jellemzik, akik több eszközt és alkalmazást használnak párhuzamosan [36] [37]. A folyamatos online jelenlét a nemzetközi összehasonlításokban is megjelenik: a 18–29 éves korosztályban több országban legalább a fiatalok fele állítja, hogy folyamatosan online van, és a napi internethasználat aránya általában magas [47]. A multitasking és a folyamatos csatlakozás a szervezeti IT-biztonság szempontjából azért fontos, mert a felhasználók egyidejűleg több szerepben (magán és munka) mozognak, több digitális csatornát használnak, és döntéseik gyakran rutinszerűvé válnak. A rutinhelyzetekben a kockázatok észlelése csökkenhet, miközben az azonnali előnyök – gyors hozzáférés, kényelem, produktivitás – erős motivációs tényezőként jelennek meg.

1.1.2 BYOD és az oktatási környezet, mint előkép

Nem meglepő, hogy az egyetemi hallgatók körében is népszerű a „hozd a saját eszközöd" BYOD gondolata. A hallgatók a saját eszközeiket használják, amelyeket jól ismernek, és amelyek az általuk preferált alkalmazásokkal, felhasználói beállításokkal állnak rendelkezésre. Egy felmérés alapján már 2014-ben az egyetemi hallgatók többsége (86%) rendelkezett okostelefonnal vagy táblagéppel az Egyesült Államokban [48], és erre válaszul a felsőoktatási intézmények meghatározó hányada BYOD-stratégiát indított. A trend azonban akkor is terjedhet, ha nincs hivatalos vagy támogatott stratégia: a felhasználók saját igényeik mentén alakítják ki a gyakorlatot [49] [50]. A hallgatók a modern és hatékony IKT-rendszerekkel való munkához hozzászoknak, és tapasztalataik befolyásolhatják általános elégedettségüket az intézménnyel kapcsolatban is [51].

A felsőoktatási környezetben megfigyelhető BYOD-jellegű gyakorlat a munka világában a saját eszközök munkacélú használatának előképe lehet. A hallgatók a digitális környezetben „globális világpolgárként" is gondolhatnak magukra, több kulturális hatás és nemzetközi média

befolyása mellett [52]. Ez a nyitott, digitálisan integrált működésmód a munkahelyen a mobil munkavégzés, a távoli hozzáférés és a rugalmas eszközhasználat iránti igényként jelentkezhet.

A gyors és azonnali megoldások iránti igény ugyanakkor a szervezeti környezetben könnyen ütközhet a szabályozott, kontrollált infrastruktúra korlátaival. Bár az IKT eszközök és rendszerek bizonyos tekintetben univerzálisak, a fogadó szervezet környezetében a felhasználók szembesülhetnek a hozzáférések korlátozottságával, a platformok eltérő elérhetőségével, különböző szoftverekkel, jelszavakkal és szabályokkal [51] [53]. A felhasználói élmény és a szervezeti kontroll közötti feszültség negatív tapasztalatokat generálhat, és elősegítheti alternatív, nem szabályozott megoldások keresését.

E problémák egyik következménye lehet a ShadowIT (árnyék informatikai rendszer) kialakulása. A ShadowIT a szervezet által kialakított, szabályozott és üzemeltetett informatikai rendszer(ek) mellett és/vagy helyett a munkavállalók által kialakított informatikai megoldásokat jelenti, amelyek többek között biztonsági kockázatokat rejthetnek, ugyanakkor bizonyos esetekben a folyamatoptimalizáció forrásai is lehetnek [24] [25]. A BYOD és a ShadowIT jelenségek közös jellemzője, hogy mindkettő a felhasználói igények és a szervezeti keretek közötti résben jelenik meg: a felhasználó a saját eszközeihez és preferált alkalmazásaihoz nyúl, ha a szervezeti környezetet túl lassúnak, túl korlátozónak vagy nem megfelelőnek érzékeli.

1.1.3 Digitális bennszülöttek és a BYOD

Az Y és Z generáció digitális környezetben kialakult sajátosságai – az azonnaliság, a folyamatos online jelenlét, a multitasking, a mobilitás iránti igény, a társas normák és a trendkövetés – olyan döntési közeget teremtenek, amelyben a digitális eszközök használata rutinszerűvé válik, és a kockázatok sok esetben kevésbé tudatosan jelennek meg. E jelenségek a BYOD szervezeti alkalmazásában is relevánsak, mivel a saját tulajdonú eszközök munkahelyi használata tipikusan a gyorsaság, kényelem és elérhetőség előnyeit kínálja, miközben a kockázatok kontrollja részben a felhasználói döntések szintjére tolódik.

A fejezetben áttekintett elméleti szempontok megalapozzák a disszertáció további részeit két irányban. Egyrészt indokolják, hogy a BYOD kockázatkezelése során a humán tényezőt a technológiai és szervezeti tényezőkkel egyenrangúan szükséges kezelni, összhangban azzal a megközelítéssel, amely szerint az ember a biztonsági rendszer meghatározó eleme [6] [7] [8] [9]. Másrészt rávilágítanak arra, hogy a BYOD környezetben a felhasználói döntések motivációs és észlelési mechanizmusai – például az azonnali előnyök preferálása, a rutin-cselekvések dominanciája és a társas normák – kulcsszerepet játszhatnak a kockázati viselkedés kialakulásában.

A következő fejezetek ennek megfelelően a BYOD jelenség fogalmi és szervezeti kereteinek pontosítására, a kapcsolódó információbiztonsági kockázatok strukturált rendszerezésére, valamint az emberi tényező – különösen az IT-biztonsággal összefüggő kockázatvállalási hajlandóság – mérhetőségének vizsgálatára fókuszálnak.

1.2 Kockázatvállalás

A BYOD-jelenség értelmezéséhez nem elegendő a technológiai sérülékenységek feltárása; szükséges annak megértése is, hogy az egyének miként viszonyulnak a bizonytalansághoz és a potenciális veszteségekhez. A BYOD környezetben a kockázatvállalás nem absztrakt gazdasági fogalom, hanem mindennapi döntések sorozatában jelenik meg: telepítünk-e egy alkalmazást, frissítjük-e az operációs rendszert, használunk-e nyilvános WiFi-hálózatot, továbbítunk-e céges dokumentumot saját postafiókba.

1.2.1 Döntés bizonytalanságban

A valós élethelyzetekben ritkán áll rendelkezésünkre teljes információ. A döntéshozó – legyen az magánszemély vagy szervezeti szereplő – a rendelkezésére álló információk, tapasztalatok és mentális modellek alapján cselekszik. A döntési helyzetet gyakran időnyomás, információhiány és a következmények bizonytalansága jellemzi.

Még abban az esetben is, ha elméletileg képesek lennénk összegyűjteni minden releváns információt, az emberi kognitív kapacitás korlátozott: egyszerre csak véges számú tényezőt tudunk mérlegelni, összehasonlítani és rendszerezni. A döntés ezért nem tökéletes optimalizálás, hanem gyakran kielégítő (satisficing) választás a bizonytalanság keretei között.

BYOD esetében ez a helyzet különösen jellemző. A felhasználó nem rendelkezik teljes körű információval:

- nem tudja pontosan, hogy egy alkalmazás milyen adatokat gyűjt és hogyan használja fel,
- nem tudja, hogy egy adott WiFi-hálózat mennyire biztonságos,
- nem tudja felmérni, hogy egy szoftverfrissítés elmulasztása milyen konkrét következményekkel járhat,
- stb.

Ennek ellenére döntést kell hoznia. A döntés pedig mindig együtt jár a kockázat vállalásával.

1.2.2 A kockázatvállalás, mint személyiségjellemző

A kockázatvállalás mértéke személyenként jelentősen eltér. Vannak, akik inkább kockázatkerülők, mások hajlamosabbak nagyobb bizonytalanság mellett is cselekedni. Számos tanulmány vizsgálta a kockázatvállalás és a kulturális háttér összefüggéseit [54] [55].

Hofstede kulturális dimenziói között kiemelt szerepet kap a bizonytalanságkerülés (uncertainty avoidance), amely azt fejezi ki, hogy egy társadalom tagjai mennyire tolerálják a bizonytalanságot és a kétértelműséget [56] [31] [32]. A Hofstede Insights adatai alapján a magyar társadalom viszonylag magas bizonytalanságkerülési indexszel jellemezhető, ami elvileg kockázatkerülőbb attitűdöt feltételez.

Ez a kulturális sajátosság azonban nem jelenti automatikusan azt, hogy az egyének információbiztonsági döntéseikben is következetesen kockázatkerülők lennének. A technológiai környezetben gyakran megfigyelhető egyfajta „észlelt alacsony kockázat” jelenség: a felhasználó nem érzékeli közvetlennek vagy valószínűnek a fenyegetést, ezért hajlamos nagyobb kockázatot vállalni.

BYOD-környezetben tehát a kockázatvállalás nemcsak kulturális, hanem kontextusfüggő jelenség is. A munkavállaló másként mérlegelhet, ha:

- a döntés kényelmet vagy időmegtakarítást eredményez,
- a negatív következmény nem azonnali és nem látható,
- a felelősség megoszlik a szervezet és az egyén között.

1.2.3 Észlelt és valós kockázat közötti eltérés

A kockázatvállalás megértéséhez fontos különbséget tenni a **valós (objektív)** és az **észlelt (szubjektív)** kockázat között. Az információbiztonság területén ez az eltérés gyakran jelentős.

A valós kockázatot meghatározza:

- a sérülékenységek száma és súlya,
- a fenyegetések jelenléte,
- a potenciális kár nagysága.

Az észlelt kockázat viszont függ:

- a felhasználó technológiai tudásától,
- korábbi tapasztalataitól,
- a média által közvetített narratíváktól,
- a közvetlen környezet visszajelzéseitől.

BYOD esetében tipikus jelenség, hogy a felhasználó alulbecsli a kockázatot („velem úgysem történik meg”), különösen akkor, ha korábban nem tapasztalt közvetlen negatív következményt. A döntések így gyakran nem a valós kockázati szinthez, hanem a szubjektív kockázatészleléshez igazodnak.

Ez a jelenség közvetlen kapcsolatban áll a dolgozat empirikus részével: amennyiben a hallgatók – mint jövőbeli munkavállalók – alacsony kockázatészleléssel rendelkeznek mobilbiztonsági kérdésekben, úgy a BYOD-környezetben is nagyobb valószínűséggel hoznak kockázatos döntéseket.

1.2.4 Kockázatvállalás és felelősségmegosztás BYOD-környezetben

A BYOD sajátossága, hogy a felelősség nem egyértelműen lokalizálható. A munkavállaló saját tulajdonú eszközt használ, de azon vállalati adatokat kezel. A kérdés ezért az, hogy ki viseli a döntés következményeit.

Amennyiben:

- a felhasználó telepít egy kockázatos alkalmazást,
- nem frissíti az operációs rendszert,
- nyilvános hálózaton keresztül kezeli a vállalati levelezést,

akkor a döntés egyéni, de a következmény szervezeti is lehet. A kockázatvállalás tehát kollektív hatású egyéni döntések sorozataként jelenik meg.

Ez különösen fontossá teszi a kockázatvállalás és a biztonságtudatosság kapcsolatának vizsgálatát. Ha a szervezet kizárólag technológiai kontrollokban gondolkodik, de nem foglalkozik az egyéni attitűdökkel, akkor a maradékkockázat magas maradhat.

1.2.5 Kapcsolódás a kutatáshoz

A jelen dolgozat empirikus része egyetemi hallgatók mobilhasználati és biztonsági attitűdjeit vizsgálja. A hallgatók a közeljövő munkavállalói, akik nagy valószínűséggel BYOD-környezetben fognak dolgozni.

A kockázatvállalás vizsgálata azért releváns, mert:

- feltárja, hogy az egyének milyen mértékben hajlandók biztonsági kompromisszumot kötni a kényelem vagy a gyorsaság érdekében,
- rávilágít arra, hogy az észlelt kockázat mennyiben tér el a valós fenyegetettségtől,
- segít megérteni, hogy a technológiai eszközhasználat mennyiben párosul tudatos kockázatkezeléssel.

A BYOD nem csupán technológiai infrastruktúra, hanem döntési környezet is. Ebben a környezetben az egyéni kockázatvállalási hajlandóság közvetlenül befolyásolja a szervezeti biztonsági szintet.

A kockázatvállalás elemzése rámutat arra, hogy a BYOD-környezetben a technológiai sérülékenységek mellett az emberi tényező is meghatározó. Ez indokolja, hogy a következő alfejezetben az egyén szerepét a vállalati biztonságban, valamint a biztonsági kultúra és biztonságtudatosság kérdését részletesebben vizsgálom.

1.3 Az egyén szerepe a vállalati biztonságban

A BYOD-környezet egyik alapvető sajátossága, hogy a technológiai infrastruktúra és az emberi viselkedés szorosabban fonódik össze, mint a klasszikus, kizárólag vállalati tulajdonú eszközök esetében. Amíg a hagyományos vállalati IT-rendszerek esetén a kontroll jelentős része központilag gyakorolható, addig a saját tulajdonú eszközök bevonásával a biztonság egy része szükségszerűen decentralizálódik.

Ez a decentralizáció az egyén szerepét a vállalati biztonságban felértékeli.

1.3.1 A szervezet, mint technikai és emberi rendszer

Egy szervezet nem pusztán technológiai infrastruktúrák összessége, hanem emberek és folyamatok dinamikus rendszere. A vállalati információbiztonság így nem kizárólag technikai kontrollokkal írható le; az emberi tényező integráns része a biztonsági rendszernek.

Parsons és munkatársai [26] kimutatták, hogy a szervezeti biztonsági szint szoros kapcsolatban áll a szervezeti tagok biztonsághoz való attitűdjével. A tudás önmagában nem elegendő: az is meghatározó, hogy az egyén miként értelmezi a biztonsági szabályokat, mennyire érzi azokat saját felelősségének, és milyen mértékben azonosul a szervezet biztonsági céljaival.

BYOD esetében ez különösen kritikus, mivel:

- az eszköz fizikailag a munkavállaló birtokában van,
- a privát és vállalati használat gyakran egyazon eszközön történik,
- a felhasználó napi rutinjában nehezen különíthető el a „munka” és a „magán” kontextus.

A biztonság így nem csupán szabályozási kérdés, hanem magatartási kérdés is.

1.3.2 Biztonsági kultúra és biztonságtudatosság

A vállalati biztonsági kultúra vizsgálata az 1990-es évek végétől került előtérbe. Da Veiga és Eloff [57] szerint a biztonsági kultúra olyan attitűdökből, meggyőződésekből, értékekből,

tudásból és normákból áll, amelyek meghatározzák, hogy a szervezet tagjai miként viszonyulnak az információbiztonsághoz.

Lazányi [58] hangsúlyozza, hogy a biztonsági kultúra a vezetői döntések támogatásában is szerepet játszik, mivel befolyásolja a szervezet egészének kockázatérzékelését és reakcióit. Parsons és munkatársai [26] eredményei szerint a megfelelő attitűd kialakítása a biztonsági ismeretek mellett kulcsfontosságú a szervezeti biztonsági szint növelésében.

A biztonságtudatosság tehát nem pusztán információk birtoklása, hanem:

- a kockázatok felismerése,
- a felelősség vállalása,
- a szabályok belső elfogadása,
- és a tudatos döntéshozatal.

BYOD esetén a biztonságtudatosság különösen fontos, mert a felhasználó döntései közvetlenül befolyásolják a vállalati információs rendszer integritását.

1.3.3 A szabályozás korlátai

A biztonsági szint eléréséhez szükség van szabályokra mind a személyes, mind a vállalati szférában. Ugyanakkor nem minden kockázat kezelhető pusztán szabályozással.

Michelberger és Lábodi [59] szerint, a biztonsági szabályozás egyik legnagyobb korlátja, hogy hiába a fejlett informatikai háttér, ha a rendszert az emberi tényező – a belső munkatársak vagy partnerek gondatlansága, szabályszegése – továbbra is sebezhetővé teszi. Emellett egy valóban hatékony, minden szervezeti szintre kiterjedő holisztikus rendszer kiépítése és fenntartása rendkívül idő- és költségigényes, amelyhez sok vállalatnak egyszerűen nincs meg a megfelelő belső erőforrása.

Szabó Attila [60] szerint a tudatosság sok esetben fontosabb, mint a puszta szabályozás. A technológiai megoldások önmagukban nem képesek teljes védelmet biztosítani, amennyiben a felhasználók nem értik és nem támogatják azokat.

Keszthelyi [7] paradigmaváltásról ír az információbiztonság területén, hangsúlyozva az emberi tényező jelentőségét. A gyakran idézett megállapítás – miszerint a biztonsági rendszer leggyengébb láncszeme az ember – a BYOD kontextusában különösen releváns.

Kristóf [28] [29] rámutat arra is, hogy a biztonságtudatosság fejlesztése tudatos szervezeti stratégiát igényel. Oktatás, képzés és folyamatos kommunikáció nélkül a szabályzatok könnyen formálissá válhatnak.

BYOD esetében a túlzott kontroll akár ellenállást is kiválthat, míg a teljes szabályozatlanság magas kockázati szintet eredményez. A megoldás ezért a technológiai kontrollok és a tudatos magatartás egyensúlyában keresendő.

1.3.4 A biztonságtudatosság érettségi modellje

Schoop és Vasvári [30] biztonságtudatossági érettségi modellje jól szemlélteti, hogy a szervezetek milyen fejlődési szinteken haladhatnak keresztül:

0. – Nem létező: a jó gyakorlat teljes hiánya
1. – Kezdő: ad hoc felismerés
2. – Ismételhető, de intuitív: növekvő tudatosság, de nem dokumentált
3. – Meghatározott folyamat: szabályozott, ismert felelősségi körök
4. – Menedzselt és mérhető: dokumentált, mérhető folyamatok
5. – Optimalizált: folyamatos fejlesztés és önértékelés

A BYOD-bevezetés sikeressége jelentős mértékben függ attól, hogy a szervezet ezen érettségi skála mely szintjén helyezkedik el. Alacsony érettségi szint esetén a saját tulajdonú eszközök integrációja aránytalanul magas kockázatot hordozhat.

1.3.5 Kapcsolódás a kutatáshoz

A jelen kutatás egyik központi kérdése, hogy a felsőoktatásban tanuló hallgatók – mint jövőbeli munkavállalók – milyen biztonságtudatossági és kockázatvállalási attitűddel rendelkeznek.

A BYOD-környezetben a következő tényezők különösen relevánsak:

- elkülönítik-e a magán és vállalati adatkezelést,
- frissítik-e rendszeresen eszközeiket,
- tudatosan kezelik-e az alkalmazás-jogosultságokat,
- mennyire hajlandók biztonsági kompromisszumot kötni a kényelem érdekében.

Amennyiben a hallgatók – akik a digitális eszközök intenzív használói – alacsony biztonságtudatossági szinttel rendelkeznek, úgy a jövőbeli szervezetek számára a BYOD nem pusztán technológiai, hanem kulturális és oktatási kihívást is jelent.

A kutatás ezért nemcsak a jelenlegi állapot feltérképezését célozza, hanem hozzájárulhat egy olyan döntéstámogatási és oktatási keretrendszer kialakításához, amely a BYOD kockázatok csökkentését szolgálja.

1.4 A kockázat fogalma és értelmezése BYOD-kontextusban

A BYOD jelenség sajátossága, hogy a szervezet informatikai és információbiztonsági környezete kitágul: a vállalati rendszerekhez való hozzáférés nem kizárólag szervezeti tulajdonú, standardizált és központilag menedzselt eszközökön keresztül történik, hanem heterogén, eltérő állapotú és eltérően használt, magántulajdonú végpontokon is. Ennek következtében az információbiztonsági kérdések nem pusztán technológiai problémaként jelennek meg, hanem szervezeti döntési helyzetként is: a szervezetnek mérlegelnie kell, milyen kockázatokat fogad el, melyeket csökkent, melyeket hárít át, és mindezt milyen költségek mellett teszi.

A BYOD-környezetben a kockázatok különösen összetettek, mivel egyszerre jelennek meg technológiai sérülékenységek, fizikai kitettségek, kommunikációs kockázatok és humán tényezőből fakadó bizonytalanságok. A fejezet célja ezért a BYOD-hoz kapcsolódó kockázatok elméletileg megalapozott keretben történő értelmezése: először a kockázat fogalmának tisztázásával, majd a BYOD sajátos kockázati struktúrájának bemutatásával.

1.4.1 A kockázat definíciója: érték és bizonytalanság kapcsolata

A kockázat fogalmának számos meghatározása ismert, de közös elemük, hogy a kockázat mindig valamilyen értékvesztés lehetőségéhez és bizonytalan kimenetelhez kapcsolódik. A dolgozat alapdefiníciójaként Renn meghatározását [11] [12] alkalmazom, amely két domináns megközelítést különít el: egyrészt a kockázat olyan helyzet vagy esemény, amelyben valamilyen emberi érték – beleértve magukat az embereket is – forog kockán, és a kimenetel bizonytalan; másrészt a kockázat egy esemény vagy tevékenység bizonytalan következménye valamilyen emberi értékkel kapcsolatban.

A két meghatározás ugyanazt a szerkezetet írja le eltérő nézőpontból. Az első a kockázatra, mint helyzetre, a második pedig, mint következményre tekint. A BYOD esetében mindkét értelmezés releváns: a BYOD egyrészt új, kockázati helyzetet teremt azáltal, hogy heterogén végpontokon keresztül biztosít hozzáférést a szervezeti rendszerekhez; másrészt bizonytalan következményeket hordoz, mivel nem garantálható, hogy az eltérő eszközállapotok és felhasználói viselkedés nem vezet incidensekhez.

A definíció egyik központi eleme az, hogy valamilyen érték forog kockán. BYOD-környezetben ez az érték több szinten jelenik meg: üzleti információk és szellemi tulajdon, személyes

adatok és azok jogszerű kezelése, a szolgáltatások működőképessége és rendelkezésre állása, a szervezet reputációja és a partnerek bizalma, végső soron pedig maga a működési képesség. A másik központi elem a bizonytalanság, amely BYOD esetében nem pusztán arra vonatkozik, hogy bekövetkezik-e támadás, hanem arra is, hogy a munkavállaló mennyiben követi a szabályokat, milyen állapotú az eszköze, milyen hálózatra csatlakozik, hová kerülnek az adatok és mentések, milyen gyorsan észlelhető egy incidens, és milyen mértékű kár realizálódik. A kockázat így nem egyetlen eseményhez, hanem döntési pontokból és eseményláncokból álló folyamatokhoz kapcsolódik.

1.4.2 A „100%-os biztonság” elvi lehetetlensége és a kockázat természetes volta

A kockázat értelmezéséhez hozzátartozik annak felismerése, hogy a biztonság nem abszolút állapot. Nem létezik százszázalékos biztonság [7], mivel minden rendszerben maradnak ismeretlen sérülékenységek, előre nem látható emberi hibák és olyan külső körülmények, amelyek a kontrollhatáron kívül esnek. Ez a tétel különösen érvényes a BYOD esetében, ahol a szervezet kontrollja eleve részleges a magántulajdonú eszközök felett [18].

A biztonság ezért nem a kockázat teljes megszüntetését jelenti, hanem annak tudatos kezelését. A szervezet azonosítja a kockázatokat, a lényegeseket kezeli, a maradékkockázatot pedig meghatározott keretek között elfogadja. A BYOD-dal kapcsolatos döntés így nem arról szól, hogy a megoldás „biztonságos-e vagy sem”, hanem arról, hogy a vállalható kockázati szint összhangban van-e a szervezeti célokkal, az erőforrásokkal és a működési igényekkel

1.4.3 Optimális biztonsági szint: költség–biztonság kompromiszum

A szervezeti kockázatkezelés egyik alaptétele, hogy a biztonság növelése költségekkel jár, és a magasabb biztonsági szint elérésére fordított ráfordítás egy bizonyos ponton túl aránytalanul megnő. A cél ezért nem a maximális, hanem az optimális biztonsági szint meghatározása, amely a költségek és a biztonsági hasznok szempontjából a legkedvezőbb egyensúlyt jelenti [61].

BYOD-környezetben ez a megközelítés különösen releváns, mivel a szervezet egyszerre szembesül megelőzési költségekkel – például szabályzatalkotás, technológiai védelem, oktatás –, észlelési és reagálási költségekkel – monitorozás, incidenskezelés –, valamint a maradékkockázat költségeivel, amelyek incidensek, bírságok vagy reputációs károk formájában jelenhetnek meg. Emellett figyelembe kell venni a használhatósági és produktivitási költségeket is: a túl szigorú kontroll csökkentheti az elfogadottságot és növelheti a ShadowIT irányába történő elmozdulást. Az optimális biztonsági szint ezért nem pusztán technológiai optimum, hanem

szervezeti optimum is, amelyben a kockázatcsökkentés arányos a ráfordítással, és nem vált ki a biztonságot összességében gyengítő ellenreakciókat.

1.4.4 Kockázat, sérülékenység és fenyegetés BYOD-környezetben

A kockázat gyakorlati értelmezéséhez szükséges elkülöníteni a hozzá kapcsolódó alapfogalmakat. Sérülékenység alatt olyan gyengeséget értünk az eszközben, a folyamatban vagy a felhasználói magatartásban, amely lehetővé teszi a károkozást. BYOD-környezetben ilyen sérülékenység lehet a frissítések hiánya, a nem megfelelő eszközvédelem vagy a magán- és vállalati adatok keveredése. Fenyegetésnek tekinthető minden olyan hatás vagy szereplő, amely képes a sérülékenységet kihasználni; ez lehet rosszindulatú támadó, kártékony alkalmazás vagy akár nem szándékos felhasználói hiba is. A következmény pedig az értékvesztés konkrét formája, amely adatvesztésben, adatkiszivárgásban, szolgáltatás-kiesésben vagy reputációromlásban nyilvánulhat meg.

A BYOD sajátossága abban áll, hogy a vállalati környezetben megszokott kontrollmechanizmusok – standard eszközpark, központi menedzsment, homogén konfigurációk – csak részben érvényesíthetők. A kockázati tér szerkezete átalakul: a szervezet „pereme” heterogén és dinamikusan változó végpontokra tolódik ki, miközben a felhasználók preferenciái, kényelmi szempontjai és attitűdjei erősebben befolyásolják a biztonsági eredőt.

1.5 A fejezet összefoglalása

A disszertáció első fejezete a saját tulajdonú mobileszközök munkacélú használatának, BYOD elméleti alapjait mutatja be. Nem csak a kérdés technológiai megközelítését, de az emberi és döntéshozatali tényezőkre is kitér.

Alapvetésem, hogy bár az informatikai védelem sokat fejlődött, a biztonsági lánc leggyengébb láncszeme továbbra is az ember.

Az új generáció és a digitális környezet

A fejezet részletesen elemzi az Y és Z generáció (digitális bennszülöttek) jellemzőit, akik számára a mobil infokommunikációs eszközök használata természetes és rutinszerű. Ez a „technológiai természetesség” azonban kettős hatással bír: azonnaliság és kényelem.

A felhasználók gyors válaszokat és folyamatos online jelenlétet várnak el, ami miatt a kényelmi szempontok gyakran felülírják a biztonsági előírásokat is. Mobilitás és szabadság: A munkavégzés térbeli és időbeli kötöttségeinek feloldása (digitális nomád életmód) növeli a BYOD iránti igényt, de egyben ellenőrizhetetlen hálózati környezeteket is teremt.

Shadow IT jelenség: Amennyiben a szervezeti szabályozás túl lassan követi le az informatikai igényeket vagy a szükségesnél is korlátozóbbnak ítélik meg, a felhasználók hajlamosak saját, nem kontrollált informatikai megoldásokat alkalmazni a feladatok elvégzésére.

Kockázatvállalás és döntéselmélet

A kockázatot nem csupán technikai paraméterként, hanem az észlelt haszon és az észlelt kockázat közötti szubjektív mérlegelés eredményeként értelmezem ebben a helyzetben. A kutatásom Weber és munkatársai által kidolgozott DOSPERT-skálára támaszkodik, amely a kockázatvállalási hajlandóságot doménspecifikusan méri. A fejezet legfontosabb eredményei és megállapításai ezen a területen az úgy nevezett percepciós aszimmetria; vagyis, a felhasználók hajlamosak alulbecsülni a digitális kockázatokat („velem úgysem történik meg", „én nem vagyok elég fontos, hogy egy ilyen támadás célpontja legyek" stb..), miközben a kényelemből fakadó azonnali hasznot túlértékelik.

Haszon-domináns döntési architektúra: Az IT-biztonsági döntésekben az észlelt előnyök súlya szignifikánsan meghaladja a kockázati tényezőkét.

A technikai kompetencia paradoxona: Kimutatásra került, hogy a magasabb technikai tudás nem feltétlenül jár együtt nagyobb szabálykövetéssel; sőt, a magabiztosabb felhasználók olykor kockázatosabb műveleteket is megtesznek (pl. vállalati adatok saját eszközre másolása).

Az egyén szerepe a vállalati biztonságban

A fejezet hangsúlyozza, hogy a BYOD-környezetben a biztonsági kontroll „pereme" a felhasználó kezében lévő eszközre tolódik el. A biztonsági kultúra és a tudatosság ezért fontosabbá válik, mint a puszta technológiai korlátozás.

A szabályozás korlátai: A túl szigorú tiltás ellenállást és Shadow IT-t szül, ezért az optimális biztonsági szintnek figyelembe kell vennie a használhatóságot és a produktivitást is.

Metaadat-kitettség: Külön kiemelt terület a mobileszközök által generált metaadatok (helyszín, hálózati adatok) kockázata, amely különösen katonai és kritikus infrastruktúra környezetben bír stratégiai jelentőséggel.

Legfontosabb hivatkozások a fejezetben

- Michelberger Pál (2022): Információ-, folyamat- és vállalatbiztonság [6]
- Keszthelyi András (2015): Paradigmaváltás - biztonság - emberi tényező [7]

- Weber U. Elke, Blais Renée Ann, Betz E. Nancy (2002): A Domain-Specific Risk-Attitude Scale: Measuring Risk Perceptions and Risk Behaviors [27]
- Renn (2017): Risk Governance, Coping with Uncertainty in a Complex World. [12]
- ENISA (2013): Az okostelefonokhoz kapcsolódó legfontosabb információbiztonsági kockázatok rendszerezése. [34]

Összességében az 1. fejezet tudományos újdonsága, hogy az IT-biztonsági kockázatvállalást nem általános személyiségjegyként, hanem egy helyzetfüggő, haszonorientált döntési folyamatként azonosítja, amelyben a generációs sajátosságok és az egyéni percepciók dominálnak a technikai korlátok felett.

2 A BYOD SZOCIO-TECHNIKAI RENDSZERE: TECHNOLÓGIAI, SZERVEZETI ÉS KOCKÁZATI DIMENZIÓK

2.1 Saját tulajdonú okoseszközök a vállalati információs térben: a BYOD

Az elmúlt években a mobilinformatikai eszközök robbanásszerű elterjedése figyelhető meg, amely a magánéleti felhasználáson túl egyre markánsabban jelenik meg a szervezeti működésben is. A hordozható eszközök technológiai fejlődése – a hardver teljesítményének növekedése, az alkalmazáskínálat bővülése, valamint a mobilhálózatok sávszélességének és lefedettségének javulása – a mindennapi munkavégzésben is olyan használati mintázatokat alakított ki, amelyek korábban kizárólag munkaállomásokhoz vagy laptopokhoz kötődtek. Az okoseszközök vállalati célú megjelenése ezért nem pusztán egy újabb technológiai csatornát jelent, hanem az információkezelés, a hozzáférés és a kontroll strukturális átalakulását is [62].

Jelen disszertációban mobilinformatikai eszközök alatt olyan hordozható infokommunikációs készülékeket értek, amelyeket a felhasználók jellemzően nem tekintenek hagyományos értelemben vett számítógépnek, ugyanakkor funkcionalitásuk a számítógépes képességekhez közelít. E fogalmi keretbe tipikusan a különböző rendszerű okostelefonok és tabletek tartoznak, ezen belül is hangsúlyosan az okostelefonok, amelyek a „kényelmesen, szinte bárhol, szinte bármikor” használható platformként váltak dominánssá [14] [15] [16]. A definíció szempontjából különösen lényeges a felhasználói percepció – „nem számítógép” – és a tényleges funkcionális kapacitás – „számítógépszerű használat” – közötti feszültség, amely a szervezeti információbiztonság szempontjából meghatározó jelentőségű.

Az okoseszközök fejlődése kettős irányt követett: egyrészt a hordozhatóság és a használhatóság optimalizálása, másrészt a képességek folyamatos bővülése volt megfigyelhető. A mobileszközök a kezdeti telefonálási és üzenetküldési funkciókon túl olyan szolgáltatásokat integráltak, amelyekhez korábban jellemzően számítógépre volt szükség, így dokumentumkezelést, felhőalapú együttműködést, vállalati alkalmazások futtatását, adatbázis-elérést vagy üzleti folyamatok támogatását. Ezzel párhuzamosan a mobilhálózatok technikai paramétereinek fejlődése olyan kommunikációs alapot teremtett, amely a folyamatos és helyfüggetlen hozzáférést számos szervezetben a munkavégzés természetes részévé tette.

A vállalati használat szempontjából az okoseszközök egyik sajátossága, hogy a felhasználók eltérően viszonyulnak hozzájuk, mint a „klasszikus” munkahelyi számítógépekhez. Míg a munkaállomásokat vagy laptopokat kifejezetten munkacélú, szabályozott eszközként kezelik, addig az okostelefonok és tabletek a mindennapi élet természetes részeként, személyes eszközként

jelennek meg. Ez a használói attitűd azért különösen releváns, mert e készülékek a szervezeti infrastruktúra irányába ugyanazokat a hozzáférési és adatkezelési képességeket biztosíthatják, mint a vállalati számítógépek: vállalati adatok megnyitását, szerkesztését, továbbítását vagy – nem megfelelő kontroll esetén – törlését is. Ennek következtében az okoseszközöket információbiztonsági nézőpontból az IT-infrastruktúra integrált, teljes értékű elemeként szükséges kezelni.

A szervezeti gyakorlatban az okoseszközök vállalati alkalmazásának egyik leggyakoribb területe a kommunikáció. A munkahelyi e-mail rendszerek elérése okostelefonról mindennapossá vált, és ezzel párhuzamosan megjelentek az üzleti célú üzenetküldő és együttműködést támogató platformok is, amelyek vállalati adatokat közvetítenek. A mobileszközökön keresztül elérhetők hálózati meghajtók, megosztott dokumentumtárak, vállalati adatbázisok, vezetői információs rendszerek és egyéb kritikus erőforrások is. A szervezet számára így nem az a kérdés, hogy a mobileszközök megjelennek-e az IT-környezetben, hanem az, hogy milyen kontrollmechanizmusok és szabályozási keretek mellett történik mindez, és milyen kockázatokat generál a hozzáférés kiterjesztése.

A saját tulajdonú eszközök munkahelyi használatának jelenségét a szakirodalom a BYOD fogalommal jelöli [63] [64] [65] [66] [67]. A BYOD keretében a munkavállalók saját, magántulajdonban lévő, jellemzően fogyasztói eszközeiket – például laptopokat, táblagépeket vagy okostelefonokat – használják professzionális kontextusban. A fogalom tehát nem általános értelemben vett „saját eszköz” használatot jelent, hanem kifejezetten a saját informatikai eszközök szervezeti célú alkalmazását.

A definíció több forrásban is hasonló módon jelenik meg. A Macmillan English Dictionary [68] szerint a BYOD gyakorlata azt jelenti, hogy a munkavállalók vagy hallgatók saját számítástechnikai eszközeiket viszik be a munkahelyre vagy oktatási intézménybe, és azokat a szervezet hálózatán használják. Baillette, Barlette és Leclercq-Vandelannoitte értelmezésében a jelenség magántulajdonú fogyasztói eszközök professzionális környezetben való alkalmazását jelenti, tipikusan laptopok, tabletek és okostelefonok formájában [17]. A hazai megközelítések közül Budai Balázs Benjamin megfogalmazása a gyakorlat lényegét ragadja meg: „Hozd a saját kütyüdet, és dolgozz azzal!” [69]. A definíciók közös elemei a magántulajdon, a professzionális használati kontextus és a szervezeti erőforrásokhoz – hálózathoz, rendszerekhez, adatokhoz – való hozzáférés.

A BYOD szervezeti relevanciáját tovább növeli, hogy a készülékek nemcsak kommunikációra, hanem vállalati adatkezelésre is alkalmazhatók, ami bizalmas adatokhoz való hozzáférést jelent [16]. A munkavállalók a kényelem és a megszokott felhasználói élmény miatt sok esetben elvárják, hogy személyes mobileszközeik a vállalati rendszerekhez ugyanúgy hozzáférést biztosítsanak, mint a munkahelyi számítógépek, beleértve a vállalati felhőt, az intranetet, az ERP-rendszereket, a levelezést vagy a dokumentumtárakat [16] [17] [70]. A hozzáférés kiterjesztése és a privát–üzleti használat összemosódása ugyanakkor a kontroll csökkenésének és a biztonsági szint potenciális gyengülésének kockázatát hordozza.

A disszertáció keretében a BYOD-eszköz fogalma ezért olyan hordozható informatikai eszközként határozható meg, amely képességeit tekintve közel azonos egy általános számítógépével – hálózati átviteli kapacitás, képernyőfelbontás, memória- és számítási kapacitás tekintetében –, ugyanakkor a felhasználói megítélés szerint nem laptop vagy hagyományos számítógép, és a munkavállaló tulajdonában áll. E definíció egyesíti a funkcionalitást, a percepciót és a tulajdonjogi keretet, amelyek együtt adják a BYOD szervezeti jelentőségét és információbiztonsági sajátosságait.

A fejezetben tárgyalt fogalmi és használati keretek kijelölik a további elemzések irányát. A BYOD nem pusztán technológiai jelenség, hanem olyan szervezeti döntési helyzet, amelyben a hozzáférés biztosítása, a kontroll eszközei, a szabályozás és a felhasználói attitűdök együttesen alakítják a biztonsági kockázatok szerkezetét. A következő alfejezetek ezért a mobileszközök biztonsági kihívásait, a BYOD szervezeti szabályozási lehetőségeit és az ezekből fakadó dilemmákat részletezik.

2.2 A BYOD és a katonai információbiztonsági környezet sajátosságai

A BYOD jelenség a polgári és vállalati információbiztonsági környezetben elsősorban hatékonysági, költség- és felhasználói élmény szempontból merül fel, ugyanakkor katonai és honvédelmi kontextusban a kérdés stratégiai jelentőséggel bír. A fegyveres erők információs rendszerei a klasszikus informatikai infrastruktúrán túl műveleti, vezetési és irányítási (C2), valamint hírszerzési és felderítési rendszerekbe ágyazódnak, amelyek működése közvetlenül befolyásolja a műveleti képességet és a nemzeti biztonságot. Ebben a környezetben a mobileszköz nem pusztán végpont, hanem potenciális perem-infrastruktúra elem, amely a védett hálózatok és a nyílt információs tér közötti átmeneti zónában helyezkedik el.

A modern katonai rendszerek egyre inkább hálózatközpontú működésre épülnek, ahol az információ megosztása, feldolgozása és továbbítása valós idejű, integrált struktúrában történik [71]

[72]. Ebben a modellben is a végpontok megbízhatósága és integritása kulcskérdés, mivel a rendszer egészének sérülékenysége a leggyengébb elem biztonsági szintjétől függ. A BYOD ebben a kontextusban a kontroll decentralizálódását jelenti: a szervezet által teljes mértékben menedzselt eszközök mellett megjelennek olyan magántulajdonú végpontok, amelyek felett a közvetlen műszaki és adminisztratív kontroll korlátozott. Ez a kontrollmegosztás új típusú kockázati szerkezetet hoz létre, amelyben a technológiai sérülékenységek és a felhasználói döntések egyaránt stratégiai jelentőségűvé válnak.

Katonai környezetben a kockázat értelmezése túlmutat az üzleti adatvesztés vagy reputációs kár dimenzióján. A minősített adatok védelme, a műveleti tervek bizalmassága, a személyi állomány mozgására vonatkozó metaadatok, valamint a kommunikációs csatornák integritása mind olyan értékek, amelyek sérülése nem csupán szervezeti, hanem nemzetbiztonsági következményekkel járhat. A kockázat klasszikus meghatározása – amely az érték, a fenyegetés, a sérülékenység és a bizonytalanság kapcsolatára épül – ebben a környezetben kiegészül a stratégiai hatás dimenziójával [11] [12] [73]. Egy látszólag alacsony szintű incidens – például metaadat-szivárgás vagy nem megfelelően konfigurált mobilalkalmazás – aggregált formában műveleti mintázatokat tehet láthatóvá, ami a katonai döntéshozatal biztonságát érintheti.

A kibertér hadműveleti dimenzióként történő értelmezése tovább erősíti a BYOD relevanciáját. A kiberhadviselés és az információs műveletek környezetében a támadási felület nem kizárólag a klasszikus szerver- és hálózati infrastruktúrára korlátozódik, hanem kiterjed a mobil végpontokra is [74]. A saját tulajdonú eszközök használata növelheti a sérülékenységi varianciát, különösen akkor, ha az eszközök eltérő frissítési állapotban vannak, különböző alkalmazás-ökoszisztémákhoz kapcsolódnak, vagy a felhasználói magatartás nem illeszkedik a szervezeti biztonsági kultúrához. A katonai szervezetekben a biztonsági kultúra és a fegyelmezett működés hagyományosan erős, azonban a digitális generációk megjelenésével a személyes és szervezeti információhasználat közötti határ elmosódása új kihívásokat teremt.

A biztonságtudományi megközelítés szerint a védelmi rendszerek hatékonysága nem csupán technológiai kérdés, hanem komplex, szocio-technikai rendszer eredője [75]. A BYOD ebben a keretben olyan rendszerelemként értelmezhető, amelyben a technológiai, szervezeti és humán tényezők kölcsönhatása határozza meg a tényleges kockázati szintet. A kontroll nem kizárólag műszaki eszközökkel érvényesül, hanem szabályozási, képzési és kulturális mechanizmusokon keresztül is. Katonai környezetben különösen fontos a döntési lánc integritása: a végponti kockázatvállalás – akár egyéni kényelmi döntés formájában – szervezeti szintű következményekhez vezethet.

A BYOD katonai kontextusban ezért nem egyszerűen informatikai irányítási kérdés, hanem a rendszerbiztonság és a műveleti képesség egyik strukturális tényezője. A saját tulajdonú eszközök integrációja csak akkor illeszthető a honvédelmi információbiztonsági architektúrába, ha a kontrollmegosztás, a kockázatvállalás és a döntési felelősség kérdése explicit módon kezelésre kerül. Ez indokolja, hogy a BYOD vizsgálata ne kizárólag technológiai vagy szervezeti síkon történjen, hanem a döntéselméleti és kockázatelméleti dimenziók integrált keretében, különös tekintettel a humán tényező szerepére.

2.3 BYOD eszközök vállalati felügyelete és szabályozási keretrendszere - tulajdonjog, kontrollhatárok, Shadow IT és mobileszköz-menedzsment (MDM)

A vállalati hálózatokban a mobilinformatikai eszközök használata folyamatosan növekszik [76]. Önmagában a mobileszközök elterjedése nem új jelenség, a BYOD térnyerésével azonban a szervezetek olyan helyzetbe kerültek, amelyben a vállalati erőforrások elérése egyre gyakrabban nem kizárólag vállalati tulajdonú és menedzselt eszközökön keresztül valósul meg. A BYOD egyik meghatározó sajátossága ebben a kontextusban az, hogy az eszközök tulajdonjoga és a szervezeti kontroll lehetősége szétválik: miközben a szervezetnek közvetlen üzleti érdeke fűződik a biztonságos hozzáféréshez, a magántulajdonú eszközök felett csak korlátozott közvetlen kontrollt képes gyakorolni. Ez a kettősség a BYOD-t alapvetően szervezeti döntési dilemmává alakítja, mert a hozzáférés biztosítása, a kockázati kitettség és a kontrollmérték kérdése egyszerre jelenik meg.

A BYOD gyakorlati alkalmazhatósága szorosan kapcsolódik a munkavégzés szervezeti elvárásaihoz. Amennyiben a munkakör megköveteli a folyamatos elérhetőséget, illetve az irodán kívüli munkavégzést, akkor a kommunikáció és a hozzáférés módja, költsége és biztonsági kontrollja kiemelt kérdéssé válik. Ilyen helyzetben felmerül, hogy a vállalat biztosít-e eszközt, vagy a munkavállaló saját eszközének használata (BYOD) válik domináns megoldássá, ugyanakkor a szervezeti integráció szempontjából nem elegendő pusztán a hozzáférés tényét vizsgálni. Érdemi kérdéssé válik az eszköz technológiai alkalmassága is: az operációs rendszer, a szoftverkörnyezet és a biztonsági beállítások mennyiben integrálhatók a vállalati infokommunikációs technológiába, és ez milyen kockázati következményekkel jár [4] [5].

A BYOD szabályozásának egyik legfontosabb kiindulópontja az eszköz tulajdonjoga. Ha az eszköz vállalati tulajdonban van, a szervezet – megfelelő jogi és belső szabályozási keretek mellett – lényegesen nagyobb kontrollt gyakorolhat a használat felett, és meghatározhatja, hogy

az eszköz mennyiben és milyen feltételekkel használható magáncélra, milyen alkalmazások telepíthetők, milyen hitelesítési eljárások kötelezők, és milyen módon történhet a hozzáférés a vállalati rendszerekhez [19]. Ez a kontroll különösen akkor érvényesíthető egyszerűen, ha az eszközhasználat fizikailag is a vállalati telephelyhez kötődik, és a hálózati környezet viszonylag zárt. Ugyanakkor a kontroll vállalati tulajdon esetén sem tekinthető automatikusan stabilnak, mert ha az eszközt a vállalati környezeten kívül, távoli helyszíneken is használják, a szervezetnek technológiai és eljárásrendi óvintézkedéseket kell alkalmaznia a vállalati infokommunikációs technológia védelmére, például mobileszköz-menedzsment megoldások (MDM) alkalmazásával. A távoli használat ebben az értelemben a kontroll részleges elvesztését jelenti, hiszen az eszköz a szervezet „határain" kívül működik heterogén hálózati környezetben, változó fizikai kockázatokkal és eltérő felhasználói szituációk mellett.

Magán tulajdonú eszköz esetén a szervezet kontroll-lehetősége még korlátozottabb, és a menedzsment kérdése lényegesen érzékenyebb. A saját eszköz használata a munkáltató számára költség- és hatékonysági szempontból előnyös lehet, ugyanakkor a teljes körű ellenőrzés és menedzsment nem kezelhető olyan egyszerűen, mint vállalati tulajdon esetén. Ennek oka nem pusztán technológiai, hanem humán és szervezeti jellegű is: a magán eszköz a munkavállaló számára személyes tér, amelyen privát adatok, alkalmazások, kommunikáció és digitális identitás is jelen van, ezért a szervezet által alkalmazott kontrollmechanizmusok – ha túl erősek vagy invazívak – ellenállást válthatnak ki, és szélsőséges esetben akár a szervezet elhagyása felé is hathatnak. A BYOD kezelésének egyik lényegi problémája így az, hogy a túl szigorú kontroll és a túl laza szabályozás egyaránt kockázatnövelő hatású lehet: előbbi ellenreakciókat és megkerülő megoldásokat, utóbbi kontrollvesztést és átláthatatlan gyakorlatokat eredményezhet.

Ebből következik, hogy a saját tulajdonú eszközök szervezeti tiltása sem feltétlenül oldja meg a problémát. A munkavállaló dönthet úgy, hogy nem használja a vállalati eszközt, vagy – ami a gyakorlatban tipikusan gyakoribb kimenet – a tiltás ellenére is igénybe veszi a saját eszközét munkacélra. Ez a jelenség közvetlenül kapcsolódik a ShadowIT kialakulásához. A ShadowIT lényege, hogy a munkavállalók a szervezet által kialakított, szabályozott és üzemeltetett informatikai rendszerek mellett és/vagy helyett saját informatikai megoldásokat használnak, vagyis olyan adatáramlást és szolgáltatáshasználatot hoznak létre, amely a formális kontrollon kívül esik. A BYOD és a ShadowIT összefüggése különösen fontos, mert a BYOD szervezeti tiltása vagy a nem megfelelően kialakított hozzáférési környezet éppen azt a kimenetet erősítheti, amelyet a szervezet el akar kerülni. A gyakorlatban tipikus eltérésnek tekinthető például a munkával

kapcsolatos e-mailek és mellékleteik továbbítása magánpostafiókba, illetve privát eszközre, ami kontrollálatlan adatmozgást és kockázatnövekedést eredményezhet [77] [78] [79] [80] [81] [82]. A döntési dilemma ebben a helyzetben jól látható: a tiltás, mint egyszerű szabály nem garantálja a tényleges tiltást a gyakorlatban, viszont növelheti a rejtett, nem dokumentált és nem menedzselt megoldások használatának valószínűségét, így a szervezet formálisan erősít a kontrollon, ténylegesen azonban csökkentheti a kontrollálhatóságot. Ezért a BYOD kérdés kezelése nem szűkíthető egy „igen/nem" típusú döntésre, hanem kontroll-, szabályozási- és technológiai keretrendszerben értelmezendő.

A mobileszközök szervezeti integrációja ezzel összefüggésben technológiai menedzsmentet igényel. Vállalati tulajdon esetén a menedzsment a szervezet részéről sokkal egyértelműbben végrehajtható, magántulajdon esetén azonban a menedzsment módja, mértéke és elfogadottsága válik kulcskérdéssé. A szervezetek gyakorlati válasza tipikusan valamilyen MDM (Mobile Device Management) vagy kapcsolódó mobileszköz-menedzsment megoldás alkalmazása, amely képes lehet a vállalati hozzáférés kontrolljára, a konfigurációk kezelésére, illetve bizonyos biztonsági követelmények érvényesítésére. A technológiai menedzsment azonban önmagában nem elegendő, mert szükséges hozzá egy írásos és követhető eljárási keretrendszer is, amely a szervezeti műveletek és a bizalmas információk kommunikációjának ellenőrzését is lehetővé teszi [83]. A heterogén információs technológiával rendelkező szervezetekben az egységesítés és a szabályozottság bevezetése idővel egyre nehezebbé válhat [79] [84], és a BYOD éppen ezt a heterogenitást növeli, mert különböző eszközök, operációs rendszerek, alkalmazások és felhasználói beállítások jelennek meg ugyanazon szervezeti hálózaton és ugyanazon üzleti folyamatokban [85]. A szervezet szempontjából a BYOD kezelése ezért lényegében egy „kontrollált heterogenitás" kialakításának feladata, ahol a teljes egységesítés sokszor nem reális (és nem is feltétlen cél), de minimumkövetelmények, elfogadott eszközlisták, kötelező biztonsági beállítások és a vállalati adatok elkülönítését támogató eljárások szükségesek [16].

A szakirodalom és a szervezeti gyakorlat alapján a munkáltatók többféle, egymástól markánsan eltérő BYOD-hoz kapcsolódó szabályozási választ követhetnek, és a BYOD mint eszközhasználati forma inkább egy szabályozási kontinuum mentén értelmezhető, mintsem bináris döntésként. A dolgozatban alkalmazott felosztás szerint a munkáltatói viszonyulás megjelenhet a személyes mobileszközök üzleti célú használatának tiltásában, a BYOD „eltűrésében" formális szabályozás nélkül [86], eseti, szóbeli vezetői engedélyhez kötött használatban, illetve írásos szabályzat kialakításában, amely információbiztonsági elemeket is tartalmaz a hozzáférési protokollok, a jóváhagyott eszközök és alkalmazások, az elfogadható operációs rendszer, a

kötelező biztonsági szoftverek, a megengedett adatkezelési műveletek, a naplózás és az adatszegregáció körében [16] [70] [87]. A kontinuum másik végén a BYOD aktív ösztönzése és támogatása áll [88]. A kategóriák tanulsága, hogy a BYOD szervezeti kezelése nem redukálható technológiai kérdéssé, mert a szabályozási szint kiválasztása a szervezeti kultúrához, a munkavégzés jellegéhez, az adatérzékenységhez és a humán tényezőhöz is kötődik. A túl laza megközelítés kontrollvesztést eredményezhet, míg a túl szigorú megközelítés ellenállást és ShadowIT irányú elmozdulást válthat ki.

Mindez indokolja, hogy a BYOD esetében a szervezet technológiai és szabályozási eszközei szükségesek, de nem elégségesek. A biztonsági szintet az is meghatározza, hogy a felhasználók milyen hozzáállással és attitűddel viszonyulnak a biztonsághoz, mert a kontroll BYOD környezetben részben szükségszerűen „átcsúszik" a felhasználói döntések szintjére: a felhasználó választ hálózatot, alkalmazást, adatkezelési rutint, és saját kényelem–biztonság kompromisszumai mentén viszonyul a szervezeti előírásokhoz. Emiatt a következő alfejezetekben indokolt a mobileszközök biztonsági fenyegetettségének részletesebb áttekintése, valamint annak bemutatása, hogy a technológiai kockázatok és a felhasználói döntések miként kapcsolódnak össze a BYOD-ban.

2.4 Mobileszköz-biztonság: fenyegetési tér, fizikai kitettség és humán faktor

A mobileszközök vállalati integrációja nem választható el azok biztonsági sajátosságaitól. Bár az okostelefonok és táblagépek funkcionalitásukban egyre inkább közelítenek a hagyományos számítógépekhez, biztonsági architektúrájuk, használati környezetük és a hozzájuk kapcsolódó felhasználói attitűdök több ponton eltérnek azoktól. A mobileszközök biztonsági vizsgálata ezért nem kizárólag technológiai kérdés, hanem szervezeti és humán dimenziókat is magában foglaló, komplex probléma.

2.4.1 A korai biztonsági aggályoktól a tömeges fenyegetettségig

Az okostelefonokkal kapcsolatos biztonsági aggályok már a 2000-es évek elején megjelentek. Gareth James 2004-ben publikált cikkében [89] rámutatott arra, hogy bár az akkori PDA-k és korai okostelefonok esetében még nem léteztek széles körben ismert, kifejezetten ezekre célzott rosszindulatú szoftverek, ugyanakkor több olyan sérülékenység volt azonosítható, amely potenciálisan lehetővé tette volna támadások sikeres végrehajtását. Az eszközök ekkor még korlátozott számban voltak jelen, ugyanakkor jellemzően politikai és üzleti döntéshozók használták őket, így potenciális célpontként kiemelt értéket képviseltek.

Azóta a helyzet alapvetően megváltozott. Az okostelefonok globális penetrációja tömegessé vált, a felhasználói kör kiszélesedett, és ezzel párhuzamosan a támadási felület is jelentősen megnőtt. A mobileszközök már nemcsak stratégiai jelentőségű célpontok, hanem tömegesen kihasználható platformok is. A fenyegetettség szerkezete is átalakult: a sérülékenységek feltárása és javítása folyamatos versenyhelyzetben zajlik a fejlesztők és a támadók között.

A rosszindulatú szoftverek számának növekedését több kutatás is alátámasztja. Már 2012-ben az F-Secure felmérése szerint 238 ismert mobil kártevő mellett abban az évben további 804 új, Android operációs rendszerhez köthető rosszindulatú programot azonosítottak [90]. A Kaspersky Lab 2014 első negyedévében több mint 2500, mobilbankolási folyamatokat célzó egyedi rosszindulatú programot tartott nyilván Android platformon, amelyek közül több mint ezret ugyanebben az időszakban azonosítottak [91] [92]. Az iOS rendszer sem volt mentes a biztonsági incidensektől: Jonathan Zdziarski publikációja az iOS rendszerben található potenciális backdoor-okra és támadási pontokra hívta fel a figyelmet, amelyet követően az Apple egy frissítés során 55 CVE-bejegyzéssel azonosított sérülékenységet zárt le [93] [94].

A mobileszközök elleni támadások száma drasztikusan megemelkedett az elmúlt két évben. A Kaspersky adatai szerint 2023-ban közel 33,8 millió támadást regisztráltak mobileszközök ellen, ami 52%-os növekedés a 2022-es évhez képest. 2024-ben átlagosan havi 2,8 millió malware és adware támadás érte az okostelefonokat világszerte [95].

A Zimperium 2024-es jelentése szerint az adathalász oldalak 82%-a már kifejezetten mobileszközöket céloz meg (ez az ún. „mobile-first” stratégia) [96].

A fertőzések összetétele jól mutatja a támadók motivációit (pénzszerzés vs. adatgyűjtés):

- Adware (Reklámvírusok): Továbbra is ez a legelterjedtebb kategória, a fertőzések 40,8% – 57%-át teszi ki. Bár kevésbé tűnik veszélyesnek, gyakran kaput nyit komolyabb kártevőknek.
- Trojan-Banker (Banki trójaiak): Ez a leggyorsabban növekvő terület. 2024-ben a banki trójai támadások száma 196%-kal emelkedett. 2025-ös előrejelzések további 56%-os növekedést mutattak.
- Spyware (Kémszoftverek): A Lookout jelentése szerint a spyware fertőzések (mint az IdShark vagy a GgTrap) kritikus szintet értek el, különösen Androidon, ahol SMS-eket, névjegyzéket és pénzügyi adatokat továbbítanak harmadik félnek. [97] [98]

Érdekes esetek és specifikus kártevők

Triada (Android): Egy rendkívül komplex trójai, amely gyakran előre telepítve vagy népszerű alkalmazás-módosításokon (pl. WhatsApp modok) keresztül terjed. 2024 elején a trójai alapú támadások 35,7%-áért ez a család volt felelős [95].

FakeCalls (Android): Egy kifinomult banki trójai, amely képes több mint 20 pénzügyi appot utánozni. Különlegessége, hogy „hangalapú adathalászatot" (vishing) is végez: ha a felhasználó felhívja a bankját, a kártevő megszakítja a hívást és egy beépített hangfelvételt játszik be, mintha egy banki ügyintéző beszélne [98].

Pegasus és társai (iOS/Android): Míg az Androidot a tömeges támadások jellemzik, az iOS elleni támadások (pl. SparkKitty) gyakran célzottabbak és „nulladik napi" (zero-day) sebezhetőségeket használnak ki [96].

Frissítési hiányosságok: A mobileszközök körül-belül 31-33%-a elavult operációs rendszert futtat, ami kritikus biztonsági réseket hagy nyitva (pl. CVE-2023-7024 a WebRTC-ben). [96]

E példák azt mutatják, hogy a mobileszköz-platformok magas biztonsági kitettséggel rendelkeznek. A két domináns operációs rendszer, az Android és az iOS piaci koncentrációja kettős természetű: a centralizált fejlesztés és frissítési mechanizmus gyors reagálási lehetőséget biztosít, ugyanakkor a széles körű elterjedtség vonzó célponttá teszi a platformokat a támadók számára.

2.4.2 Fizikai és adatbiztonsági kockázatok

A szoftveres fenyegetések mellett kiemelten kezelendő a mobileszközök fizikai kitettsége is. A hordozhatóság – amely a mobileszközök egyik legfontosabb előnye – egyben jelentős kockázati tényező. Az eszköz elvesztése, ellopása vagy illetéktelen fizikai hozzáférése közvetlen adatbiztonsági veszélyt jelenthet, különösen akkor, ha az eszköz vállalati adatokat tárol vagy vállalati rendszerekhez biztosít hozzáférést.

Egy 2014-es, Londonban végzett felmérés szerint 300 taxisofőr évente átlagosan 8 mobiltelefont talált, ami a városban dolgozó mintegy 24 000 taxis esetében évente körülbelül 190 000 elhagyott mobiltelefont jelenthetett [99]. Bár az adat földrajzilag specifikus, a jelenség általános: a mobileszközök fizikai elvesztése gyakori és nehezen kontrollálható esemény.

A European Network and Information Security Agency, ENISA által meghatározott kockázati csoportosítás szerint az eszköz elvesztése az egyik legjelentősebb fenyegetési kategóriába

sorolható [34]. Amennyiben a mobileszköz vállalati hozzáférést biztosít, az elvesztés nemcsak adatvesztést, hanem jogosulatlan hozzáférést, identitás-visszaélést és reputációs kárt is okozhat.

Mark James rámutatott arra, hogy a felhasználók gyakran alábecsülik saját kitettségüket: a kiberbűnözés széles körű publicitása ellenére sokan nem tekintik magukat valós célpontnak [99]. Ez a percepciós torzítás különösen veszélyes a vállalati környezetben, ahol a mobileszközök a szervezeti hálózatokhoz vezető kapcsolódási pontként működnek.

2.4.3 Kommunikációs csatornák és metaadat-kitettség

A mobileszközök biztonsági sajátossága, hogy működésük során jelentős mennyiségű metaadatot generálnak és továbbítanak. A kommunikáció nem korlátozódik a klasszikus adatforgalomra: a készülékek földrajzi koordinátákat, hálózati kapcsolódási adatokat, mozgásparamétereket és egyéb környezeti információkat is kezelhetnek. A Bluetooth-, WiFi- és NFC-kapcsolatok további támadási felületet jelentenek, amelyek bizonyos körülmények között lehallgathatók vagy manipulálhatók.

A hangkommunikáció önmagában is érzékeny adatot hordozhat, így a kockázat nemcsak dokumentum- és fájlszinten, hanem kommunikációs metaadatok és beszédinformációk szintjén is megjelenik. A magas szintű titkosítás és hitelesítési eljárások alkalmazása önmagában nem garantál teljes védelmet, különösen akkor, ha a felhasználói viselkedés nem támogatja a biztonsági célokat.

2.4.4 A humán tényező, mint meghatározó biztonsági faktor

A mobileszközök technológiai fenyegetettsége mellett a humán tényező kiemelt jelentőségű. Parsons és munkatársai rámutattak arra, hogy a szervezet biztonsági szintje szoros kapcsolatban áll a szervezeti tagok biztonsághoz való hozzáállásával és attitűdjével [26]. A biztonsági irányelvek puszta ismerete önmagában nem elegendő; a biztonságtudatos attitűd kialakítása nélkül a technológiai védelem hatékonysága korlátozott marad.

A mobileszközök használata során a felhasználók gyakran a kényelmet és a gyorsaságot részesítik előnyben a biztonsággal szemben. A jelszóhasználat, a frissítések telepítése, a hálózati kapcsolatok megválasztása vagy a privát és üzleti használat elkülönítése mind olyan döntési helyzetek, amelyekben a felhasználói attitűd meghatározó. A biztonsági kultúra hiányosságait több hazai kutatás is hangsúlyozza [100] [21] és ezek a mobileszközök esetében különösen élesen jelentkeznek, mivel az eszközök a felhasználó személyes teréhez kötődnek.

A gyakran idézett megállapítás, miszerint „a rendszer leggyengébb láncszeme az ember” [21], a mobileszközök esetében fokozottan érvényes. A technológiai védelem szükséges, de nem elegendő: a felhasználói döntések, a kockázatészlelés és a kockázatvállalási hajlandóság közvetlenül befolyásolja a biztonsági szintet.

A mobileszközök biztonsági elemzése így rámutat arra, hogy a fenyegetettség többdimenziós jellegű: technológiai sérülékenységek, fizikai kitettség, metaadat-kezelés és humán tényezők egyaránt szerepet játszanak. A BYOD környezetben ezek a kockázatok összeadódnak és kölcsönhatásba lépnek egymással, ezért a szervezet számára nem elegendő az egyes fenyegetések izolált kezelése. Szükség van a kockázatok strukturált, elméletileg megalapozott értelmezésére.

A következő fejezetben ezért a kockázat fogalmának elméleti megalapozása és a BYOD-ban rejlő kockázatok rendszerezése kerül középpontba, különös tekintettel arra, hogy a kockázat miként értelmezhető szervezeti és egyéni döntési kontextusban.

2.5 BYOD-specifikus strukturális kockázati források

A Bring Your Own Device megoldások a szervezetek számára egyszerre jelentenek rugalmasságot és kockázatot, mivel a munkavállalók saját tulajdonú eszközeinek munkacélú használata a vállalati információs környezetet a szervezet közvetlen kontrollján kívül eső eszközökre és felhasználói gyakorlatokra is kiterjeszti. Ebben a működési modellben az információbiztonsági kockázat nem kizárólag technikai sérülékenységekből ered, hanem abból is, hogy a vállalati adatok és folyamatok a magánhasználat szférájával ugyanazon eszközön, gyakran azonos felhasználói rutinok mentén találkoznak. A kívánt biztonsági szint elérése ezért BYOD környezetben tipikusan nem oldható meg pusztán technológiai eszközökkel: szükség van szabályokra, kontrollmechanizmusokra és a felhasználói viselkedés tudatos alakítására is.

A vállalati adatok védelme a mobileszközök korában eleve új megközelítést kíván, és ennek központi eleme a személyes és vállalati adatok elkülöníthetősége. A mobileszközökön ez a szeparáció gyakran problémás, mert sem vállalati tulajdonú eszköz esetében nem garantálható, hogy ne jelenjenek meg rajta személyes adatok, sem saját tulajdonú eszköznél nem zárható ki, hogy vállalati adatok kerüljenek a magánszférába [14]. A BYOD ebből következően alapvetően a „határok” elmosódásának kockázatát hordozza: nehezebben kontrollálhatóvá válik a céges és privát adatok, a céges és privát alkalmazások, valamint a munkahelyi és a munkahelyen kívüli adatkezelési helyzetek közötti választóvonal [17] [101].

A BYOD elterjedésének gyakori szervezeti háttere, hogy egyes munkakörökben a folyamatos elérhetőség – akár 24/7 készenlét – implicit vagy explicit elvárás, ami a kommunikációs

csatornák és hozzáférések állandó fenntartását igényli. Ilyen helyzetben a kapcsolattartás költségének csökkentése és a kommunikáció egyszerűsítése könnyen a BYOD irányába terelheti a szervezetet, miközben a munkavállalók jellemzően nem szeretnek több eszközt magukkal vinni, és a számukra megszokott környezetet preferálják. Ennek része lehet az eszköztípushoz, az operációs rendszerhez és az alkalmazáskészlethez való ragaszkodás, szélsőséges esetben akár konkrét eszközpreferencia is [80] [81]. Biztonsági nézőpontból ez azért válik jelentős kockázati tényezővé, mert az eszköz standardizáció lehetősége beszűkül: eltérő eszközök, operációsrendszer-verziók, beállítások és alkalmazás-ökoszisztémák heterogén végponti környezetet hoznak létre, ahol a kontrollok következetes érvényesítése nehezebb. Így a költség- és kényelmi szempontokból érkező nyomás könnyen a biztonsági szint csökkenéséhez vezethet, különösen akkor, ha a szervezet nem alakít ki működtethető és ténylegesen betartható BYOD-keretrendszert.

A BYOD kockázati profilját meghatározó további alapvető tényező a tulajdonjog és az ebből következő kontroll. Vállalati tulajdonú eszközök esetében a szervezet – szükség esetén – jóval szélesebb kontrollt tud gyakorolni: az IKT/IT részleg menedzselheti a konfigurációt, frissítéseket, jogosultságokat, és elvileg kikényszerítheti a szabályszerű használatot. Ugyanakkor a magánjellegű használat teljes tiltása ellenállást válthat ki, szélsőséges esetben akár a munkavállaló kilépéséhez is vezethet, vagyis a túl szigorú megközelítés önmagában nem garantálja a kockázat csökkenését. Saját tulajdonú eszközök vállalati célú használata ezzel szemben gyakran együtt járhat magasabb produktivitással és felhasználói elégedettséggel, kockázati értelemben azonban kontrollvesztést hordoz: ha nincs megfelelően kialakított és ténylegesen betartott szabályzat, a munkavállaló akár tiltás ellenére is képes vállalati adatokat saját környezetébe továbbítani. A gyakorlatban az egyik legtipikusabb fegyelmezetlenség a vállalati levelek és mellékleteik automatikus továbbítása privát postafiókba, ami az adatkezelés kontrollálhatóságát és nyomonkövethetőségét jelentősen rontja [78] [79] [82]. Ebből következően a BYOD kezelése nem pusztán technológiai, hanem kormányzási kérdés is: a szervezetnek azt kell tisztáznia, milyen jogosultsági és hozzáférési rend mellett, milyen feltételekkel engedhető meg, hogy vállalati információk magáneszközön megjelenjenek.

A kockázatok harmadik, rendszeresen visszatérő forrása a felhasználói viselkedés, amelyben a kényelmi szempontok gyakran felülírják a biztonsági megfontolásokat. A biztonsági előírások sok esetben több lépést, több figyelmet és nagyobb adminisztratív terhet jelentenek, ami megkerülő magatartáshoz vezethet. Ide illeszkedik az a tapasztalat is, hogy a hosszú jelszavak erőltetése vagy azok öncélú, kiegészítő okok nélküli rendszeres cseréje kontraproduktív lehet, és

önmagában nem feltétlenül növeli a biztonsági szintet [102]. Hasonlóképp növelheti a kezelési terhet a hardveres biztonsági kulcsok alkalmazása, míg a biometrikus azonosítás – ujjlenyomat, írisz- vagy arcazonosítás – technikai és jogi kérdéseket vethet fel, különösen akkor, ha a szervezetnek korlátozott ráhatása van a beállításokra és a biometrikus adatok kezelésének körülményeire [16] [103] [104]. A kockázati képhez hozzátartozhat az is, hogy kiemelt pozícióban lévő, IT-közeli munkavállalók szükségtelenül széles jogosultságokat szerezhetnek; BYOD környezetben ez különösen problémás, mert a magas jogosultságú hozzáférések magáneszközön is megjelenhetnek, ami a potenciális kár mértékét növeli [16].

A BYOD gyakorlata a szervezeteknél különböző szabályozottsági szinteken jelenik meg, és ez a heterogenitás önmagában kockázati tényező. Bár a magáneszközök munkahelyi használata más területeken sem ismeretlen (például saját gépkocsi), ott sokszor kiforrott a költségtérítési, biztosítási és adózási szabályozás, míg BYOD esetén a gyakorlat jóval széttartóbb. Előfordulhat, hogy a BYOD csupán „megtűrt” gyakorlat formális szabályozás nélkül, ami különösen kritikus helyzetet teremt, mert nincs írott rend, kontroll és felelősségi struktúra, így a vállalati adatok könnyen kikerülhetnek a kontrollált környezetből [86] [105]. Más esetekben a használat eseti, szóbeli engedélyhez kötött, ami ugyan rugalmas, de a szabályok transzparenciája, auditálhatósága és következetessége korlátozott lehet [105]. Kiforrottabb modellben írott szabályzat is létezhet részletes információbiztonsági elemekkel, amely például csatlakozási protokollokat, használható eszköz- és alkalmazáslistát, elfogadott operációs rendszert és verziókat, kötelező biztonsági szoftvereket, a mobilról engedett tranzakciók körét, naplózási rendet, valamint a privát és céges adatok szétválasztásának szabályait rögzíti [16] [70]. Előfordulhat az is, hogy a szervezet aktívan ösztönzi a BYOD-t, ami növelheti a produktivitást és csökkentheti bizonyos költségeket, de csak akkor tartható fenn elfogadható kockázati szint mellett, ha a szabályozási és technológiai kontrollok erősek [70] [105]. Mindezek mellett BYOD-ban külön kezelendő a magánélet és az eredményességi elvárások konfliktusa is: a magánélet teljes kizárása reálisan nem megoldható, ugyanakkor arányos korlátozás felmerülhet, miközben Magyarországon a magánéletet a munkáltató nem ellenőrizheti, de a munkakörhöz méltó magatartás munkaidőn kívül is elvárható [105] [106]. A fenti képlet lényege, hogy a BYOD-kockázat számottevő része szabályozottsági szint kérdése: ugyanaz a technológia eltérő szabályozási és kontrollkörnyezetben egészen más kockázati eredőt ad.

A BYOD nemcsak elvi kockázatokat jelent, hanem operatív döntési pontok sorát is, amelyeknél a bizonytalanság és a kontrollhatárok a mindennapi működésben jelennek meg. Ilyen kérdés például, hogy milyen biztonságú hálózatról történhet csatlakozás, hová és hogyan kerülnek a

mentések a munkavállaló eszközén, vagy azon kívül hálózaton keresztül, szükséges-e időbeli korlátozás a vállalati erőforrások elérésében, hány sikertelen bejelentkezés után blokkol a rendszer, kizárható-e eszköz vagy felhasználó, milyen autentikációs logika ad arányos védelmet, elérhet-e a felhasználó több postafiókot vagy megosztott erőforrást és milyen feltételekkel, illetve engedélyezhető-e adathordozók és perifériák használata és az adatok mozgatása a vállalati erőforrások irányába [105] [107] [108]. Ezek a pontok jellemzően a BYOD-kockázatok gyakorlati „magját" adják, mert incidensek és szabálysértések sokszor ott keletkeznek, ahol a szabály nem egyértelmű, nem betartható, vagy a kontroll a felhasználói kényelmi logikával ütközik.

Elméleti sűrítésben a BYOD-kockázatok kulcsforrásai néhány, egymással összefüggő mechanizmusra vezethetők vissza. Ilyen a vállalati adatok feletti ellenőrzés részleges elvesztése, mert az adatok engedély vagy kellő gondosság nélkül átkerülhetnek magáneszközre vagy magáncsatornákra; az eszközök heterogenitása és korlátozott menedzselhetősége, amely növeli a sérülékenységi varianciát; a „biztonság túl kényelmetlen" jelensége, amely megkerülő megoldásokat ösztönöz; és végül a szabályozatlan vagy nem betartott BYOD-használat, amely értékes információk kontrollálatlan szivárgásához vezethet. Ezek a kockázatok szorosan kapcsolódnak a ShadowIT jelenségéhez is, mert ha a szervezet tilt, de nem kínál működő alternatívát, vagy ha a szabályok betarthatatlanok, a munkavállalók informális megoldásokat alakíthatnak ki. A ShadowIT (StealthIT, ClientIT) olyan szervezeten belül használt IT-megoldásokat jelent, amelyek kifejezett szervezeti jóváhagyás nélkül kerülnek bevezetésre vagy használatra [109] [110] [111] [112]. A BYOD és a ShadowIT ezért gyakran ugyanannak a szervezeti problémának két oldalát jelenti: az üzleti igények és a formális IT-szabályozás közötti rés kitöltését. A jelenség megítélése ugyanakkor nem kizárólag negatív, mivel több IT szakértő a felhasználói kezdeményezéseket és a ShadowIT-t az innováció és a problémamegoldás forrásaként is értelmezi, mert a felhasználók gyakran hatékonyabb folyamatmegoldásokat alakítanak ki [113]. Biztonsági szempontból viszont ezek a megoldások sokszor nem felelnek meg a kontroll, dokumentáció, megbízhatóság és információbiztonság alapkövetelményeinek, ezért a tiltás önmagában ritkán elégséges; a keretrendszer és a betartható szabályozás viszont alkalmas lehet a kockázatok csökkentésére.

A BYOD kockázati értelmezése illeszthető az ENISA nézőpontjához is, amely szerint az okostelefonokat fenyegető legnagyobb kockázatok három csoportba sorolhatók: az adatok kiszivárgása eszközvesztés vagy lopás miatt, az adatok akaratlan közzététele, valamint a nem megfelelően kezelt eszközök támadása és az ezekből történő adatszerzés [34]. BYOD-ban e kockázatok

súlya növekszik, mert az eszköz nemcsak privát célra szolgál, hanem üzleti hozzáférési pontként is működik, így a következmények nem kizárólag egyéniek, hanem szervezeti szinten is jelentkezhetnek. Az ENISA ráadásul széles körű „értékkört” azonosít, amelyet a kockázatok érinthetnek: személyes adatok, vállalati szellemi tulajdon, minősített információk, pénzügyi eszközök, eszközök és szolgáltatások működőképessége, valamint akár személyes és politikai hírnév is [34]. Ez a szemlélet összhangban áll azzal, hogy BYOD-ban a kockázat lényege az: sokféle érték forog kockán, miközben a kimenetel a technológiai, szervezeti és humán tényezők együttállása miatt bizonytalan.

2.6 Támadási mintázatok BYOD-környezetben

Az okostelefonok és mobil operációs rendszerek elterjedésével párhuzamosan a támadási felület is számottevően növekedett. Közel másfél évtizeddel az első iPhone és Android-alapú eszközök megjelenése után [114] a mobileszközök a mindennapi kommunikáció és információkezelés elsődleges platformjaivá váltak: a klasszikus hanghívások és SMS-ek szerepe csökkent, miközben az alkalmazásokon keresztüli adatmegosztás és információfogyasztás vált dominánssá [115] [116]. Ezzel együtt az is általánosabbá lett, hogy a felhasználók érzékeny személyes és vállalati adatokat harmadik fél által fejlesztett alkalmazásokra bíznak, sokszor a kockázatok tudatos mérlegelése nélkül [117]. A következő esetek azt szemléltetik, hogy BYOD-környezetben a kockázatok több, egymást erősítő forrásból eredhetnek: megjelenhetnek már az eszköz beszerzési és gyártói láncában, fakadhatnak alkalmazás-szintű megoldásokból, a felhasználói döntésekből, illetve ismert sérülékenységek kihasználásából.

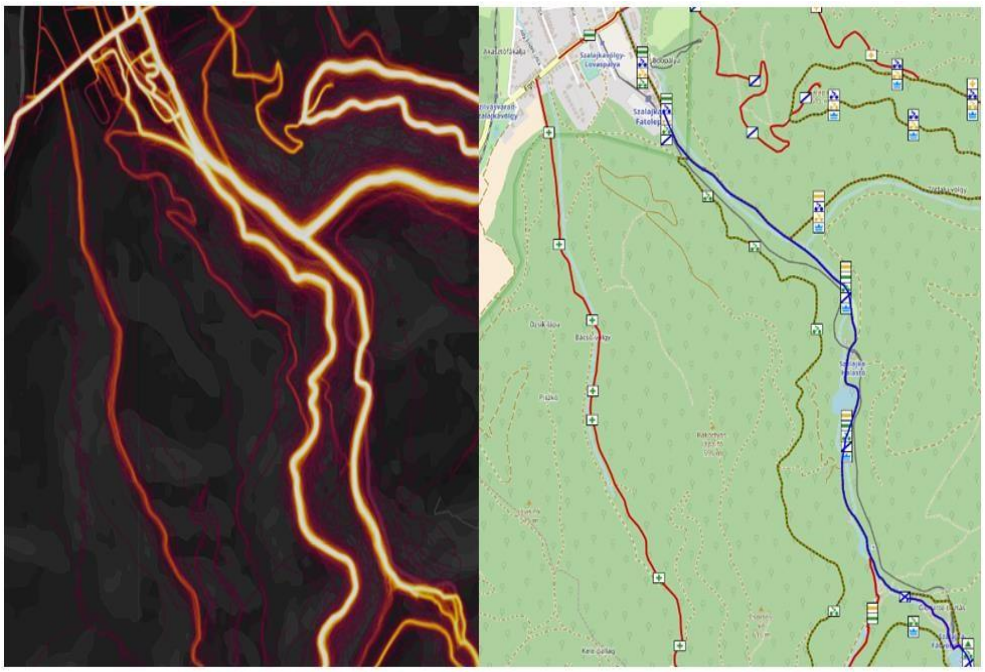
Az első kockázati mintázat az előre telepített rosszindulatú programok kérdéséhez kapcsolódik. Amikor a felhasználó új okoseszközt vesz át – akár kereskedelmi forrásból, akár munkahelyi eszközként –, az eszköz már egy előtelepített operációs rendszerrel, valamint a gyártó, a szolgáltató és esetenként harmadik felek alkalmazásaival érkezik, és a felhasználó jellemzően implicit módon megbízik ebben a környezetben. A gyakorlat ugyanakkor azt mutatja, hogy a kompromittáltság már az átadás pillanatában jelen lehet: 2017-ben a Check Point kutatói [118] 36 olyan telefontípust azonosítottak, amelyeknél az előre telepített szoftvercsomag rosszindulatú programot tartalmazott, 2018 elején pedig a Dr. Web [119] 40 telefontípust jelölt meg, amelyekre az Android.Triada.231 malware már előtelepítés során felkerült, és banki adatok lehallgatására, illetve tranzakciók manipulálására is képes volt [119] [120] [121] [122]. BYOD szempontból ennek az a tanulsága, hogy a kockázat nem kizárólag a felhasználói magatartásból fakad: a szervezet BYOD esetén tipikusan nem ismeri és nem ellenőrzi az eszköz eredetét,

előtelepített szoftverkörnyezetét és integritását, vagyis a kockázat már a hálózatra csatlakozás pillanatában „készen” lehet.

A második mintázat a felhasználó által telepített alkalmazásokhoz és az azokkal összefüggő túlzott jogosultságokhoz köthető. A mobilalkalmazások gyakran kérnek hozzáférést a készülék különböző funkcióihoz – például a kamerához, mikrofonhoz, helyadatokhoz vagy a képernyő bizonyos elemeihez –, miközben a jogosultságok elfogadása sokszor rutinszerűen, a következmények mérlegelése nélkül történik. 2017-ben nyilvánosságra került [123], hogy az Uber iOS-alkalmazása egy olyan interfészen keresztül hozzáférést kaphatott a képernyőrögzítési funkcióhoz, amely potenciálisan lehetővé tehette a kijelzőn megjelenő információk megfigyelését, akkor is, amikor az alkalmazás futott, de más applikációk voltak előtérben ; bár a vállalat szerint tesztverzióról volt szó és konkrét visszaélés nem ismert, a lehetőség elvileg érzékeny adatok (például jelszavak vagy banki információk) kitettségével járt [118] [124] [125]. Hasonló logika mentén az évek során számos ransomware és kémprogram jellegű alkalmazás is megjelent, amelyek a felhasználó engedélyével vagy megtévesztéssel települve hozzáfértek az eszköz erőforrásaihoz [126] [127] [128]. BYOD környezetben ez azért kritikus, mert a szervezet sokszor nem képes teljeskörűen kontrollálni, milyen alkalmazások kerülnek az eszközre, így a sérülékenység a privát használat csatornáján keresztül hatolhat be a vállalati információs térbe.

A harmadik esetkör azt mutatja meg, hogy az adatszivárgás nem feltétlenül rosszindulatú támadás következménye: gyakran a felhasználó beleegyezésével, az adatmegosztási beállítások és a metaadatok következményeinek alulértékelésével történik.

Egy navigációs vagy fitneszalkalmazás esetén a helyadatok használata funkcionálisan indokolható, de a felhasználó sokszor nincs tisztában azzal, hogy a továbbított adatok szolgáltatói felhasználása következményekhez vezethetnek. 2018-ban a Strava fitneszalkalmazás egy hőtérképhez hasonló használati gyakorisági térképet publikált több milliárd GPS-koordináta alapján, ezzel láthatóvá téve felhasználói mozgási mintázatokat.



1. ábra Strava applikáció felhasználói adatok vizualizációja (bal oldalt)
és ugyanazon hely turista térképen (jobb oldalt).
Forrás: Saját szerkesztés a Strava térképének és a turistautak.openstreetmap.hu felhasználásával

Nathan Ruser elemzése rámutatott, hogy ezen, nyilvánosan elérhető adatok alapján, katonai bázisok környékén is kirajzolódtak a mozgási szokások [129] [130].

2. ábra Strava által rögzített felhasználói mozgás GPS adatpontok alapján készített vizualizációja egy ismert amerikai előretolt bázis környékéről a Közel-Keleten.
Forrás: Nathan Ruser Twitter bejegyzése a Strava térképének részletével

Hasonlóan kiemelt érdeklődésre okot adó eset volt 2014-ben, amikor egy orosz katona Instagram-fotója a geotag információ révén felfedte a kép készítésének pontos helyét [131].

BYOD szempontból ezen incidensekben is jól látszik, hogy a vállalati és privát adatok, illetve a metaadatok összefonódása miatt a kockázat gyakran közvetett, és a szervezeti kontroll számára nehezen megragadható és időben is késleltetett lehet.

A negyedik mintázat az ismert sérülékenységek és azok kihasználását bemutató ismert exploitok problémája. Az operációs rendszerek és alkalmazások természetüknél fogva tartalmazhatnak hibákat, és az okoseszközök operációs rendszeréből, illetve szoftver környezetéből több sérülékenység vált ismertté az évek során, különösen a régebbi verziókban [132]. A 2011–2015 közötti időszakban számos széles körben ismert exploit jelent meg – például a RageAgainstTheCage, a TacoRoot vagy a Stagefright –, amelyek jogosultság kiterjesztést, vagy távoli kódfuttatást tettek lehetővé [133] [134]. Bár e hibák jelentős része később javításra került, a frissítések hiánya vagy késlekedése miatt eszközök hosszabb ideig sebezhető állapotban maradhattak, s a probléma későbbi sérülékenységek és exploitok miatt fennáll és fenn is fog állni. BYOD alkalmazása esetén mindez azért különösen nagy kihívásokkal jár, mert a heterogén, eltérő verziószámú és eltérő frissítési állapotú végpontok megnövelik a sérülékenységi varianciát, és a szervezet nem feltétlenül képes garantálni a biztonságos minimumszintet minden csatlakozó eszközön.

Az ismertetett esetek összességében négy strukturális kockázati mintázatot rajzolnak ki:

- megjelenik az ellátási lánc eredetű kockázat az előre telepített malware formájában,
- a felhasználói döntésekből fakadó kitettség
    - az alkalmazás-telepítések és
    - jogosultságadások révén, a metaadat- és kontextusalapú kockázat a beleegyezéses adatmegosztás következményein keresztül, valamint
- a szoftversérülékenységi kockázat az ismert, de nem (időben) javított hibák miatt.

Ezek a mintázatok jól illeszkednek a korábban tárgyalt BYOD-kockázati forrásokhoz is: a kontrollvesztéshez, a heterogenitáshoz, a kényelmi motivációkhoz és a szabályozottság hiányához. Az esetek így azt támasztják alá, hogy a BYOD nem elszigetelt technológiai jelenség, hanem komplex kockázati tér, ahol technológiai, szervezeti és humán tényezők kölcsönhatásban alakítják a biztonsági eredőt.

2.7 A BYOD-kockázatok típusai és szerkezete

A BYOD-jelenségből eredő kockázatok akkor kezelhetők hatékonyan, ha átlátható, egymásra épülő rendszerbe rendezzük őket. A korábbi fejezetek alapján a kockázatok nem szűkíthetők

technológiai kérdésre: szervezeti működéshez és felhasználói magatartáshoz kötődő tényezők ugyanúgy alakítják a kitettséget. A fejezet célja ezért olyan rendszerezési logika kialakítása, amely később döntéstámogatási modellben is alkalmazható, vagyis egyszerre teszi értelmezhetővé a kockázatok természetét, és megnyitja a lehetőséget a priorizálásukra.

2.7.1 Információbiztonsági alapmodell: a CIA-triád alkalmazása BYOD-ban

Az információbiztonság klasszikus megközelítése a bizalmasság, a sértetlenség és a rendelkezésre állás hármasa mentén írható le [135]. A bizalmasság azt jelenti, hogy az információhoz csak a jogosult személyek férhetnek hozzá, a sértetlenség az információ teljességének és pontosságának megőrzését jelenti, míg a rendelkezésre állás azt, hogy az információ a jogosult felhasználók számára ténylegesen elérhető [135]. BYOD-környezetben mindhárom dimenzió sérülhet, csak eltérő módon: a bizalmasság tipikusan adatvesztés, adatszivárgás vagy lehallgatás révén, a sértetlenség rosszindulatú szoftverek vagy jogosulatlan módosítás következtében, a rendelkezésre állás pedig akár szolgáltatásmegtagadás, akár eszközblokkolás miatt.

A kockázatok kezeléséhez a dolgozat a kockázatkezelési logikát az ISO 31000 keretében értelmezi, amely több alapvető stratégiát különböztet meg: a bekövetkezési valószínűség csökkentését, a potenciális kár mérséklését, a kockázat átruházását (például kiszervezés útján), illetve a kockázat megosztását (például biztosítással) [136]. Ez a keret nemcsak definíciós hátteret ad, hanem azt is megmutatja, hogy ugyanazt a BYOD-kitettséget többféle szervezeti döntési irányból lehet kezelni.

2.7.2 A BYOD-kockázatok fő dimenziói

A szakirodalom alapján a BYOD-kockázatok többféle módon osztályozhatók, de a közös tanulság, hogy a kitettség egyszerre fakad az eszközök technikai állapotából, az adatkezelés és kommunikáció sajátosságaiból, a felhasználói magatartásból, valamint a szervezeti kontroll kereteiből [17] [137] [83]. Ennek megfelelően a dolgozat egy négydimenziós felosztást alkalmaz: technológiai kockázatokat, adat- és kommunikációs kockázatokat, humán és viselkedési kockázatokat, valamint szervezeti és infrastrukturális kockázatokat különít el. A bontás célja nem pusztán leíró jellegű: azért előnyös, mert alkalmas a későbbi modellalkotásra, ahol a dimenziók egymásra hatása és relatív súlya is értelmezhetővé válik.

2.7.3 Technológiai kockázatok

Technológiai kockázatként értelmezhető minden olyan fenyegetettség, amely az eszköz hardveréből, szoftveréből, illetve ezek manipulációjából származik. E körbe tartozik a készülék jogosulatlan módosítása, például rootolás vagy jailbreak (K1), továbbá a rosszindulatú szoftverek

megjelenése – ideértve a vírusokat, trójai programokat, zsarolóprogramokat és kémprogramokat (K3) –, valamint a szoftveres sérülékenységek kérdése, mint az elmaradt frissítések, megbízhatatlan forrásból telepített alkalmazások vagy firmware-hibák (K5). Ezek a kockázatok elsődlegesen a sértetlenséget és a bizalmasságot fenyegetik, de közvetett módon a rendelkezésre állásra is kihatással lehetnek. BYOD esetében e kitettségek súlyát növeli az eszközpark heterogenitása és az a tény, hogy a szervezet kontrollja a frissítési fegyelem és a konfiguráció egységesítése felett gyakran korlátozott.

2.7.4 Adat- és kommunikációs kockázatok

Az adat- és kommunikációs kockázatok közé azok a fenyegetések tartoznak, amelyek a hálózati kapcsolódás, az adatátvitel, valamint a metaadatok keletkezése és kezelése során jelennek meg. A hangkommunikáció lehallgatása (K2) akkor válik relevánssá, ha érzékeny beszélgetések kompromittálódhatnak, míg az adatátviteli kockázatok (K6) tipikusan a man-in-the-middle jellegű támadásokhoz, a nyilvános WiFi használatához vagy a titkosítatlan adatforgalomhoz kapcsolódnak. Ehhez szorosan illeszkedik az adatszivárgás és a metaadat-kitettség problémája is, amelyben helyadatok, GPS-információk vagy akár felhőszinkronizációs mechanizmusok révén válhatnak érzékeny mintázatok és tartalmak hozzáférhetővé. E dimenzió elsősorban a bizalmasságot érinti, ugyanakkor BYOD környezetben a privát és vállalati adatforgalom keveredése a határok elmosódása miatt tovább nehezíti a kontrollt és a nyomon követhetőséget.

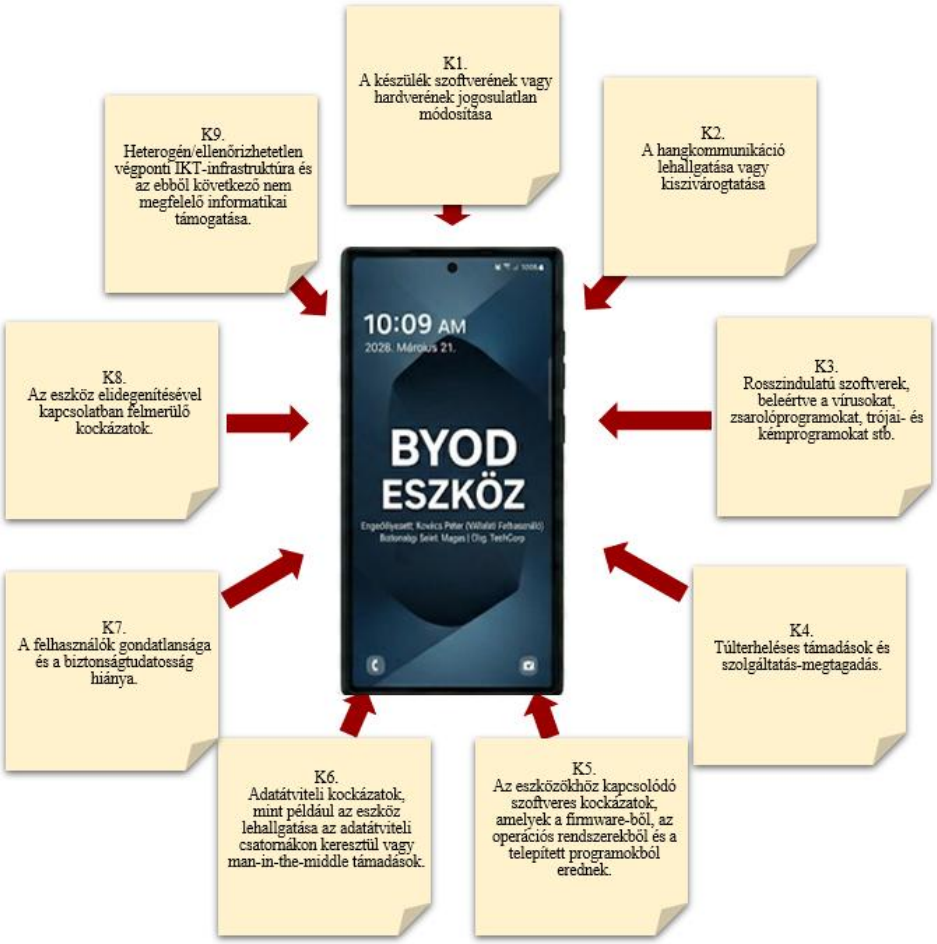
2.7.5 Humán és viselkedési kockázatok

A humán dimenzió a BYOD egyik meghatározó területe, mert a technológiai kontrollok korlátozottan képesek kompenzálni a tudatos vagy tudattalan kockázatvállalást. Ide sorolható a felhasználói gondatlanság (K7), amelynek tipikus megnyilvánulása az eszköz elvesztése, a jelszókezelési hiányosságok, vagy az, hogy a felhasználó social engineering áldozatává válik [138]. A kockázatot erősítik a kényelmi motivációk is: a gyenge jelszavak, az automatikus e-mail továbbítás, illetve a jogosultságok indokolatlan kiterjesztése olyan mintázatok, amelyek a mindennapi rutinok szintjén termelnek sérülékenységet. BYOD esetében a humán tényező különösen hangsúlyos, mert a felhasználó a saját eszközét jellemzően „személyes térként” kezeli, és a biztonsági elvárásokat könnyen a használhatóság rovására megélt korlátozásnak érzékelheti.

2.7.6 Szervezeti és infrastruktúrális kockázatok

A szervezeti és infrastrukturális kockázatok a szabályozás, a kontroll és az IT-támogatás hiányosságaihoz, illetve a BYOD által felerősített heterogenitáshoz kötődnek. Ide tartozik például az eszköz elidegenítésének kezelése (K8), amikor az adatok nem megfelelő törlése vagy a jogosultságok visszavonásának hiánya marad kockázati tényező, illetve a heterogén végponti

infrastruktúra (K9), amely eltérő operációs rendszerek, verziók és inkompatibilis biztonsági megoldások miatt növeli a sérülékenységi varianciát. Ebben a dimenzióban értelmezhető a ShadowIT jelensége is, vagyis a nem engedélyezett rendszerek és alkalmazások szervezeten belüli használata [109] [110] [111] [112]. A ShadowIT azért különösen ambivalens, mert bizonyos értelmezésekben innovációs és problémamegoldási potenciált is hordozhat [113], ugyanakkor információbiztonsági szempontból gyakran éppen a dokumentáltság, a kontroll és a megbízhatóság hiánya miatt válik kockázati tényezővé. BYOD környezetben a két jelenség sokszor összefonódik: a privát eszköz használata és az informális megoldások könnyen egy közös „árnyéktérben” jelennek meg.



3. ábra BYOD kockázatok csoportosítása

Forrás: saját szerkesztés az irodalomkutatás alapján

2.7.7 ENISA kockázati prioritások

Az ENISA, The European Union Agency for Cybersecurity (Európai Uniós Hálózat- és Információbiztonsági Ügynökség) [34] okostelefonokra vonatkozó kockázati nézőpontja három fő prioritást emel ki: az adatszivárgást eszközvesztés vagy lopás miatt, az akaratlan

adatközzétételt, valamint a nem megfelelően kezelt eszközök kompromittálását. E kockázatok közvetlenül érinthetnek személyes adatokat, vállalati szellemi tulajdont, minősített információkat, pénzügyi eszközöket, a szolgáltatások rendelkezésre állását és a reputációt. Mindez azt támasztja alá, hogy BYOD esetében a kockázat nem csupán IT-operatív probléma, hanem stratégiai és bizalmi dimenzióval is rendelkezik.

A fenti csoportosítás alapján a BYOD-kockázatok több dimenziósak, egymással kölcsönhatásban állnak, és nem értelmezhetők kizárólag technológiai jelenségként. A javasolt négydimenziós struktúra – technológiai, adat- és kommunikációs, humán és viselkedési, valamint szervezeti és infrastrukturális – alkalmas arra, hogy a későbbi stratégiai alapmodellekhez kiindulópontot adjon, támogassa a döntéshozót a kockázatok priorizálásában, és összekapcsolható legyen az empirikus eredményekkel, különösen a humán dimenzió mentén.

2.8 BYOD-stratégiai modellek és szervezeti válaszok

A saját tulajdonú mobileszközök szervezeti célú alkalmazása a modern információbiztonsági kihívások egyik tipikus példája, mivel egyszerre kapcsolódik technológiai, jogi, szervezeti és humán tényezőkhöz. A BYOD nem pusztán eszközhasználati kérdés: a vállalati adatokhoz való hozzáférés, az adatok továbbítása, tárolása és feldolgozása olyan kontrolligényt teremt, amely a hagyományos, vállalati tulajdonú IT-eszközökhöz képest lényegesen bonyolultabb. A 2. fejezetben bemutatott kockázati tényezők alapján jól látható, hogy a BYOD esetén a kockázatok nem kizárólag a technikai sebezhetőségekből fakadnak, hanem a szabályozottság hiányából, a magán- és üzleti adatok keveredéséből, valamint a felhasználói magatartásból is.

A BYOD elterjedését részben a munkavállalói igények – kényelem, gyors hozzáférés, ismert felhasználói környezet – részben pedig a szervezeti költség- és hatékonysági szempontok támogatják. Ugyanakkor a BYOD gyakorlata akkor válik szervezeti szempontból fenntarthatóvá, ha a vállalat képes egyszerre kezelni a vállalati adatvédelem és a munkavállalói magánszféra védelmének követelményeit. E kettős cél eléréséhez világos stratégiai döntésre, megfelelő szabályozásra, valamint a végrehajtást támogató technológiai megoldásokra (például MDM rendszerekre) van szükség [16] [17] [2] [5].

2.8.1 A BYOD jogi szabályozása

A BYOD jogi szabályozásával kapcsolatban elsőként megállapítható, hogy nincs önálló, kizárólag a saját tulajdonú mobileszközök munkavégzési célú használatára létrehozott jogszabályi keret. A BYOD-hoz kapcsolódó helyzeteket több, általános hatályú szabályozás együttes alkalmazásával lehet értelmezni és kezelni: ilyenek többek között a Munka Törvénykönyve, az

adatvédelmi szabályozás, illetve egyes esetekben a Büntető Törvénykönyv releváns rendelkezései [22].

A 2012. évi I. törvény a munka törvénykönyvéről alapján (VIII. fejezet 51. §) [139] a munkáltató kötelessége a munkavégzéshez szükséges eszközök biztosítása. Ugyanakkor a jog lehetőséget ad arra, hogy a felek külön megállapodással ettől eltérjenek, ami megteremti a BYOD jogalapját is. A BYOD gyakorlatának egyik kulcsfogalma az adott helyzetben általánosan elvárható magatartás elve: a munkavállaló akkor jár el megfelelően, ha a saját eszköz munkacélú használata szervezeti megállapodáson alapul, és összhangban áll a vonatkozó belső szabályozással.

A BYOD-hoz kapcsolódó jogi kockázatok súlyát mutatja, hogy a gyakorlatban sok esetben nem történik meg a szükséges formális rendezés. Egy nemzetközi felmérés szerint a válaszadók jelentős része úgy használta saját eszközét munkavégzésre, hogy a munkáltató vagy nem tudott erről, vagy nem létezett vonatkozó szabályzat, vagy ha létezett is, azt nem írták alá [140]. E helyzet munkáltatói oldalon olyan mulasztásokhoz vezethet, amelyek felelősségi kérdéseket vethetnek fel egy későbbi incidensnél.

A munkaviszony megszűnésekor, eszközcsere esetén vagy biztonsági esemény bekövetkeztekor különösen élesen jelenik meg a jogi dilemma: a munkáltató vállalati adatokhoz kapcsolódó védelmi kötelezettsége és a munkavállaló magánszférájának védelme könnyen konfliktusba kerül. Ha nincs külön megállapodás, a munkáltató vagy úgy próbál ellenőrzést gyakorolni, hogy közben érintheti a munkavállaló személyes adatait, vagy pedig nem ellenőrzi az eszközt, így a vállalati adatvédelem sérülhet. E kockázatot erősíti, hogy a mobileszközök elvesztése vagy ellopása a legjelentősebb kockázati tényezők közé tartozik, különösen akkor, ha a készüléken üzleti adatok is jelen vannak [34].

A BYOD helyzet tehát jogi szempontból akkor kezelhető stabilan, ha a felek között létezik dokumentált és elfogadott megállapodás, és a szervezet képes a vállalati adatok védelmét úgy biztosítani, hogy közben a munkavállaló személyes adatainak védelme is teljesüljön.

2.8.2 BYOD stratégiák

Az elméleti bevezetés és az esettanulmányok tanulságai alapján megállapítható, hogy a szervezeteknek tudatosan kell tervezniük a mobileszközökön megjelenő adatok körét, az adatok elérésének feltételeit, valamint az alkalmazott védelmi megoldásokat [6]. A védekezés már az eszközválasztásnál elkezdődik: olyan gyártói ökoszisztéma preferálása indokolt, amely a tervezett élettartam alatt biztosítja a biztonsági frissítések elérhetőségét. Emellett az eszköz

konfigurálásában is az adatbiztonsági szempontokat kell előtérbe helyezni, ideértve a megbízható forrásból történő alkalmazástelepítést és a jogosultságok minimalizálását.

A bizalmas vállalati adatok védelme a BYOD esetén új biztonságpolitikai megközelítést igényel. A magán- és üzleti használat szétválasztása elvi szinten alapvető fontosságú, ugyanakkor a napi gyakorlatban nehezen várható el, hogy a munkavállaló folyamatosan nála lévő eszközét ne használja magáncélra, különösen akkor, ha az eszköz az ő tulajdonában van, vagy az előfizetést részben/egészben ő finanszírozza [16] [17].

A BYOD védelmi tevékenység ezért két irányban válik szét. Egyrészt szükséges egy írásos, követhető, a szervezeti működéshez illeszkedő eljárásrend kialakítása, amely szabályozza a bizalmas vállalati adatok kezelését és kommunikációját. Másrészt szükség van technológiai védelemre, amely a mobileszközökön és a hozzáférési folyamatokban képes kontrollt biztosítani [2] [5] [141].

A szervezeti gyakorlatok több szinten különbözhetnek. A BYOD kezelésében tipikusan megjelennek a tiltó, eltűrő, eseti engedélyező, formálisan szabályozó, illetve aktívan támogató stratégiák. A szabályozási érettség alacsonyabb szintjein gyakori, hogy a BYOD „megtűrt" jelenségként működik, miközben hiányzik az írásos keretrendszer [103] [104]. A magasabb szinteken már részletes előírások jelennek meg: meghatározhatók a csatlakozási protokollok, az elfogadott eszköz- és operációsrendszer-típusok, a kötelező biztonsági szoftverek, a megengedett tranzakciók köre, valamint a naplózás és a szétválasztás technikai rendje [83] [70]. Egyes szervezetek a BYOD-t kifejezetten támogatják és ösztönzik is [142].

2.8.3 BYOD stratégia kialakítása

A BYOD-stratégia felé tett első lépés a vezetői szintű stratégiai döntés. A szervezetnek ki kell jelölnie azt az alapállást, amely mentén a BYOD-t tiltja, tűri vagy szabályozottan támogatja. E döntést érdemben csak a BYOD-hoz kapcsolódó kockázatok előzetes felmérése és strukturált értékelése támaszthatja alá.

A stratégiai döntés megalapozására a korábban bemutatott kockázati csoportok (2.7 fejezet) alkalmazhatók oly módon, hogy a szervezet előszűri azokat a stratégiai alternatívákat, amelyek valamely kockázati területen elfogadhatatlan vagy kezelhetetlen kockázat szintet generálnak. A kockázati csoportok súlyozásával és értékelésével a döntési helyzet átláthatóbbá válik, és lehetővé válik egy összesített kockázati szint megállapítása. Ennek támogatására javasolt több szempontú módszer (például Combinex) alkalmazása, ahol a súlyok összege 100% (vagy 1,00), és minden alternatívát azonos skálán szükséges értékelni [143].

Amennyiben a döntés a tolerált vagy támogatott BYOD irányába mutat, megkezdődhet a BYOD-irányelv tényleges kidolgozása és integrálása a mobileszköz-kezelési megoldásba. Itt kulcskérdés, hogy ne alakuljon ki ellenőrizetlen adatáramlás a vállalati és a személyes eszközök között, mert ez egyszerre vezethet adatvédelmi és üzleti titokvédelmi problémákhoz. A munkáltató nem kötelezheti a munkavállalót személyes mobileszköz vállalati célú használatára, így a stratégia fenntarthatósága nagymértékben a szervezeti elfogadottságon, a szabályok betarthatóságán és a technológiai támogatottságon múlik.

A BYOD kezeléséhez a mobileszközök központi menedzsmentje is szükségessé vált, amelyet a szakirodalom MDM (Mobile Device Management) rendszerekként ír le [23]. Ezek célja, hogy a mobileszközök üzleti célú használatát támogassák, miközben a vállalati információbiztonsági szintet fenntartják. Az MDM által lefedett funkciók közé tartozik a felhasználók és eszközök azonosítása/hitelesítése, a szabályzatoknak való megfelelés támogatása, a szoftverkörnyezet naprakészen tartása, az eszközhasználat nyomon követése, a privát- és vállalatiadatok elkülönítése, valamint távoli beavatkozási lehetőség biztonsági események esetén - például távolról elindított adattörlés az eszköz eltulajdonításának vagy elvesztésének jelentésekor.

A BYOD kezelésének szervezeti realitását jól mutatja a nemzetközi vállalati gyakorlat, amelyben többféle támogatási szint jelenik meg:

- minden eszköz támogatása,
- kijelölt eszközök támogatása,
- csak hálózati hozzáférés biztosítása támogatás nélkül, illetve
- a tiltás.

A dolgozók motivációi a kényelemhez, szabadsághoz és a preferált eszközhasználathoz kapcsolódnak, így a stratégia kialakításának emberi és szervezeti tényezőkre is reagálnia kell [144].

2.8.4 Stratégiai kérdések összegzése

Összegzésként megállapítható, hogy a BYOD kezelése vezetői szintű stratégiai döntést igényel, amelynek középpontjában az áll, hogy milyen típusú adatok milyen körülmények között és milyen formában jelenhetnek meg a dolgozó mobileszközén. Dönteni kell a támogatott eszközkörről, a hozzáférési jogosultságok logikájáról, valamint arról is, hogy szervezeti szerep és munkakör szerint mely feladatok végezhetők BYOD-eszközön, és melyek nem.

A munkakör-alapú szabályozás ugyanakkor önmagában nem elégséges: indokolt lehet egyéni szinten is értékelni, hogy az adott munkavállaló milyen információbiztonsági kockázatot jelent

a szervezet számára, és ennek megfelelően kialakítani a hozzáférési és jogosultsági rendszert. A BYOD stratégia így akkor lehet stabil és fenntartható, ha (1) jogilag rendezett, (2) szervezeti szempontból elfogadott és betartható, valamint (3) technológiailag támogatott.

4. ábra A saját tulajdonú okoseszközök szabályozási lehetőségeinek szintjei
Forrás: saját szerkesztés az irodalomkutatásom alapján

2.9 A BYOD, mint adaptív döntési és kockázati rendszer

A BYOD jelenség a korábbi fejezetek alapján nem értelmezhető pusztán technológiai eszközhasználati kérdésként. A saját tulajdonú mobileszközök vállalati integrációja olyan összetett döntési helyzetet hoz létre, amelyben a technológiai infrastruktúra, a jogi szabályozás, a szervezeti kontrollmechanizmusok és az egyéni döntési mintázatok egyszerre formálják a kockázati struktúrát. BYOD környezetben a kontroll részben decentralizálódik: míg vállalati tulajdonú eszközök esetében a technikai és szervezeti kontroll alapvetően a munkáltató kezében koncentrálódik, addig magántulajdonú eszközöknél a kockázatkezelés egy része szükségszerűen a felhasználó döntésein keresztül érvényesül. A hozzáférési helyzetek kezelése, az alkalmazástelepítési gyakorlat, a hálózati csatlakozások megválasztása és az adatkezelési rutinok mind olyan mikroszintű döntések, amelyek aggregált hatásukban szervezeti szintű kockázatot generálnak. Ennek megfelelően a BYOD olyan döntési rendszerként ragadható meg, amelyben a kockázat nem statikus állapot, hanem folyamatosan alakuló interakciók eredője.

2.9.1 A BYOD döntési szintek rendszere

A BYOD döntési logikája több szinten értelmezhető. Stratégiai szinten a szervezet vezetése határozza meg az alapállást, vagyis azt, hogy a BYOD tiltott, megtűrt, szabályozott vagy tudatosan támogatott gyakorlatként jelenik meg. Ez a döntés nemcsak operatív kérdés, hanem kihat

a teljes információbiztonsági architektúrára, valamint a szervezeti kultúrára is. Taktikai szinten az IT- és információbiztonság-vezetés alakítja ki azokat a működtethető hozzáférési modelleket, eszközprofilokat és kontrollmechanizmusokat, amelyek a stratégiai irányt technikai és eljárásrendi megoldásokra fordítják le, ideértve az MDM-típusú megoldásokat is. Operatív szinten pedig a felhasználók mindennapi döntései határozzák meg a tényleges kitettséget: az, hogy milyen hálózatra csatlakoznak, milyen alkalmazásokat használnak, és hogyan kezelik a vállalati adatokat, közvetlenül befolyásolja a valós kockázati szintet.

A három szint közötti összhang hiánya önmagában strukturális sérülékenységet hozhat létre. Ha a stratégiai döntés nem tükröződik a taktikai szabályozásban, vagy a taktikai szabályozás nem illeszkedik a felhasználói viselkedéshez és munkavégzési realitásokhoz, akkor a rendszerben kockázati torzulás keletkezik: a formális kontroll erősnek látszik, miközben a tényleges kontrollálhatóság gyengülhet.

2.9.2 A kockázat szerkezeti újraértelmezése BYOD környezetben

A klasszikus információbiztonsági megközelítés a CIA-triád – bizalmasság, sértetlenség, rendelkezésre állás – mentén strukturálja a kockázatokat. BYOD esetében ez a keret továbbra is releváns, ugyanakkor kiegészül egy sajátos szervezeti dimenzióval: a kontroll eloszlásának kérdésével. Magántulajdonú eszközök használatakor a bizalmasság sérülhet az adatok keveredése vagy az eszköz elvesztése miatt, a sértetlenség sérülhet nem ellenőrzött alkalmazások és jogosultságok révén, a rendelkezésre állás pedig heterogén technológiai környezetben, eltérő konfigurációk és állapotok mellett válhat sérülékennyé. Mindezek mellett azonban a BYOD lényegi sajátossága, hogy a kontroll nem kizárólag szervezeti kézben van: megoszlik a szervezet és az egyén között. Ez a megosztottság az a tényező, amely a BYOD-t döntéselméleti szempontból különösen relevánssá teszi, mert a kockázati kimeneteket a szabályozás mellett a felhasználói döntési mechanizmusok is strukturálják.

2.9.3 A humán tényező, mint strukturális kockázati változó

A korábban bemutatott generációs sajátosságok és kockázatvállalási attitűdök alapján a felhasználói döntések nem pusztán információhiányból fakadnak, hanem értékorientációk, percepciók és rutinok által vezérelt viselkedési mintázatokként is értelmezhetők. BYOD környezetben a felhasználó visszatérően kompromisszumos helyzetekben dönt: a kényelem és a biztonság, a gyors hozzáférés és a szabályozási megfelelés, illetve a saját preferenciák és a szervezeti előírások között. E döntések szerkezeti sajátossága, hogy a haszon gyakran közvetlen és azonnali, míg a kockázat elvont, bizonytalan és sokszor késleltetett következmények formájában jelenik

meg. Ez a döntési aszimmetria önmagában növeli a kockázatos magatartás valószínűségét, különösen akkor, ha a szabályok betartása a felhasználói élményt jelentősen rontja.

Ebből következően a szervezet BYOD-környezetben nem támaszkodhat kizárólag technológiai eszközökre: a kockázatok csökkentéséhez tudatosságfejlesztésre, kultúraformálásra és olyan megközelítésekre is szükség van, amelyek a felhasználói kockázatészlelés és kockázatvállalás sajátosságait kezelhetővé teszik.

2.9.4 A BYOD, mint adaptív rendszer

A BYOD nem egyszeri döntés, hanem adaptív folyamat, mert a kockázati környezet folyamatosan változik. Új technológiai sérülékenységek jelennek meg, új alkalmazások terjednek el, a munkavállalói összetétel és digitális kompetencia időben átalakul, miközben a jogi környezet is módosulhat. Emiatt a BYOD-stratégia nem tekinthető statikus szabályzatnak: inkább olyan iteratív módon frissítendő rendszerként értelmezhető, amelyben a folyamatos visszacsatolás és korrekció indokolt. Ebben a keretben a PDCA-ciklus (Plan-Do-Check-Act iteratív, folyamatos fejlesztési módszertan) alkalmazása logikus, mert lehetővé teszi, hogy a szabályozás, a technológiai kontrollok és a felhasználói gyakorlatok alakulása ne elszigetelten, hanem egymásra reagálva legyen kezelhető.

Az eddigi fejezetek elméleti keretet adtak a BYOD komplex értelmezéséhez, és egyértelművé tették, hogy a technológiai, szervezeti és jogi dimenziók mellett a kockázati struktúra egyik kulcseleme a humán tényező, különösen az IT-biztonsági kontextusban megjelenő kockázatvállalási hajlandóság. A következő fejezetek ennek megfelelően azt vizsgálják, hogy az általános kockázatvállalási attitűd és az IT-biztonsági döntési mintázatok milyen kapcsolatban állnak egymással, illetve miként integrálhatók a szervezeti BYOD-stratégia kialakításába.

2.10 A fejezet összefoglalása

Az értekezés 2. fő fejezete a BYOD szocio-technikai rendszerét elemzi, magában foglalva a technológiai, szervezeti és kockázati dimenziókat. A fejezet központi állítása, hogy a BYOD nem csupán informatikai probléma, hanem egy összetett, folyamatosan változó rendszer, ahol a technikai sebezhetőségek és az emberi döntéshozatali mechanizmusok szorosan összefonódnak.

A BYOD technológiai és szervezeti keretei

Hangsúlyozom, hogy a saját tulajdonú eszközök használata elmosta a határokat a magánszféra és a vállalati információs tér között. Ez a kevert használati modell új típusú kihívásokat teremt:

Shadow IT (Árnyékinformatika): A munkavállalók gyakran a szervezet által nem jóváhagyott szoftvereket vagy szolgáltatásokat használnak feladataik elvégzéséhez, ami kontrollvesztéshez vezet.

MDM (Mobileszköz-menedzsment): A fejezet bemutatja azokat a szoftveres megoldásokat, amelyek lehetővé teszik a szervezetek számára az eszközök távoli felügyeletét és biztonsági szabályozását.

Katonai és stratégiai kontextus: Külön hangsúlyt kap a metaadat-kitettség (helyszín, hálózati adatok), amely katonai környezetben operatív vagy akár nemzetbiztonsági kockázatot is jelenthet az adatok aggregálhatósága miatt.

A kockázat szerkezeti elemzése

A fejezet egyik legfontosabb elméleti hozzájárulása a BYOD-kockázatok rendszerezése a klasszikus CIA-triád (bizalmasság, sértetlenség, rendelkezésre állás) mentén.

A kockázatokat négy fő dimenzióba sorolja:

1. Technológiai kockázatok: Eszközspecifikus sérülékenységek, operációs rendszerek korlátozásainak eltávolítása (Rootolás/Jailbreak).
2. Adat- és kommunikációs kockázatok: Adatszivárgás, titkosítatlan vagy nem megfelelően titkosított csatornák használata.
3. Humán és viselkedési kockázatok: A kényelemből fakadó óvatlanság és a szubjektív kockázatészlelés hibái.
4. Szervezeti és infrastrukturális kockázatok: A szabályozás hiánya vagy a túl szigorú kontroll miatti ellenállás.

Stratégiai modellek és döntési mechanizmusok

Megállapítottam, hogy a szervezeteknek nem csupán technikai védelmet kell kiépíteniük, hanem tudatos BYOD-stratégiát kell alkotniuk.

Ennek részei:

Költség–biztonság összefüggés: Az optimális biztonsági szint megtalálása, felismerve, hogy a „100%-os biztonság” elvi okokból sem elérhető.

Adaptív rendszer: A BYOD-t olyan rendszerként kell kezelni, amely folyamatosan alkalmazkodik a technológiai trendekhez és a felhasználói szokásokhoz.

A fejezet legfontosabb eredményei

A humán faktor dominanciája: A kutatás megerősíti, hogy a biztonsági lánc leggyengébb láncszeme az ember, akinek a kényelemszeretete és a „velem úgysem történik meg” attitűdje szisztematikusan alulbecsli a digitális veszélyeket.

A technikai kompetencia paradoxona: Kimutatható, hogy a magasabb informatikai képzettség nem jár automatikusan óvatosabb viselkedéssel; a technikai magabiztosság néha még növelheti is a kockázatvállalást.

Strukturális aszimmetria: A döntéshozatali folyamatban az észlelt haszon (gyorsaság, kényelem) súlya jelentősen meghaladja az észlelt kockázatét, ami a biztonsági szabályok megkerülésére ösztönözheti a felhasználót.

Legfontosabb hivatkozások a fejezetben:

- Renn (2017): Risk Governance, Coping with Uncertainty in a Complex World. [12]
- Weber U. Elke, Blais Renée Ann, Betz E. Nancy (2002): A Domain-Specific Risk-Attitude Scale: Measuring Risk Perceptions and Risk Behaviors [27]
- ENISA (2013): Az okostelefonokhoz kapcsolódó legfontosabb információbiztonsági kockázatok rendszerezése. [34]
- Michelberger Pál (2022): Információ-, folyamat- és vállalatbiztonság [6]
- ISO/IEC 27001: Information security, cybersecurity and privacy protection [135]

Ez a fejezet teremti meg az elméleti hidat a technológiai adottságok és a dolgozat későbbirészében bemutatott empirikus vizsgálatok között, bizonyítva, hogy a BYOD biztonságának alapfeltétele a megfelelő humán döntési architektúra.

3 EMPIRIKUS VIZSGÁLAT ÉS MODELLÉPÍTÉS AZ IT-BIZTONSÁGI KOCKÁZATVÁLLALÁS TERÜLETÉN

3.1 A kutatási modell és hipotézisrendszer felépítése

A disszertáció elméleti fejezetei rámutattak arra, hogy a BYOD-környezetben megjelenő információbiztonsági kockázatok nem redukálhatók kizárólag technológiai sebezhetőségekre. A klasszikus információbiztonsági megközelítés – különösen az ISO/IEC 27001 által is hangsúlyozott bizalmasság, sértetlenség és rendelkezésre állás (CIA) attribútumai – rendszerszintű kockázatokat ír le, azonban a BYOD kontextus sajátossága, hogy a vállalati és magánhasználat közötti határ elmosódik. Ennek következtében az egyéni döntések közvetlenül szervezeti kockázattá transzformálódnak.

A kockázat fogalmának Renn [11] [12] által adott meghatározása – miszerint kockázatról akkor beszélünk, amikor emberi érték forog kockán bizonytalan kimenetel mellett – különösen releváns a BYOD esetében. Itt ugyanis nem pusztán technikai hibáról, hanem értéket érintő döntésekről van szó: vállalati adatok kezelése, hálózati csatlakozás, autentikációs gyakorlatok, mind olyan helyzetek, ahol az egyéni kockázatészlelés és kockázatvállalás meghatározó szerepet játszik.

A disszertáció egyik központi elméleti kérdése ezért az volt, hogy az információbiztonsági kontextusban megjelenő kockázatvállalás tekinthető-e az általános kockázatvállalási attitűd részének, vagy sajátos, kontextusfüggő jelenségként kezelendő. A kérdés megválaszolásához a Weber, Blais és Betz [27] által kidolgozott DOSPERT modell szolgált kiindulópontként, amely a kockázatvállalást domén-specifikus jelenségként értelmezi. A modell implicit módon abból indul ki, hogy az egyén kockázatvállalási preferenciája a várható haszon és az észlelt kockázat szubjektív mérlegelésének eredménye.

A BYOD környezetben azonban a „várható haszon” és az „észlelt kockázat” viszonya sajátos. A mobilitás, a kényelem és a produktivitás növekedése rövid távú előnyként jelenik meg, míg a biztonsági incidensek valószínűsége és következménye gyakran absztrakt, távoli és alulészlelt. Ebből következően indokolt volt annak vizsgálata, hogy az IT-biztonsági döntések a DOSPERT eredeti doménjeinek logikájába illeszkednek-e, vagy külön mérési dimenziót igényelnek.

Ennek megfelelően az első vizsgálati irány arra irányult, hogy a DOSPERT eredeti elemei képesek-e előre jelezni az IT-biztonsági helyzetekre adott válaszokat. Ha az információbiztonsági kockázatvállalás pusztán az általános kockázatvállalási attitűd egyik megnyilvánulása lenne,

akkor a pénzügyi, etikai, egészségügyi vagy szociális doménben mért értékek szignifikáns magyarázóerővel kellene, hogy rendelkezzenek az IT-domén elemeire nézve is.

A vizsgálat eredményeinek empirikus tesztelhetősége érdekében az alábbi hipotéziseket fogalmaztam meg:

H1: A DOSPERT eredeti doménjei nem képesek szignifikáns mértékben előre jelezni az IT-biztonsági kockázati kérdésekre adott válaszokat.

Ez a hipotézis implicit módon azt vizsgálja, hogy az IT-biztonsági kockázatvállalás önálló dimenzióként értelmezhető-e, és ezzel hozzájárul a domén-specifikus kockázatelmélet finomításához.

A második kutatási kérdés a kockázatészlelés relatív súlyára irányult. A kockázatpszichológiai irodalom szerint az emberek hajlamosak bizonyos típusú kockázatokat – különösen a közvetlen fizikai vagy etikai következményekkel járókat – magasabbnak értékelni, mint a technológiai vagy absztrakt természetű veszélyeket. Ha az IT-biztonsági kockázatok az észlelt rangsor közép- vagy alsó mezőnyében helyezkednek el, az a biztonságtudatosság strukturális hiányosságára utalhat.

Ennek empirikus vizsgálatára a következő hipotézis került megfogalmazásra:

H2: Az IT-biztonsági domén észlelt kockázati szintje nem a legmagasabb a vizsgált kockázati domének között.

Ez a hipotézis közvetlen kapcsolatban áll az információbiztonsági kultúra érettségének kérdésével, amelyet a korábbi fejezetekben bemutatott biztonságtudatossági modellek is hangsúlyoztak.

A harmadik vizsgálati irány a tudás és attitűd kapcsolatára fókuszált. Az elméleti keretben bemutatásra került, hogy a technikai kompetencia és a kockázatészlelés között nem feltétlenül lineáris kapcsolat áll fenn. Egyrészt feltételezhető, hogy a magasabb szintű informatikai tudás növeli a veszélyek felismerésének képességét; másrészt a technikai magabiztosság csökkentheti a szubjektív kockázatérzetet.

E dilemmára reflektálva került megfogalmazásra a következő hipotézis:

H3: A különböző szakok hallgatói között szignifikáns különbség mutatható ki az IT-biztonsági kockázatok észlelésében.

Ez a hipotézis lehetővé teszi annak vizsgálatát, hogy a képzési háttér milyen mértékben strukturálja a kockázatészlelést.

A negyedik kutatási irány már a kockázatészlelés és a tényleges viselkedés kapcsolatát vizsgálta. A racionális döntéselméleti modellek szerint a magasabb észlelt kockázat alacsonyabb kockázatvállalási hajlandósággal jár együtt. Ugyanakkor a viselkedéstudományi kutatások többek között Hofstede és munkatársai rámutattak, hogy az attitűd és a viselkedés közötti kapcsolat nem mindig közvetlen [31] [32].

Ennek vizsgálatára a következő hipotézis került megfogalmazásra:

H4: Az IT-biztonsági kockázatok magasabb észlelése pozitív kapcsolatban áll a biztonságtudatos viselkedési gyakorlatok alkalmazásával.

Ez a hipotézis a kockázatészlelés és a preventív viselkedés közötti kapcsolat empirikus ellenőrzését teszi lehetővé.

Végül a kutatás során azonosításra került egy potenciális paradox jelenség is, amely szerint bizonyos technikailag tudatos felhasználók hajlamosak lehetnek olyan magatartásra is, amely szervezeti szempontból kockázatosnak tekinthető, például vállalati adatok saját eszközre történő másolására. Ez a jelenség arra utalhat, hogy a technikai biztonságtudatosság és a szervezeti lojalitás vagy szabálykövetés nem azonos dimenziók mentén szerveződik.

Ennek vizsgálatára az alábbi hipotézis került megfogalmazásra:

H5: A technikai biztonságtudatosság egyes formái együtt járhatnak BYOD-kontextusban magasabb szervezeti kockázatvállalási hajlandósággal.

Ez a hipotézis túlmutat a lineáris kockázatmodell-értelmezésen, és a viselkedési komplexitás vizsgálatát teszi lehetővé.

A fenti hipotézisek elsősorban az IT-biztonsági kockázatvállalás domén-specifikusságára, relatív észlelési pozíciójára és a viselkedési összefüggésekre fókuszáltak. A kutatás további szakaszában azonban indokolttá vált a döntési struktúra belső súlyozási mechanizmusának mélyebb vizsgálata is.

A DOSPERT modell elméleti kerete implicit módon abból indul ki, hogy a kockázatvállalási döntések az észlelt haszon és az észlelt kockázat szubjektív mérlegelésének eredményei. A klasszikus döntéselméleti modellek kiegyensúlyozott nyereség–veszteség integrációt feltételeznek. Ugyanakkor az IT-biztonsági kontextus sajátosságai – az azonnali kényelem és produktivitás előnye, valamint a késleltetett és absztrakt következmények – arra utalnak, hogy a döntési architektúra aszimmetrikus lehet.

Ezért a kutatás egy további vizsgálati iránya annak empirikus ellenőrzésére irányult, hogy az IT-biztonsági helyzetekben a viselkedési szándék kialakulásában az észlelt haszon és az észlelt kockázat relatív súlya kiegyensúlyozott-e, vagy strukturális dominancia figyelhető meg.

Ennek empirikus vizsgálatára az alábbi hipotézist fogalmaztam meg:

H6: Az IT-biztonsági döntésekben az észlelt haszon standardizált regressziós súlya szignifikánsan meghaladja az észlelt kockázat abszolút értékű regressziós súlyát.

Ez a hipotézis a döntési architektúra aszimmetriáját vizsgálja, és túlmutat a puszta korrelációs összefüggéseken. Amennyiben a haszon dominanciája igazolódik, az arra utal, hogy az IT-biztonsági kockázatvállalás nem pusztán veszteségelkerülési mechanizmus mentén szerveződik, hanem megközelítés-orientált motivációs struktúrát tükröz.

A következő vizsgálati irány annak feltárására irányult, hogy ez az esetleges haszon-dominancia kizárólag az IT-domén sajátossága-e, vagy más kockázati területeken is megfigyelhető strukturális mintázat. Amennyiben az aszimmetria több doménben stabilan fennáll, az a döntéshozatal általánosabb szerkezeti sajátosságára utal.

Ennek megfelelően a következő hipotézis:

H7: Az észlelt haszon és az észlelt kockázat közötti súlyozási aszimmetria nem kizárólag az IT-biztonsági doménre jellemző, hanem más kockázati területeken is kimutatható.

Ez a hipotézis lehetővé teszi a döntési mechanizmus strukturális összehasonlítását, és hozzájárul a domén-specifikus kockázatelmélet finomításához.

A kutatás további kiterjesztése során indokolttá vált a demográfiai háttértényezők kontrollált vizsgálata is. Bár a korábbi hipotézisek érintették a szakok közötti különbségeket, a nem és az életkor hatása önálló modellben, az általános kockázati dimenziók kontrollálása mellett is vizsgálhatóvá vált. Ennek megfelelően állítottam fel a következő hipotéziseket:

H8: Az életkor az általános kockázatvállalási dimenziók kontrollálása mellett szignifikáns magyarázóerővel bír az IT-biztonsági kockázatvállalás tekintetében.

H9: A nem az általános kockázatvállalási dimenziók kontrollálása mellett is szignifikáns kapcsolatban áll az IT-biztonsági kockázatvállalással.

Ezen hipotézisek lehetővé teszik annak vizsgálatát, hogy az IT-biztonsági döntések mennyiben tekinthetők tisztán attitűdalapú jelenségnek, és mennyiben strukturálódnak stabil demográfiai háttértényezők mentén.

3.2 Módszertani keret és empirikus adatgyűjtés

A disszertáció empirikus vizsgálatai kvantitatív, kérdőíves módszertanra épültek, amelynek célja az információbiztonsági kontextusban megjelenő kockázatvállalási hajlandóság szerkezetének feltárása, annak mérési lehetőségeinek vizsgálata, valamint a kockázatészlelés és a biztonságtudatos viselkedés közötti összefüggések elemzése volt. A kutatási terv több, egymásra épülő adatfelvételi szakaszból állt, amelyek különböző mintákon, de azonos mérési logikával vizsgálták a kérdéskört.

A disszertáció empirikus alapját két, időben elkülönülő adatfelvétel képezi, amelyek azonos mérési logikával, de eltérő mintákon valósultak meg.

Az első adatfelvételre 2019 őszén került sor, amelynek keretében 357 fő (az egyes elemzésekben 302–357 fő közötti a minta nagysága, a hiányzó válaszok függvényében) egyetemi hallgató töltötte ki a módosított DOSPERT kérdőívet. Ez az adatfelvétel elsősorban a mérési konstrukció vizsgálatára, az IT-domén elkülönülésének tesztelésére, valamint a regressziós modellek alkalmazhatóságának elemzésére szolgált. A második adatfelvételre 2025 őszén került sor, kibővített kérdőív alkalmazásával, amely már nemcsak az IT-domén elemeit, hanem az észlelt haszon, észlelt kockázat és viselkedési szándék külön mérését is lehetővé tette. E második kutatás során a kérdőívet 772 töltötte ki. Így, ez a vizsgálat nagyobb mintán zajlott, és a disszertációban bemutatott, valamint a kapcsolódó tudományos publikációkban ismertetett döntési architektúra-elemzések alapját képezte. A két adatfelvétel nem paneljellegű, tehát nem ugyanazon válaszadók ismételt méréséről van szó, hanem egymástól független mintákon végzett, konzisztens mérési struktúrán alapuló vizsgálatokról. A kutatási terv így lehetővé tette az eredmények részleges replikációját és a modell stabilitásának ellenőrzését.

A mérési konstrukció alapját a Weber, Blais és Betz [27] által kidolgozott DOSPERT kérdőív 2006-os változatának magyar nyelvű, Radnóti István által készített fordítása képezte, amely a

kockázatvállalási hajlandóságot domén-specifikus struktúrában ragadja meg. A kérdőív magyar nyelvű adaptációja került alkalmazásra, amely öt eredeti domént tartalmaz: pénzügyi, egészség/biztonsági, rekreációs, etikai és szociális területet. A disszertáció elméleti keretében megfogalmazott kutatási kérdések alapján a kérdőívet kiegészíttettem egy információ-biztonsági doménnel, amely öt, kifejezetten IT- és BYOD-kontextusban értelmezhető szituatív elemet tartalmazott. E kérdések a vállalati adatok privát csatornán történő továbbítására, nyílt WiFi-hálózathoz való csatlakozásra, jelszóhasználatra, eszközátadásra és vállalati adatok saját tulajdonú eszközre másolására vonatkoztak. A válaszadás minden esetben hétfokozatú Likert-skálán történt, amely az észlelt kockázat, illetve a cselekvési hajlandóság szubjektív értékelését tette lehetővé. A skála ordinális jellegéből adódóan az adatelemzés során a normalitási feltételek vizsgálata után paraméteres vagy nem-paraméteres eljárásokat alkalmaztam.

A hipotézisek vizsgálata eltérő statisztikai módszereket igényelt, összhangban a mérési konstrukció természetével és a vizsgált összefüggések típusával.

Az első hipotézis annak tesztelésére irányult, hogy a DOSPERT eredeti doménjei képesek-e előre jelezni az IT-biztonsági kockázati kérdésekre adott válaszokat. Ennek vizsgálatára többszörös lineáris regresszióelemzést alkalmaztam. Az IT-domén egyes elemei – illetve az ezekből képzett aggregált mutató – függő változóként, míg az öt eredeti domén átlagértékei független változóként szerepeltek a modellben. A regressziós elemzés lehetővé tette annak meghatározását, hogy az általános, domén-specifikus kockázatvállalási attitűd milyen mértékben rendelkezik magyarázóerővel az információbiztonsági összefüggésben megjelenő döntések tekintetében. A modell értékelése során a determinációs együttható (R^2), az egyes regressziós együtthatók szignifikanciaszintje, valamint a modell globális illeszkedése szolgált döntési kritériumként.

A második hipotézis a kockázatészlelés relatív súlyát vizsgálta, vagyis azt, hogy az IT-biztonsági domén az észlelt kockázati rangsorban milyen pozíciót foglal el a többi doménhez képest. Ennek empirikus elemzéséhez leíró statisztikai mutatókat – átlagok és szórások – számoltam minden domén esetében, majd az egyes domének közötti különbségek vizsgálatára ismételt méréses varianciaanalízist vagy – a normalitási feltételek sérülése esetén – Friedman-próbát alkalmaztam. A cél annak megállapítása volt, hogy az IT-domén szignifikánsan eltér-e a többi területtől, illetve hogy a rangsorban milyen pozíciót foglal el.

A harmadik hipotézis a képzési háttér és az IT-kockázatészlelés közötti kapcsolat vizsgálatára irányult. A szak szerinti csoportok közötti különbségek elemzéséhez két csoport esetén

független mintás t-próba, több csoport esetén egyutas varianciaanalízis (ANOVA) került alkalmazásra. Amennyiben a varianciahomogenitás vagy normalitás feltétele nem teljesült, nemparaméteres alternatívákat – Mann–Whitney-próba vagy Kruskal–Wallis-teszt –alkalmaztam. Az elemzés célja annak meghatározása volt, hogy a képzési háttér strukturálja-e az információbiztonsági kockázatok észlelését.

A negyedik hipotézis a kockázatészlelés és a biztonságtudatos viselkedés közötti kapcsolatot vizsgálta. Mivel a biztonsági gyakorlatokra vonatkozó kérdések ordinális vagy dichotóm jellegűek voltak, az összefüggések elemzéséhez Spearman-féle rangkorrelációs együtthatót használtam. A vizsgálat arra irányult, hogy az IT-biztonsági helyzetek magasabb észlelt kockázata együtt jár-e preventív viselkedési mintázatokkal, például kétfaktoros hitelesítés használatával, rendszeres frissítések telepítésével vagy jelszókezelő alkalmazásával.

Az ötödik hipotézis egy komplexebb viselkedési paradoxon vizsgálatára irányult, amely szerint a technikai biztonságtudatosság bizonyos formái együtt járhatnak szervezeti szempontból kockázatos magatartással, például vállalati adatok saját tulajdonú eszközre másolásával. Ennek vizsgálatához szintén Spearman-korreláció, illetve szükség esetén logisztikus regresszióelemzést alkalmaztam, ahol a kockázatos magatartás dichotóm függő változóként szerepelt. Ez az elemzés lehetővé tette annak feltárását, hogy a biztonságtudatos technikai gyakorlatok és a BYOD-kontextusban megjelenő szervezeti kockázatvállalás milyen mintázatot mutat.

Az elemzések minden esetben 5%-os szignifikanciaszint mellett kerültek értékelésre. A statisztikai számítások SPSS szoftver segítségével történtek. A minta nem reprezentatív jellege miatt az eredmények általánosíthatósága korlátozott, azonban a cél nem populációs becslés, hanem elméleti konstrukciók empirikus tesztelése volt.

Összességében a módszertani megközelítés lehetővé tette a kockázatvállalási attitűd doménspecifikus szerkezetének, az IT-biztonsági dimenzió önállóságának, valamint a kockázatészlelés és viselkedés közötti kapcsolat differenciált vizsgálatát. A választott statisztikai eljárások minden hipotézis esetében közvetlenül illeszkedtek a vizsgált konstrukció természetéhez, biztosítva az elméleti kérdésfeltevések empirikus tesztelhetőségét.

A két adatfelvétel nemcsak időben, hanem kutatási fókuszában is eltérő hangsúlyokkal rendelkezett, amely indokolttá teszi a hipotézisek adatforráshoz való egyértelmű hozzárendelését.

Az első, 2019-ben végzett adatfelvétel (N ≈ 357 fő) elsődleges célja az információbiztonsági domén elkülönülésének vizsgálata és a módosított DOSPERT mérési konstrukció validálása volt. Ennek keretében kerültek tesztelésre a következő hipotézisek:

- H1: a DOSPERT eredeti doménjeinek prediktív ereje az IT-elemekre vonatkozóan,
- H2: az IT-domén relatív észlelt kockázati pozíciója,
- H3: a képzési háttér hatása az IT-kockázatészlelésre,
- H4: a kockázatészlelés és a biztonságtudatos viselkedés kapcsolata,
- H5: a technikai biztonságtudatosság és a szervezeti kockázat paradox viszonya.

Ez az adatfelvétel tehát elsősorban a domén-specifikusság és a viselkedési összefüggések strukturális vizsgálatát tette lehetővé.

A második, 2025 őszén megvalósított adatfelvétel már kiterjesztett mérési logikával készült. Ebben az esetben az észlelt kockázat, az észlelt haszon és a viselkedési szándék elkülönített mérése is megtörtént, amely lehetővé tette a döntési architektúra regressziós modellben történő elemzését. A második adatfelvétel szolgált alapul a döntési súlyozási mechanizmus vizsgálatához, valamint a demográfiai háttértényezők kontrollált elemzéséhez.

Ennek keretében kerültek empirikusan tesztelésre a következő hipotézisek:

- H6: az észlelt haszon regressziós súlya meghaladja az észlelt kockázat abszolút értékű súlyát az IT-döntésekben,
- H7: a haszon–kockázat súlyozási aszimmetria más kockázati doménekben is kimutatható,
- H8: az életkor kontrollált modellben is szignifikáns magyarázóerővel bír az IT-kockázatvállalás tekintetében,
- H9: a nem kontrollált modellben is kapcsolatban áll az IT-kockázatvállalással.

A két adatfelvétel egymástól független mintákon történt, így nem longitudinális vizsgálatról, hanem egymásra épülő, de keresztmetszeti jellegű elemzésekről van szó. Ugyanakkor az azonos mérési alaplogika és a konstrukciós konzisztencia lehetővé tette az eredmények részleges replikációját és a modell stabilitásának vizsgálatát. E módszertani felépítés erősíti a disszertáció belső koherenciáját: az első adatfelvétel a mérési konstrukció és a domén-specifikusság kérdésére fókuszált, míg a második adatfelvétel a döntési architektúra finomabb, regressziós szintű elemzését tette lehetővé.

3.3 Az empirikus vizsgálat eredményei

H1: A DOSPERT eredeti doménjei nem képesek szignifikáns mértékben előre jelezni az IT-biztonsági kockázati kérdésekre adott válaszokat.

Az első hipotézis a disszertáció egyik központi elméleti kérdésére reflektál: vajon az információbiztonsági kockázatvállalás az általános, domén-specifikus kockázatvállalási attitűd részének tekinthető-e, vagy önálló konstrukcióként értelmezendő. A kérdés nem pusztán módszertani, hanem elméleti jelentőségű is, hiszen amennyiben az IT-biztonsági kockázatvállalás beágyazódik a DOSPERT eredeti struktúrájába, akkor külön mérési dimenzió kialakítása nem indokolt. Ellenkező esetben azonban a technológiai kontextus sajátosságai önálló attitűdstruktúrát implikálnak.

A vizsgálat során többszörös regresszióelemzést alkalmaztam, amelyben az IT-domén egyes elemei (például: vállalati adatok privát e-mail címre történő továbbítása, nyílt WiFi-hálózathoz való csatlakozás, jelszó mások előtti használata stb.) függő változóként, míg a DOSPERT eredeti öt doménjének aggregált mutatói független változóként szerepeltek.

Az elemzések minden egyes IT domén elemei esetében alacsony determinációs együtthatót (R^2) eredményeztek, ami azt jelzi, hogy az eredeti doménstruktúra csekély mértékben magyarázza az IT-biztonsági döntéseket. Az egyes regressziós együtthatók többsége nem bizonyult szignifikánsnak, és ahol gyenge kapcsolat kimutatható volt, az nem alkotott konzisztens mintázatot.

A vállalati adatok privát e-mail címre történő továbbításának kérdése esetében (lásd 1. táblázat) az eredmények azt mutatták, hogy a DOSPERT eredeti doménjei nem rendelkeznek érdemi magyarázóerővel. Egyedül a „hazasétálni egyedül egy nem biztonságos városrészben” kérdéssel volt kimutatható gyenge pozitív kapcsolat. Azonban ez nem utal strukturális prediktív összefüggésre, inkább véletlenszerű együttjárásnak tekinthető.

1. táblázat Regresszió számítás eredménye a privát e-mail címre továbbított vállalati adatok kérdése és a további kérdések között

Model Summary - ICT KOCKÁZAT Vállalati adatokat a privát emailcímemre továbbítani. 3

Model	R	R^2	Adjusted R^2	RMSE
H_0	0.000	0.000	0.000	1.614
H_1	0.576	0.332	0.277	1.372

ANOVA

Model		Sum of Squares	df	Mean Square	F	p
H_1	Regression	307.977	27	11.407	6.061	< .001
	Residual	619.155	329	1.882		
	Total	927.132	356			

Note. The intercept model is omitted, as no meaningful information can be shown.

Coefficients

Model		Unstandardized	Standard Error	Standardized	t	p
H_0	(Intercept)	3.852	0.085		45.094	< .001
H_1	(Intercept)	-0.125	0.472		-0.265	0.791
	E KOCKÁZAT Megkérdőjelezhető költségeket leírni az adóbevallásban.3	0.217	0.069	0.186	3.141	0.002
	E KOCKÁZAT Más munkáját a sajátomként felhasználni. 3	0.103	0.062	0.090	1.666	0.097
	E KOCKÁZAT Egy barát titkát kifecsegni. 3	0.030	0.059	0.027	0.510	0.611
	E KOCKÁZAT Egy kisgyereket magára hagyni otthon egyedül, amíg elmegy a boltba. 3	0.180	0.056	0.175	3.238	0.001
	E KOCKÁZAT Egy 50.000 Ft-ot tartalmazó pénztárcát megtartani. 2	0.028	0.050	0.030	0.570	0.569
	F KOCKÁZAT A napi jövedelmem feltenni lóversenyre. 3	0.053	0.070	0.047	0.748	0.455
	F KOCKÁZAT Az éves jövedelmem 10% -át befektetni egy mérsékelt növekedésű, diverzifikált alapba. 3	0.001	0.064	8.192×10^{-4}	0.016	0.987
	F KOCKÁZAT Egy napi jövedelmet feltenni egy kockázatos pókerjátszmában. 3	-0.100	0.071	-0.090	-1.422	0.156
	F KOCKÁZAT Az éves jövedelmem 5%-át egy magaskockázatú befektetésbe fektetni. 3	-0.014	0.063	-0.013	-0.232	0.817
	F KOCKÁZAT Egy napi jövedelmet feltenni egy sportmérkőzésre. 3	0.065	0.070	0.061	0.929	0.354
	F KOCKÁZAT Az éves jövedelmem 10%-át egy új üzleti lehetőségbe fektetni. 3	0.059	0.067	0.049	0.884	0.378
	H KOCKÁZAT Túl sok alkoholt fogyasztani egy társadalmi eseményen, például egy esküvőn. 3	0.047	0.052	0.049	0.917	0.360
	H KOCKÁZAT Biztonságiöv viselése nélkül vezetni. 3	0.064	0.069	0.061	0.934	0.351
	H KOCKÁZAT Bukósisak nélkül motorozni.3	-0.039	0.079	-0.031	-0.494	0.622
	H KOCKÁZAT Naptej nélkül napozni. 3	-0.042	0.056	-0.039	-0.761	0.447
	H KOCKÁZAT Hazasétálni egyedül egy nem biztonságos városrészben. 3	0.241	0.064	0.201	3.760	< .001
	R KOCKÁZAT Olyan sípályán lesiklani, ami meghaladja a képességeim. 3	-0.042	0.065	-0.036	-0.649	0.517
	R KOCKÁZAT Vadvízi evezésre menni tavasszal, nagy vízállás esetén.3	-0.004	0.063	-0.004	-0.063	0.950
	R KOCKÁZAT Ejtőernyőzni.3	-0.011	0.064	-0.011	-0.172	0.864
	R KOCKÁZAT Bungeejumpingozni egy magas hídról. 3	0.034	0.066	0.034	0.519	0.604
	R KOCKÁZAT Kis repülőgépet vezetni. 3	-0.101	0.058	-0.095	-1.721	0.086
	S KOCKÁZAT Beismerni egy barátomnak, hogy az ízlésem különbözik az övétől.3	-0.063	0.059	-0.053	-1.069	0.286
	S KOCKÁZAT Egy hatósági személlyel összekülönbözni.3	0.063	0.069	0.052	0.912	0.362
	S KOCKÁZAT Izgalmasabb karrierbe kezdeni egy biztosabb karrirer helyett. 2	-0.077	0.081	-0.052	-0.954	0.341
	S KOCKÁZAT Egy kellemetlen témáról beszélni egy munkahelyi megbeszélésen. 2	0.040	0.069	0.031	0.569	0.569
	S KOCKÁZAT A családtól és a rokonoktól távolra költözni. 3	0.148	0.063	0.124	2.361	0.019
	S KOCKÁZAT Harmincötévesen új karrierbe kezdeni. 2	0.157	0.075	0.118	2.076	0.039

Forrás: saját szerkesztés a minta alapján

A nyílt WiFi-hálózathoz való csatlakozás esetében (2. táblázat) nem volt kimutatható szignifikáns kapcsolat az eredeti doménekkel. Ez különösen fontos eredmény, mivel a nyílt hálózathasználat objektív információbiztonsági kockázata magas, mégsem illeszkedik az általános kockázatvállalási mintázatokhoz.

2. táblázat Regresszió számítás eredménye a nyilvánosan elérhető nyílt WiFi hálózatokhoz való csatlakozás kérdése és a további kérdések között

Model Summary - ICT KOCKÁZAT Egy nyilvános wifihez csatlakozni. 3

Model	R	R^2	Adjusted R^2	RMSE
H_0	0.000	0.000	0.000	1.568
H_1	0.425	0.181	0.114	1.476

ANOVA

Model		Sum of Squares	df	Mean Square	F	p
H_1	Regression	158.293	27	5.863	2.692	< .001
	Residual	716.564	329	2.178		
	Total	874.857	356			

Note. The intercept model is omitted, as no meaningful information can be shown.

Coefficients

Model		Unstandardized	Standard Error	Standardized	t	p
H_0	(Intercept)	2.714	0.083		32.715	< .001
H_1	(Intercept)	0.443	0.508		0.872	0.384
	E KOCKÁZAT Megkérdőjelezhető költségeket leírni az adóbevallásban.3	-0.033	0.074	-0.029	-0.439	0.661
	E KOCKÁZAT Más munkáját a sajátomként felhasználni. 3	0.048	0.066	0.043	0.722	0.471
	E KOCKÁZAT Egy barát titkát kifecsegni. 3	0.088	0.064	0.081	1.382	0.168
	E KOCKÁZAT Egy kisgyereket magára hagyni otthon egyedül, amíg elmegy a boltba. 3	-0.093	0.060	-0.093	-1.551	0.122
	E KOCKÁZAT Egy 50.000 Ft-ot tartalmazó pénztárcát megtartani. 2	0.012	0.054	0.013	0.226	0.821
	F KOCKÁZAT A napi jövedelmem feltenni lóversenyre. 3	-0.014	0.076	-0.013	-0.182	0.855
	F KOCKÁZAT Az éves jövedelmem 10% -át befektetni egy mérsékelt növekedésű, diverzifikált alapba. 3	0.065	0.069	0.055	0.951	0.342
	F KOCKÁZAT Egy napi jövedelmet feltenni egy kockázatos pókerjátszmában. 3	-0.134	0.076	-0.123	-1.765	0.078
	F KOCKÁZAT Az éves jövedelmem 5%-át egy magaskockázatú befektetésbe fektetni. 3	0.065	0.067	0.058	0.960	0.338
	F KOCKÁZAT Egy napi jövedelmet feltenni egy sportmérkőzésre. 3	-0.045	0.075	-0.043	-0.599	0.549
	F KOCKÁZAT Az éves jövedelmem 10%-át egy új üzleti lehetőségbe fektetni. 3	0.017	0.072	0.014	0.233	0.816
	H KOCKÁZAT Túl sok alkoholt fogyasztani egy társadalmi eseményen, például egy esküvőn. 3	0.023	0.056	0.024	0.408	0.684
	H KOCKÁZAT Biztonságiöv viselése nélkül vezetni. 3	0.122	0.074	0.118	1.643	0.101
	H KOCKÁZAT Bukósisak nélkül motorozni.3	-0.043	0.085	-0.035	-0.504	0.614
	H KOCKÁZAT Naptej nélkül napozni. 3	0.090	0.060	0.086	1.511	0.132
	H KOCKÁZAT Hazasétálni egyedül egy nem biztonságos városrészben. 3	0.205	0.069	0.176	2.966	0.003
	R KOCKÁZAT Olyan sípályán lesiklani, ami meghaladja a képességeim. 3	-0.024	0.070	-0.021	-0.345	0.730
	R KOCKÁZAT Vadvízi evezésre menni tavasszal, nagy vízállás esetén.3	-0.026	0.068	-0.024	-0.384	0.701
	R KOCKÁZAT Ejtőernyőzni.3	-0.034	0.069	-0.034	-0.493	0.622
	R KOCKÁZAT Bungeejumpingozni egy magas hídról. 3	0.017	0.071	0.018	0.241	0.809
	R KOCKÁZAT Kis repülőgépet vezetni. 3	0.130	0.063	0.126	2.060	0.040
	S KOCKÁZAT Beismerni egy barátomnak, hogy az ízlésem különbözik az övétől.3	0.110	0.063	0.096	1.743	0.082
	S KOCKÁZAT Egy hatósági személlyel összekülönbözni.3	-0.021	0.074	-0.018	-0.281	0.779
	S KOCKÁZAT Izgalmasabb karrierbe kezdeni egy biztosabb karrirer helyett. 2	0.019	0.087	0.013	0.214	0.831
	S KOCKÁZAT Egy kellemetlen témáról beszélni egy munkahelyi megbeszélésen. 2	0.181	0.075	0.149	2.427	0.016
	S KOCKÁZAT A családtól és a rokonoktól távolra költözni. 3	-0.006	0.067	-0.005	-0.091	0.927
	S KOCKÁZAT Harmincötévesen új karrierbe kezdeni. 2	0.075	0.081	0.059	0.929	0.354

Forrás: saját szerkesztés a minta alapján

A jelszó vagy PIN mások előtti használatának kérdése (3. táblázat) esetében két gyenge kapcsolat volt megfigyelhető, például extrém fizikai kockázati helyzetekkel (pl. bungee jumping). Ezek azonban tematikusan és elméletileg sem indokolják az IT-domén beágyazottságát a rekreációs vagy fizikai kockázati dimenzióba.

3. táblázat Regresszió számítás eredménye a válaszadó PIN kódjának vagy jelszavának használata mások előtt kérdés és a további kérdések között

Model Summary - ICT KOCKÁZAT Mások előtt a pinkódomat / biztonsági mintámat használni. 2

Model	R	R^2	Adjusted R^2	RMSE
H_0	0.000	0.000	0.000	1.536
H_1	0.567	0.322	0.266	1.316

ANOVA

Model		Sum of Squares	df	Mean Square	F	p
H_1	Regression	270.084	27	10.003	5.776	< .001
	Residual	569.798	329	1.732		
	Total	839.882	356			

Note. The intercept model is omitted, as no meaningful information can be shown.

Coefficients

Model		Unstandardized	Standard Error	Standardized	t	p
H_0	(Intercept)	4.176	0.081		51.376	< .001
H_1	(Intercept)	0.645	0.453		1.423	0.156
	E KOCKÁZAT Megkérdőjelezhető költségeket leírni az adóbevallásban.3	-0.071	0.066	-0.064	-1.072	0.285
	E KOCKÁZAT Más munkáját a sajátomként felhasználni. 3	0.156	0.059	0.144	2.638	0.009
	E KOCKÁZAT Egy barát titkát kifecsegni. 3	0.113	0.057	0.107	1.993	0.047
	E KOCKÁZAT Egy kisgyereket magára hagyni otthon egyedül, amíg elmegy a boltba. 3	0.056	0.053	0.057	1.047	0.296
	E KOCKÁZAT Egy 50.000 Ft-ot tartalmazó pénztárcát megtartani. 2	0.026	0.048	0.028	0.536	0.592
	F KOCKÁZAT A napi jövedelmem feltenni lóversenyre. 3	0.009	0.067	0.009	0.139	0.890
	F KOCKÁZAT Az éves jövedelmem 10% -át befektetni egy mérsékelt növekedésű, diverzifikált alapba. 3	-0.034	0.061	-0.030	-0.561	0.575
	F KOCKÁZAT Egy napi jövedelmet feltenni egy kockázatos pókerjátszmában. 3	0.003	0.068	0.003	0.048	0.962
	F KOCKÁZAT Az éves jövedelmem 5%-át egy magaskockázatú befektetésbe fektetni. 3	0.086	0.060	0.079	1.435	0.152
	F KOCKÁZAT Egy napi jövedelmet feltenni egy sportmérkőzésre. 3	-0.046	0.067	-0.046	-0.692	0.489
	F KOCKÁZAT Az éves jövedelmem 10%-át egy új üzleti lehetőségbe fektetni. 3	-0.015	0.064	-0.013	-0.240	0.811
	H KOCKÁZAT Túl sok alkoholt fogyasztani egy társadalmi eseményen, például egy esküvőn. 3	0.058	0.050	0.063	1.180	0.239
	H KOCKÁZAT Biztonságiöv viselése nélkül vezetni. 3	0.054	0.066	0.053	0.812	0.418
	H KOCKÁZAT Bukósisak nélkül motorozni.3	0.111	0.076	0.094	1.469	0.143
	H KOCKÁZAT Naptej nélkül napozni. 3	0.104	0.053	0.100	1.944	0.053
	H KOCKÁZAT Hazasétálni egyedül egy nem biztonságos városrészben. 3	0.212	0.062	0.186	3.453	< .001
	R KOCKÁZAT Olyan sípályán lesiklani, ami meghaladja a képességeim. 3	-0.056	0.062	-0.050	-0.900	0.369
	R KOCKÁZAT Vadvízi evezésre menni tavasszal, nagy vízállás esetén.3	-0.062	0.061	-0.059	-1.020	0.308
	R KOCKÁZAT Ejtőernyőzni.3	-0.101	0.061	-0.105	-1.651	0.100
	R KOCKÁZAT Bungeejumpingozni egy magas hídról. 3	0.241	0.063	0.256	3.839	< .001
	R KOCKÁZAT Kis repülőgépet vezetni. 3	-0.075	0.056	-0.075	-1.340	0.181
	S KOCKÁZAT Beismerni egy barátomnak, hogy az ízlésem különbözik az övétől.3	0.055	0.056	0.049	0.977	0.330
	S KOCKÁZAT Egy hatósági személlyel összekülönbözni.3	0.011	0.066	0.009	0.162	0.871
	S KOCKÁZAT Izgalmasabb karrierbe kezdeni egy biztosabb karrirer helyett. 2	-0.086	0.078	-0.060	-1.103	0.271
	S KOCKÁZAT Egy kellemetlen témáról beszélni egy munkahelyi megbeszélésen. 2	0.095	0.067	0.080	1.430	0.154
	S KOCKÁZAT A családtól és a rokonoktól távolra költözni. 3	-0.054	0.060	-0.048	-0.908	0.364
	S KOCKÁZAT Harmincötévesen új karrierbe kezdeni. 2	0.143	0.072	0.114	1.982	0.048

Forrás: saját szerkesztés a minta alapján

A beleegyezés nélküli eszközhasználat (4. táblázat) gyenge kapcsolatot mutatott etikai jellegű elemekkel, azonban ez sem jelentett konzisztens prediktív struktúrát.

4. táblázat Regresszió számítás eredménye a beleegyezés nélküli használat kérdése és a további kérdések között

Model Summary - ICT KOCKÁZAT Hagyni, hogy más használja a telefonját a tudta nélkül. 3

Model	R	R^2	Adjusted R^2	RMSE
H_0	0.000	0.000	0.000	1.566
H_1	0.552	0.305	0.248	1.358

ANOVA

Model		Sum of Squares	df	Mean Square	F	p
H_1	Regression	266.259	27	9.861	5.345	< .001
	Residual	606.956	329	1.845		
	Total	873.216	356			

Note. The intercept model is omitted, as no meaningful information can be shown.

Coefficients

Model		Unstandardized	Standard Error	Standardized	t	p
H_0	(Intercept)	3.843	0.083		46.364	< .001
H_1	(Intercept)	0.501	0.468		1.071	0.285
	E KOCKÁZAT Megkérdőjelezhető költségeket leírni az adóbevallásban.3	0.049	0.069	0.043	0.716	0.475
	E KOCKÁZAT Más munkáját a sajátomként felhasználni. 3	0.017	0.061	0.015	0.281	0.779
	E KOCKÁZAT Egy barát titkát kifecsegni. 3	0.232	0.059	0.214	3.954	< .001
	E KOCKÁZAT Egy kisgyereket magára hagyni otthon egyedül, amíg elmegy a boltba. 3	0.069	0.055	0.069	1.257	0.210
	E KOCKÁZAT Egy 50.000 Ft-ot tartalmazó pénztárcát megtartani. 2	0.042	0.050	0.045	0.841	0.401
	F KOCKÁZAT A napi jövedelmem feltenni lóversenyre. 3	0.009	0.069	0.008	0.127	0.899
	F KOCKÁZAT Az éves jövedelmem 10% -át befektetni egy mérsékelt növekedésű, diverzifikált alapba. 3	-0.032	0.063	-0.027	-0.498	0.619
	F KOCKÁZAT Egy napi jövedelmet feltenni egy kockázatos pókerjátszmában. 3	-0.008	0.070	-0.007	-0.112	0.911
	F KOCKÁZAT Az éves jövedelmem 5%-át egy magaskockázatú befektetésbe fektetni. 3	-0.132	0.062	-0.119	-2.134	0.034
	F KOCKÁZAT Egy napi jövedelmet feltenni egy sportmérközésre. 3	0.143	0.069	0.138	2.065	0.040
	F KOCKÁZAT Az éves jövedelmem 10%-át egy új üzleti lehetőségbe fektetni. 3	-0.059	0.066	-0.051	-0.898	0.370
	H KOCKÁZAT Túl sok alkoholt fogyasztani egy társadalmi eseményen, például egy esküvőn. 3	-0.002	0.051	-0.002	-0.035	0.972
	H KOCKÁZAT Biztonságiöv viselése nélkül vezetni. 3	0.021	0.068	0.020	0.308	0.758
	H KOCKÁZAT Bukósisak nélkül motorozni.3	-6.432×10^{-4}	0.078	-5.340×10^{-4}	-0.008	0.993
	H KOCKÁZAT Naptej nélkül napozni. 3	0.092	0.055	0.087	1.671	0.096
	H KOCKÁZAT Hazasétálni egyedül egy nem biztonságos városrészben. 3	0.155	0.063	0.133	2.438	0.015
	R KOCKÁZAT Olyan sípályán lesiklani, ami meghaladja a képességeim. 3	0.112	0.064	0.099	1.750	0.081
	R KOCKÁZAT Vadvízi evezésre menni tavasszal, nagy vízállás esetén.3	0.002	0.063	0.002	0.040	0.968
	R KOCKÁZAT Ejtőernyőzni.3	-0.053	0.063	-0.053	-0.829	0.408
	R KOCKÁZAT Bungeejumpingozni egy magas hídról. 3	0.081	0.065	0.084	1.242	0.215
	R KOCKÁZAT Kis repülőgépet vezetni. 3	-0.136	0.058	-0.133	-2.355	0.019
	S KOCKÁZAT Beismerni egy barátomnak, hogy az ízlésem különbözik az övétől.3	0.037	0.058	0.032	0.630	0.529
	S KOCKÁZAT Egy hatósági személlyel összekülönbözni.3	-0.034	0.068	-0.029	-0.506	0.613
	S KOCKÁZAT Izgalmasabb karrierbe kezdeni egy biztosabb karrirer helyett. 2	0.079	0.080	0.054	0.977	0.329
	S KOCKÁZAT Egy kellemetlen témáról beszélni egy munkahelyi megbeszélésen. 2	0.137	0.069	0.113	1.999	0.046
	S KOCKÁZAT A családtól és a rokonoktól távolra költözni. 3	0.079	0.062	0.068	1.270	0.205
	S KOCKÁZAT Harmincötévesen új karrierbe kezdeni. 2	0.014	0.075	0.011	0.193	0.847

Forrás: saját szerkesztés a minta alapján

A vállalati adatok saját tulajdonú eszközre történő másolása (5. táblázat) esetében egy gyenge pozitív kapcsolat volt kimutatható az adóbevallási szabályszegésre vonatkozó elemmel. Ez etikai dimenzióval való részleges átfedést sugallhat, azonban a kapcsolat gyenge és nem általánosítható.

5. táblázat Regresszió számítás eredménye a vállalati adatok saját tulajdonú okostelefonra történő másolásának kérdése és a további kérdések között

Model Summary - ICT KOCKÁZAT Munkahelyi adatok, dokumentumok mobiltelefonra másolása. 3

Model	R	R^2	Adjusted R^2	RMSE
H_0	0.000	0.000	0.000	1.702
H_1	0.529	0.280	0.221	1.502

ANOVA

Model		Sum of Squares	df	Mean Square	F	p
H_1	Regression	288.405	27	10.682	4.734	< .001
	Residual	742.407	329	2.257		
	Total	1030.812	356			

Note. The intercept model is omitted, as no meaningful information can be shown.

Coefficients

Model		Unstandardized	Standard Error	Standardized	t	p
H_0	(Intercept)	3.868	0.090		42.953	< .001
H_1	(Intercept)	-0.328	0.517		-0.634	0.527
	E KOCKÁZAT Megkérdőjelezhető költségeket leírni az adóbevallásban.3	0.269	0.076	0.218	3.548	< .001
	E KOCKÁZAT Más munkáját a sajátomként felhasználni. 3	0.127	0.067	0.105	1.880	0.061
	E KOCKÁZAT Egy barát titkát kifecsegni. 3	0.067	0.065	0.057	1.028	0.305
	E KOCKÁZAT Egy kisgyereket magára hagyni otthon egyedül, amíg elmegy a boltba. 3	0.126	0.061	0.117	2.076	0.039
	E KOCKÁZAT Egy 50.000 Ft-ot tartalmazó pénztárcát megtartani. 2	0.010	0.055	0.010	0.184	0.854
	F KOCKÁZAT A napi jövedelmem feltenni lóversenyre. 3	0.110	0.077	0.093	1.433	0.153
	F KOCKÁZAT Az éves jövedelmem 10% -át befektetni egy mérsékelt növekedésű, diverzifikált alapba. 3	0.037	0.070	0.029	0.533	0.595
	F KOCKÁZAT Egy napi jövedelmet feltenni egy kockázatos pókerjátszmában. 3	-0.121	0.077	-0.103	-1.570	0.117
	F KOCKÁZAT Az éves jövedelmem 5%-át egy magaskockázatú befektetésbe fektetni. 3	0.156	0.069	0.129	2.282	0.023
	F KOCKÁZAT Egy napi jövedelmet feltenni egy sportmérkőzésre. 3	-0.033	0.077	-0.029	-0.429	0.668
	F KOCKÁZAT Az éves jövedelmem 10%-át egy új üzleti lehetőségbe fektetni. 3	0.104	0.073	0.083	1.430	0.154
	H KOCKÁZAT Túl sok alkoholt fogyasztani egy társadalmi eseményen, például egy esküvőn. 3	-0.015	0.057	-0.014	-0.263	0.793
	H KOCKÁZAT Biztonságiöv viselése nélkül vezetni. 3	0.010	0.076	0.009	0.138	0.891
	H KOCKÁZAT Bukósisak nélkül motorozni.3	-0.050	0.086	-0.038	-0.581	0.561
	H KOCKÁZAT Naptej nélkül napozni. 3	-0.013	0.061	-0.011	-0.215	0.830
	H KOCKÁZAT Hazasétálni egyedül egy nem biztonságos városrészben. 3	0.130	0.070	0.103	1.853	0.065
	R KOCKÁZAT Olyan sípályán lesiklani, ami meghaladja a képességeim. 3	-0.122	0.071	-0.099	-1.714	0.087
	R KOCKÁZAT Vadvízi evezésre menni tavasszal, nagy vízállás esetén.3	0.021	0.069	0.018	0.299	0.765
	R KOCKÁZAT Ejtőernyőzni.3	0.123	0.070	0.114	1.751	0.081
	R KOCKÁZAT Bungeejumpingozni egy magas hídról. 3	-0.009	0.072	-0.009	-0.128	0.898
	R KOCKÁZAT Kis repülőgépet vezetni. 3	0.003	0.064	0.002	0.042	0.967
	S KOCKÁZAT Beismerni egy barátomnak, hogy az ízlésem különbözik az övétől.3	-0.044	0.064	-0.036	-0.687	0.493
	S KOCKÁZAT Egy hatósági személlyel összekülönbözni.3	0.032	0.075	0.025	0.422	0.673
	S KOCKÁZAT Izgalmasabb karrierbe kezdeni egy biztosabb karrirer helyett. 2	-0.044	0.089	-0.028	-0.492	0.623
	S KOCKÁZAT Egy kellemetlen témáról beszélni egy munkahelyi megbeszélésen. 2	0.208	0.076	0.157	2.730	0.007
	S KOCKÁZAT A családtól és a rokonoktól távolra költözni. 3	-0.031	0.068	-0.025	-0.454	0.650
	S KOCKÁZAT Harmincötévesen új karrierbe kezdeni. 2	0.012	0.083	0.008	0.141	0.888

Forrás: saját szerkesztés a minta alapján

Az eredmények alapján az első hipotézis egyértelműen elfogadható: az IT-biztonsági kockázatvállalás nem vezethető vissza az eredeti DOSPERT doménstruktúrára.

Ez az eredmény több szempontból jelentős:

- Igazolja az IT-domén beemelésének módszertani szükségességét.
- Alátámasztja, hogy az információbiztonsági döntések kontextus-specifikusak.
- Empirikusan is megerősíti, hogy a technológiai kockázatok észlelése eltér a fizikai, etikai vagy pénzügyi kockázatokétól.

Az IT-kockázatvállalás tehát nem pusztán az általános kockázatvállalási attitűd egy alskálája, hanem önálló, kontextusfüggő konstrukcióként értelmezendő.

3.3.1 Az IT-biztonsági kockázatpercepció

H2: Az IT-biztonsági domén észlelt kockázati szintje nem a legmagasabb a vizsgált kockázati domének között.

A második hipotézis a disszertáció egyik kulcskérdésére irányult: vajon az információbiztonsági kockázatok észlelt súlya a vizsgált mintákban kiemelkedőnek tekinthető-e, vagy inkább a kockázati mezőny közép- vagy alsó szegmensében helyezkedik el. A kérdés túlmutat a puszta rangsoroláson, hiszen az észlelt kockázat a viselkedési döntések egyik legfontosabb meghatározója. Amennyiben az IT-biztonsági kockázatok nem jelennek meg a hallgatók percepciójában magas kockázati kategóriaként, az közvetlen következményekkel jár a biztonságtudatossági programok tervezésére és a BYOD-stratégiák kialakítására nézve.

Az elemzés első lépéseként doménenként számoltam ki az észlelt kockázat átlagértékeit. Az IT-domén öt elemének átlaga külön-külön, valamint aggregált formában is elemzésre került. Az eredmények azt mutatták, hogy az IT-biztonsági domén nem a legmagasabb észlelt kockázati értéket mutatta a vizsgált hat terület közül.

Az IT-biztonsági kérdések részletes átlagértékeit szakonként a következő táblázat tartalmazza:

6. táblázat Az IT biztonsággal kapcsolatos érzékeltkockázat értékének átlaga szakonként

	Gazdaságinformatikus Bsc	Gépészmérnök BSc	Villamosmérnök BSc
Továbbítana-e vállalati adatokat a privát e-mail címére?	4,77	4,86	4,93
Csatlakozna-e nyilvános, nyílt WiFi-hez?	3,8	3,56	3,97
Engedné-e, hogy valaki az Ön előzetes beleegyezése nélkül használja az Ön okoseszközét?	4,51	4,72	5,26
Használná-e a PIN kódját / jelszavát / feloldási mintáját mások előtt?	4,98	5,06	5,51
Másolna-e vállalati adatokat a saját tulajdonú okostelefonjára?	4,8	4,62	5,04

Forrás: saját szerkesztés az SPSS segítségével végzett statisztikai adatelemzés alapján (N=357)

A táblázat adatai alapján megállapítható, hogy az egyes IT domén elemei közül a legmagasabb észlelt kockázat a jelszó/PIN mások előtti használata volt (5,51 maximális átlagérték), míg a legalacsonyabb értéket a nyílt WiFi-hálózathoz való csatlakozás kapta (3,56–3,97 közötti értékek). Ez különösen figyelemre méltó, mivel a szakirodalom az utóbbi viselkedést jelentős információbiztonsági kockázatként azonosítja.

Ez az eredmény már önmagában is arra utal, hogy az IT-kockázatok észlelése nem egységes: a közvetlen, látható, személyes kontrollhoz kötött kockázatok (pl. jelszóhasználat) magasabb értékelést kapnak, míg az infrastrukturális jellegű veszélyek (pl. nyílt hálózat) alacsonyabb percepciós súlyt.

A doménenkénti összehasonlítás a teljes DOSPERT-struktúra figyelembevételével történt. Az észlelt kockázatok doménenkénti megoszlását az alábbi táblázat szemlélteti:

7. táblázat Az érzékelt kockázatok megoszlása doménenként és szakonként

Szak	Statisztika	Szociális	Pénzügyi	Egészség és biztonság	Etikai	Szabadidős	IKT biztonság
Gazdaság-informatikus	Átlag	3,8626	4,6112	4,8355	5,2336	4,6579	4,5738
	N	107	107	107	107	107	107
	Szórás	0,7888	1,0097	1,0550	1,0387	1,2050	1,1088
Villamosmérnöki	Átlag	4,0630	4,7815	5,1389	5,4500	4,5704	4,9407
	N	108	108	108	108	108	108
	Szórás	0,7540	0,8242	0,8461	0,9261	0,9018	1,0355
Gépészmérnöki	Átlag	3,9892	4,5183	4,9806	5,2387	4,5183	4,5656
	N	93	93	93	93	93	93
	Szórás	0,6068	0,9013	0,9113	0,8440	0,8337	0,9653
Teljes minta	Átlag	3,9711	4,6429	4,9857	5,3110	4,5851	4,7000
	N	308	308	308	308	308	308
	Szórás	0,7283	0,9187	0,9481	0,9463	0,9982	1,0531

Forrás: saját szerkesztés az SPSS segítségével végzett statisztikai adatelemzés alapján (N=308)

A 7. táblázat alapján megállapítható, hogy az etikai, valamint az egészség/biztonsági domén magasabb átlagos észlelt kockázati értékeket mutatott, mint az IT-domén. Az IT-biztonsági terület a vizsgált mintában a középmezőnyben vagy annak alsó részében helyezkedett el.

Ez az eredmény különösen jelentős abból a szempontból, hogy a vizsgálatban részt vevő hallgatók műszaki és informatikai képzésben részesültek, így feltételezhető lett volna magasabb érzékenység az IT-biztonsági kérdések iránt. Az empirikus adatok azonban nem támasztották alá ezt a feltételezést.

3.3.2 A képzési háttér és a szakirányú szocializáció szerepe a kockázatértékelésben

A doménpozíciók szakok szerinti összevetése további árnyalást tett lehetővé. A gazdaságinformatikus hallgatók esetében az IT-domén az utolsó előtti helyen szerepelt, ami különösen figyelemre méltó, tekintettel arra, hogy ezen hallgatók képzésük során közvetlenül találkoznak információbiztonsági kérdésekkel. A szakok közötti különbségek statisztikai vizsgálatát a következő táblázatban mutatom be:

8. táblázat A T-próba eredménye a gazdaságinformatikus és a villamosmérnök hallgatók vizsgálatára

Domain	Varianciák	Levene: F	Levene: Szign.	t	df	kétoldali szignifikancia	Átlagok különbsége	Különbség std. hibája	95% KI (Alsó határ)	95% KI (Felső határ)
Egészség és biztonság	Egyenlő varianciák feltételezve	2,139	0,145	-2,327	213	0,021	-0,30337	0,13037	-0,56035	-0,04639
	Egyenlő varianciák nem feltételezve			-2,325	202,623	0,021	-0,30337	0,1305	-0,56069	-0,04606
IKT biztonság	Egyenlő varianciák feltételezve	0,114	0,736	-2,508	213	0,013	-0,36691	0,14631	-0,65531	-0,07851
	Egyenlő varianciák nem feltételezve			-2,507	211,725	0,013	-0,36691	0,14635	-0,65541	-0,07841

Forrás: saját szerkesztés az SPSS segítségével végzett statisztikai adatelemzés alapján

H3: A különböző szakok hallgatói között szignifikáns különbség mutatható ki az IT-biztonsági kockázatok észlelésében.

A harmadik hipotézis abból az elméleti feltevésből indult ki, hogy a formális képzés – különösen a műszaki és informatikai területen – befolyásolhatja a kockázatészlelés mintázatát. A biztonságtudatossági szakirodalom gyakran implicit módon feltételezi, hogy a magasabb szintű technikai tudás együtt jár a kockázatok pontosabb felismerésével és magasabb észlelt veszélyérzettel. Ennek empirikus vizsgálata különösen fontos volt a jelen kutatásban, mivel a minta döntően műszaki felsőoktatásban részt vevő hallgatókból állt.

A szakok szerinti megoszlást és a minta struktúráját az alábbi táblázat tartalmazza:

9. táblázat A válaszadó hallgatók által tanult szakok megoszlása a mintában

Szak	fő
Gépészmérnök BSc	96
Mechatronikai mérnök BSc	1
Villamosmérnöki szak BSc	135
Gazdaságinformatikus BSc	72
Műszaki Menedzser BSc	2
Gazdálkodási és menedzsment BSc	28
Kereskedelem és marketing BSc	17
Kereskedelem és marketing felsőoktatási szakképzés	3
Gazdálkodási és menedzsment felsőoktatási szakképzés	3

Forrás: saját szerkesztés a minta alapján

A minta összetétele alapján a legnagyobb csoportot a villamosmérnök és a gépészmérnök hallgatók alkották, míg a gazdaságinformatikus hallgatók szintén jelentős arányban szerepeltek. A szakok közötti összehasonlítás ezért módszertanilag megalapozott volt.

Az IT-biztonsági kérdések átlagértékeinek szakonkénti bontását korábban az 6. táblázat (lásd 72 oldal) mutatta be, azonban ebben a szakaszban már nem csupán leíró, hanem összehasonlító elemzés történik.

10. táblázat Az IT biztonsággal kapcsolatos érzékeltkockázat értékének átlaga szakonként

	Gazdaságinformatikus Bsc	Gépészmérnök BSc	Villamosmérnöki BSc
Továbbítana-e vállalati adatokat a privát e-mail címére?	4,77	4,86	4,93
Csatlakozna-e nyilvános, nyílt WiFi-hez?	3,8	3,56	3,97
Engedné-e, hogy valaki az Ön előzetes beleegyezése nélkül használja az Ön okoseszközét?	4,51	4,72	5,26
Használná-e a PIN kódját / jelszavát / feloldási mintáját mások előtt?	4,98	5,06	5,51
Másolna-e vállalati adatokat a saját tulajdonú okostelefonjára?	4,8	4,62	5,04

Forrás: saját szerkesztés a minta alapján

Az adatok alapján nem rajzolódott ki egyértelmű mintázat, amely szerint az informatikai vagy gazdaságinformatikus képzésben részt vevő hallgatók minden IT domén elemei esetében magasabb észlelt kockázati értéket adtak volna. Bizonyos esetekben a villamosmérnök hallgatók mutattak magasabb átlagértékeket, ami ellentmondott az előzetes feltételezésnek.

Ez az eredmény már előrevetítette, hogy a szak szerinti különbségek nem lesznek egyértelműen strukturális jellegűek.

A szakok közötti különbségek tesztelése független mintás t-próbával történt.

11. táblázat A T-próba eredménye a hallgatók vizsgálatára

Szak	Statisztika	Szociális	Pénzügyi	Egészség és biztonság	Etikai	Szabadidős	IKT biztonság
Gazdaság-informatikus	Átlag	3,8626	4,6112	4,8355	5,2336	4,6579	4,5738
	N	107	107	107	107	107	107
	Szórás	0,7888	1,0097	1,0550	1,0387	1,2050	1,1088
Villamosmérnöki	Átlag	4,0630	4,7815	5,1389	5,4500	4,5704	4,9407
	N	108	108	108	108	108	108
	Szórás	0,7540	0,8242	0,8461	0,9261	0,9018	1,0355
Gépészmérnöki	Átlag	3,9892	4,5183	4,9806	5,2387	4,5183	4,5656
	N	93	93	93	93	93	93
	Szórás	0,6068	0,9013	0,9113	0,8440	0,8337	0,9653
Teljes minta	Átlag	3,9711	4,6429	4,9857	5,3110	4,5851	4,7000
	N	308	308	308	308	308	308
	Szórás	0,7283	0,9187	0,9481	0,9463	0,9982	1,0531

Forrás: saját szerkesztés az SPSS segítségével végzett statisztikai adatelemzés alapján

A t-próba eredményei azt mutatták, hogy az IT-domén tekintetében csak bizonyos kérdések esetében volt kimutatható szignifikáns különbség, és ezek sem alkottak konzisztens mintázatot. Az informatikai képzésben részt vevő hallgatók nem mutattak minden esetben magasabb kockázatészlelést, sőt, egyes kérdésekben alacsonyabb átlagértékeket adtak.

Ez az eredmény különösen fontos elméleti következtetéshez vezet: a technikai kompetencia nem azonos a kockázati érzékenységgel.

A harmadik hipotézis részleges igazolást nyert. Bár bizonyos szakpárok között kimutatható volt szignifikáns különbség, ezek nem voltak általánosíthatók az IT-domén egészére.

Ezért a H3 hipotézis nem tekinthető teljes mértékben igazoltnak.

Elméleti szempontból ez az eredmény azt sugallja, hogy a kockázatészlelés nem pusztán tudásfüggő konstrukció. A képzési háttér önmagában nem determinálja az IT-biztonsági veszélyek észlelésének szintjét. Ez összhangban áll a viselkedéstudományi megközelítésekkel, amelyek szerint a kockázatészlelést nemcsak a kognitív tudás, hanem az attitűdök, normák, tapasztalatok és személyes relevanciaérzet együttesen alakítják.

A műszaki vagy informatikai képzés tehát nem garantál magasabb IT-biztonsági kockázatészlelést, ami különösen fontos következtetés a felsőoktatási biztonságtudatossági programok tervezése szempontjából.

H4: Az IT-biztonsági kockázatok magasabb észlelése pozitív kapcsolatban áll a biztonságtudatos viselkedési gyakorlatok alkalmazásával.

3.3.3 A biztonságtudatosság és a technikai óvintézkedések kapcsolata

A negyedik hipotézis a disszertáció egyik legfontosabb viselkedéstudományi kérdésére irányult: Vajon az észlelt kockázat ténylegesen befolyásolja-e a biztonságtudatos viselkedést? A klasszikus racionális döntéselméleti modellek – beleértve az elvárt hasznosság elméletet és a kockázat–nyereség mérlegelési modelleket – azt feltételezik, hogy az egyén döntéseit a várható következmények és a szubjektíven észlelt kockázat súlyozása alakítja. Ennek megfelelően a magasabb észlelt veszélyérzetnek preventív magatartással kellene együtt járnia. A jelen vizsgálat ezt az összefüggést az IT-biztonsági domén elemei és konkrét biztonságtudatos gyakorlatok közötti kapcsolat elemzésével tesztelte. A statisztikai elemzés Spearman-féle rangkorrelációval történt, tekintettel a változók ordinális jellegére.

Az egyik legfontosabb eredmény a nyílt WiFi-hálózathoz való csatlakozás észlelt kockázata és a kétfaktoros hitelesítés használata közötti kapcsolat volt.

12. táblázat Összefüggés vizsgálata a nyílt WiFi hálózatokhoz való csatlakozás kockázatának érzése és a kétfaktoros hitelesítés használata között (n=357)

Statisztikai módszer	Változó	Mutató	**Kockázatérzet nyílt WiFi hálózatokhoz való csatlakozáskor**
Spearman-féle rho	**Kétfaktoros hitelesítés használata**	Korrelációs együttható	0,233**
		Kétoldali szignifikancia	0,008

**A korreláció 0,01-es szinten szignifikáns (kétoldali).

Forrás: saját szerkesztés az SPSS segítségével végzett statisztikai adatelemzés alapján

Az eredmények gyenge-közepes erősségű, szignifikáns pozitív kapcsolatot jeleztek. Ez azt jelenti, hogy azok a válaszadók, akik magasabb kockázatot tulajdonítottak a nyílt WiFi-hálózathoz való csatlakozásnak, nagyobb valószínűséggel alkalmaztak kétfaktoros hitelesítést. Ez az eredmény erős empirikus alátámasztást nyújt a hipotézis számára, és illeszkedik a racionális kockázatkezelési logikához: a magasabb észlelt veszély fokozott preventív magatartást eredményez.

A következő vizsgált kapcsolat a nyílt WiFi-használat és a rendszeres operációs rendszer-, illetve biztonsági frissítések telepítése között volt.

13. táblázat Összefüggés vizsgálata a nyílt WiFi hálózatokhoz való csatlakozás és az operációs rendszerek frissítése és biztonsági frissítések telepítése közötti összefüggés (n=357)

Statisztikai módszer	Változó	Mutató	**Nyílt WiFi hálózatokhoz való csatlakozás**
Spearman-féle rho	**Biztonsági frissítések telepítése az operációs rendszerhez**	Korrelációs együttható	-,205*
		Kétoldali szignifikancia	0,035

**A korreláció 0,05-ös szinten szignifikáns (kétoldali).

Forrás: saját szerkesztés az SPSS segítségével végzett statisztikai adatelemzés alapján

Az eredmények negatív irányú kapcsolatot mutattak a kockázatos viselkedés (nyílt WiFi-használat) és a frissítések rendszeres telepítése között. Azok, akik nagyobb valószínűséggel telepítették a frissítéseket, kisebb valószínűséggel csatlakoztak nyílt hálózathoz. Ez a kapcsolat ismételten azt mutatja, hogy a magasabb biztonságtudatosság és a magasabb észlelt kockázat preventív viselkedéssel társul.

3.3.4 Szervezeti adatkezelési rutinok és a biztonságtudatos gyakorlatok összefüggései

Az IT-biztonsági viselkedés komplexebb aspektusát mutatta a vállalati adatok saját okostelefonra történő másolása és a frissítések telepítése közötti kapcsolat.

14. táblázat Összefüggés vizsgálata a vállalati adatok privát okostelefonra történő másolása és a biztonsági frissítések és operációs rendszer frissítése között (n=357)

Statisztikai módszer	Változó	Mutató	**Vállalati adatok másolása privát okostelefonra**
Spearman-féle rho	**Biztonsági frissítések telepítése az operációs rendszerhez**	Korrelációs együttható	,197*
		Szign. (kétoldali)	0,021

**A korreláció 0,05-ös szinten szignifikáns (kétoldali).

Forrás: saját szerkesztés az SPSS segítségével végzett statisztikai adatelemzés alapján

Az eredmény itt árnyaltabb képet mutatott: bár a frissítések telepítése pozitív biztonságtudatos magatartás, a vállalati adatok saját eszközre másolása szervezeti szempontból kockázatos. A kapcsolat arra utal, hogy a technikai biztonságtudatosság nem feltétlenül jár együtt szervezeti szabálykövetéssel.

15. táblázat Összefüggés vizsgálata a vállalati adatok saját okostelefonra történő másolása és a jelszókezelő szoftver használata közötti összefüggés (n=357)

Statisztikai módszer	Változó	Mutató	**Vállalati adatok másolása privát okostelefonra**
Spearman-féle rho	**Jelszókezelő szoftver használata**	Korrelációs együttható	-,200*
		Szign. (kétoldali)	0,02

**A korreláció 0,05-ös szinten szignifikáns (kétoldali).

Forrás: saját szerkesztés az SPSS segítségével végzett statisztikai adatelemzés alapján

Az eredmény gyenge negatív kapcsolatot mutatott: akik nagyobb valószínűséggel használtak jelszókezelőt, kisebb valószínűséggel másoltak vállalati adatot saját eszközre. Ez a kapcsolat már egyértelműen a biztonságtudatos viselkedés konzisztens mintázatára utal.

16. táblázat Összefüggés vizsgálata a vállalati adatok privát e-mailben történő elküldése és az e-mailek csatolmányának biztonságtudatos kezelése között (n=357)

Statisztikai módszer	Változó	Mutató	**Vállalati adatok küldése privát e-mail címre**
Spearman-féle rho	**Biztonságtudatosság csatolmányt tartalmazó bejövő e-mailek kezelésekor**	Korrelációs együttható	-,231**
		Szign. (kétoldali)	0,009

**A korreláció 0,01-es szinten szignifikáns (kétoldali).

Forrás: saját szerkesztés az SPSS segítségével végzett statisztikai adatelemzés alapján

Az eredmények szerint azok, akik biztonságtudatosan kezelték az e-mail csatolmányokat, kisebb valószínűséggel küldtek vállalati adatot privát e-mail címre. Ez a kapcsolat különösen fontos, mivel a humán tényező az egyik legkritikusabb eleme az információbiztonsági incidenseknek. A bemutatott korrelációs eredmények alapján a H4 hipotézist elfogadtam. Az IT-biztonsági kockázatok magasabb észlelése több esetben szignifikáns, irányhelyes kapcsolatot mutatott a biztonságtudatos viselkedési gyakorlatokkal.

Ugyanakkor az összefüggések többsége gyenge vagy közepes erősségű volt, ami arra utal, hogy az attitűd és a viselkedés kapcsolata nem teljesen lineáris. A kockázatészlelés fontos, de nem kizárólagos magyarázó tényező. Ez az eredmény megerősíti a humán tényező szerepét az információbiztonságban, és empirikusan alátámasztja, hogy a percepció alakítása – például oktatás és tudatosságnövelés révén – befolyásolhatja a viselkedést.

H5: A technikai biztonságtudatosság egyes formái együtt járhatnak BYOD-kontextusban magasabb szervezeti kockázatvállalási hajlandósággal.

3.3.5 A biztonságtudatossági paradoxon és a szervezeti kockázatvállalás

Az ötödik hipotézis a kutatás egyik legösszetettebb és elméletileg legérdekesebb kérdését vizsgálta. A korábbi hipotézisek elsősorban arra irányultak, hogy az IT-biztonsági kockázatészlelés elkülönül-e az általános kockázatvállalási struktúrától, illetve, hogy az észlelt kockázat együtt jár-e preventív viselkedéssel. A H5 azonban egy másik irányból közelített: vajon előfordulhat-e, hogy a technikai értelemben vett biztonságtudatosság bizonyos elemei együtt járnak szervezeti szempontból kockázatos magatartással? A kérdés különösen releváns BYOD-környezetben, ahol az egyéni eszközhasználat és a vállalati adatkezelés határa elmosódik. A technikailag kompetens felhasználó magabiztosabban kezeli eszközét, rendszeresen telepít frissítéseket, használ jelszókezelőt, ugyanakkor éppen ezen kompetenciaérzet miatt nagyobb valószínű-

séggel használja saját eszközét vállalati célokra is. Ez a jelenség potenciálisan magasabb szervezeti kockázatot eredményezhet.

A hipotézis vizsgálatának központi változója a „vállalati adatok saját tulajdonú okostelefonra történő másolása” elem volt, amely BYOD-kontextusban egyértelműen szervezeti kockázati magatartásként értelmezhető. Az elemzés során ezt az elemet vetettük össze különböző technikai biztonságtudatos viselkedési változókkal. Az első fontos eredmény a rendszeres biztonsági frissítések telepítése és a vállalati adatok privát emailcímre való továbbítása közötti kapcsolat volt, lásd 1. táblázat Regresszió számítás eredménye a privát e-mail címre továbbított vállalati adatok kérdése és a további kérdések között 67. oldalon.

Az eredmények gyenge pozitív kapcsolatot mutattak a frissítések telepítése és a vállalati adatok saját eszközre másolása között. Ez azt jelenti, hogy azok a válaszadók, akik rendszeresen gondoskodtak eszközeik technikai biztonságáról, nagyobb valószínűséggel másoltak vállalati adatokat saját tulajdonú eszközükre. Ez az eredmény első látásra ellentmondásosnak tűnhet, hiszen a frissítések telepítése klasszikus biztonságtudatos magatartás. Ugyanakkor a jelenség értelmezhető úgy, hogy a technikai kompetencia növeli az eszközhasználati önbizalmat, ami a vállalati kontrollmechanizmusok részleges megkerüléséhez vezethet.

A második vizsgált kapcsolat a jelszókezelő szoftver használata és a vállalati adatok saját eszközre másolása között volt. Lásd 2. táblázat Regresszió számítás eredménye a nyilvánosan elérhető nyílt WiFi hálózatokhoz való csatlakozás kérdése és a további kérdések között, a 68. oldalon.

Ebben az esetben gyenge negatív kapcsolat volt megfigyelhető: akik nagyobb valószínűséggel használtak jelszókezelőt, kisebb valószínűséggel másoltak vállalati adatokat saját eszközre. Ez az eredmény azt mutatja, hogy a technikai biztonságtudatosság nem homogén konstrukció. Egyes elemei (például jelszókezelő használat) a szervezeti szempontból is biztonságos viselkedéssel járnak együtt, míg más elemei (például frissítések telepítése és eszközhasználati magabiztosság) együtt járhatnak magasabb szervezeti kockázatvállalással.

3.3.6 A döntéshozatali modell statisztikai verifikációja és regressziós elemzése

A vállalati adatok saját eszközre másolása kérdés regressziós eredményei korábban már bemutatásra kerültek. Lásd 5. táblázat Regresszió számítás eredménye a vállalati adatok saját tulajdonú okostelefonra történő másolásának kérdése és a további kérdések között 71. oldalon.

A regressziós modellben az IT biztonsági domén elemei közötti kapcsolat gyenge volt, azonban kimutatható volt kapcsolat etikai jellegű elemekkel (például adóbevallási szabályszegés). Ez arra utalhat, hogy a vállalati adatmásolás nem kizárólag technikai kompetenciával, hanem normatív attitűdökkel is összefügg.

A H5 hipotézis részben igazoltnak tekinthető. Az eredmények azt mutatták, hogy a technikai biztonságtudatosság egyes formái együtt járhatnak szervezeti szempontból kockázatos magatartással, különösen a BYOD-kontextusban.

Ugyanakkor a kapcsolat nem volt egyértelműen lineáris vagy minden technikai viselkedésre kiterjedő. Inkább arról beszélhetünk, hogy a biztonságtudatosság többdimenziós konstrukció:

- van technikai biztonságtudatosság,
- van szervezeti szabálykövetés,
- és van normatív-etikai attitűd.

E dimenziók nem feltétlenül mozognak együtt.

Ez az eredmény különösen fontos a BYOD-stratégia szempontjából. A szervezet nem feltételezheti, hogy a technikailag kompetens munkavállaló automatikusan alacsonyabb szervezeti kockázatot jelent. A technikai tudás növelheti az eszközhasználat önállóságát és intenzitását, ami szabályozás hiányában kockázati tényezővé válhat.

A H5 eredménye így közvetlenül visszacsatol a disszertáció BYOD-stratégiai fejezeteihez: a technikai kontroll (MDM, frissítések, autentikáció) önmagában nem elegendő, szükséges a szervezeti normák, jogosultságkezelés és kontrollmechanizmusok egyértelmű meghatározása.

H6: Az IT-biztonsági döntésekben az észlelt haszon standardizált regressziós súlya szignifikánsan meghaladja az észlelt kockázat abszolút értékű regressziós súlyát.

A hatodik hipotézis az információbiztonsági döntések belső súlyozási szerkezetének vizsgálatára irányult. A korábbi hipotézisek a kockázati döntések általános mintázatát és doménközi stabilitását elemezték, míg a H6 kifejezetten az IT-biztonsági kontextuson belüli regressziós súlyok relatív nagyságára fókuszált. A kérdés az volt, hogy az IT-biztonsági döntésekben az észlelt haszon és az észlelt kockázat integrációja kiegyensúlyozott-e, vagy strukturális aszimmetria figyelhető meg a két komponens között.

Kiindulópontként a globális regressziós modell eredményei szolgáltak, amelyek szerint a cselekvési valószínűség varianciájának 58,2%-át magyarázta a modell ($R^2 = 0,582$; $F(2, 769) = 535,73$; $p < 0,001$). A standardizált regressziós együtthatók jelentős különbséget mutattak: az észlelt haszon $\beta = 0,727$ ($p < 0,001$), míg az észlelt kockázat $\beta = -0,077$ ($p = 0,003$) volt. Az abszolút értékek aránya ($0,727 / 0,077 \approx 9,44$) azt jelezte, hogy a haszon hatása közel tízszerese a kockázat hatásának. Ez a globális mintázat már önmagában erős aszimmetrikus súlyozásra utal.

A H6 azonban kifejezetten az IT-biztonsági doménre vonatkozott, ezért a doménszintű regressziós modell eredményei tekintendők döntőnek. A B-doménben (IT-biztonsági kontextus) a modell magyarázóereje $R^2 = 0,541$ volt, ami azt jelenti, hogy a cselekvési valószínűség varianciájának 54,1%-át magyarázta a két percepciós dimenzió. A standardizált regressziós együtthatók itt is markáns különbséget mutattak: az észlelt haszon $\beta = 0,679$, míg az észlelt kockázat $\beta = -0,125$ volt. Az abszolút értékek aránya ($0,679 / 0,125 \approx 5,43$) azt jelzi, hogy az IT-biztonsági döntésekben az észlelt haszon hatása több mint ötszöröse az észlelt kockázat hatásának.

Ez az eltérés nem pusztán statisztikai szignifikanciát jelent, hanem a döntési súlyozás strukturális aszimmetriáját tükrözi. Bár az észlelt kockázat negatív irányú hatása kimutatható, annak nagyságrendje lényegesen kisebb, mint az észlelt haszon pozitív hatása. A cselekvési valószínűséget tehát elsődlegesen az észlelt előnyök „húzzák” felfelé, míg a kockázat inkább korrekciós jellegű tényezőként működik.

Az IT-biztonsági kontextus sajátosságai – különösen a BYOD-helyzetekben megjelenő azonnali kényelmi és hatékonysági előnyök – jól illeszkednek ehhez az empirikus mintázathoz. A biztonsági incidensek potenciális következményei gyakran időben távoliak és absztraktak, míg az előnyök közvetlenül tapasztalhatók, ami magyarázhatja a haszon regressziós dominanciáját.

A bemutatott doménszintű eredmények alapján a H6 hipotézis egyértelmű empirikus alátámasztást nyert. Az IT-biztonsági döntésekben az észlelt haszon standardizált regressziós súlya szignifikánsan és nagyságrendileg is meghaladja az észlelt kockázat abszolút értékű regressziós súlyát. A döntési architektúra tehát nem kiegyensúlyozott nyereség–veszteség integrációként írható le, hanem haszon-domináns struktúrát mutat.

Elméleti szempontból ez az eredmény finomítja a domén-specifikus kockázatelmélet információbiztonsági alkalmazását, mivel arra utal, hogy a veszteségelkerülési mechanizmusok önmagukban nem dominálják a döntési folyamatot. Gyakorlati implikációként pedig az következik, hogy a biztonságtudatossági intervenciók hatékonysága korlátozott lehet, ha kizárólag a

veszélyek hangsúlyozására épülnek. Amennyiben a döntési struktúra haszon-domináns, úgy a beavatkozásoknak a biztonságos viselkedéshez kapcsolódó előnyök explicitté tételére is ki kell terjedniük.

H7: Az észlelt haszon és az észlelt kockázat közötti súlyozási aszimmetria nem kizárólag az IT-biztonsági doménre jellemző, hanem más kockázati területeken is kimutatható.

A hetedik hipotézis a döntési súlyozási mechanizmus doménközi stabilitását vizsgálta. Míg a H6 az IT-biztonsági (B) doménben igazolta az észlelt haszon regressziós dominanciáját, a H7 arra irányult, hogy ez az aszimmetrikus súlyozás kizárólag az információbiztonsági kontextus sajátossága-e, vagy más kockázati területeken is megjelenik.

A vizsgálat során a cselekvési valószínűség standardizált mutatója szolgált függő változóként, míg az észlelt haszon és az észlelt kockázat standardizált értékei prediktorként szerepeltek minden egyes doménben külön-külön. A doménszintű regressziós modellek eredményei azt mutatták, hogy az aszimmetrikus súlyozás nem korlátozódik az IT-biztonsági kontextusra.

Az A-doménben (Nem IT-biztonsági kontextus elemei esetén) a modell a variancia 37,7%-át magyarázta ($R^2 = 0{,}377$), ahol az észlelt haszon standardizált regressziós együtthatója $\beta = 0{,}522$, míg az észlelt kockázaté $\beta = -0{,}212$ volt. A dominancia arány 2,46-nak adódott, ami azt jelzi, hogy a haszon hatása több mint kétszerese a kockázat hatásának.

A B-doménben (IT-biztonsági kontextus) a modell magyarázóereje $R^2 = 0{,}541$ volt, az észlelt haszon $\beta = 0{,}679$, az észlelt kockázat $\beta = -0{,}125$ értéket mutatott, a dominancia arány pedig 5,43 volt.

Mindkét doménben tehát egyértelműen kimutatható az észlelt haszon regressziós dominanciája. Annak vizsgálatára, hogy a dominancia mértéke különbözik-e a két domén között, páros mintás t-próba került alkalmazásra. Az eredmények nem mutattak szignifikáns különbséget ($t(771) = 0{,}711$; $p = 0{,}478$; Cohen $d = 0{,}026$), ami arra utal, hogy a haszon-dominancia mértéke statisztikailag nem tér el a vizsgált kockázati területek között.

A standardizált regressziós együtthatók különbségének formális tesztje ($Z = 21{,}84$; $p < 0{,}001$) megerősítette, hogy az aszimmetrikus súlyozás mindkét doménben szignifikáns. A multikollinearitási mutatók (maximális condition index = 1,50) stabil becslést jeleztek.

Az eredmények alapján megállapítható, hogy a haszon-dominancia nem kizárólag az IT-biztonsági döntések sajátossága, hanem más kockázati területen is strukturálisan megjelenik. A

döntési architektúra tehát nem kiegyensúlyozott nyereség–veszteség integrációként írható le, hanem több doménben is haszonorientált mintázatot mutat.

A H7 hipotézis ennek megfelelően empirikus alátámasztást nyert. Az észlelt haszon és az észlelt kockázat közötti súlyozási aszimmetria doménfüggetlen stabilitást mutat a vizsgált populációban, ami elméleti szempontból a kockázati döntések motivációs szerkezetének újraértelmezését indokolja. Gyakorlati implikációként ez arra utal, hogy a kockázatkommunikáció és viselkedésbefolyásolás nem alapozható kizárólag a veszélyek hangsúlyozására, mivel a döntési struktúrában a potenciális előnyök perceptuális ereje meghatározó szerepet játszik több kockázati területen is.

H8: Az életkor az általános kockázatvállalási dimenziók kontrollálása mellett szignifikáns magyarázóerővel bír az IT-biztonsági kockázatvállalás tekintetében.

A nyolcadik hipotézis annak vizsgálatára irányult, hogy az életkor önálló magyarázóerővel rendelkezik-e az IT-biztonsági kockázatvállalás tekintetében, amennyiben az általános kockázatvállalási dimenziók statisztikai kontroll alá kerülnek. A kérdés elméleti jelentősége abban áll, hogy tisztázható: az IT-biztonsági kockázatvállalás pusztán az általános kockázati attitűdök speciális megnyilvánulása-e, vagy demográfiai háttérváltozók is strukturáló szerepet játszanak benne.

A bivariáns korrelációs elemzés alapján az életkor és az IT-biztonsági kockázatvállalás között nem mutatkozott szignifikáns kapcsolat ($r = –0{,}004$; $p = 0{,}91$), ami önmagában nem indokolná az életkor szerepének hangsúlyozását. Ez azonban nem zárja ki, hogy az életkor hatása más változók kontrollálása mellett jelenjen meg.

A hierarchikus többszörös lineáris regressziós elemzés első lépésében az általános kockázatvállalási dimenziók – észlelt haszon, észlelt kockázat és cselekvési valószínűség – kerültek bevonásra kontrollváltozóként. A második lépésben az életkor és a nem került a modellbe. A teljes modell szignifikáns illeszkedést mutatott ($F(5, 766) = 137{,}20$; $p < 0{,}001$), és a variancia 47,2%-át magyarázta ($R^2 = 0{,}47$).

Az eredmények szerint az életkor a kontrollváltozók bevonása mellett is szignifikáns, pozitív kapcsolatban állt az IT-biztonsági kockázatvállalással ($\beta = 0{,}08$; $p = 0{,}002$). Ez azt jelenti, hogy az életkor növekedése – azonos szintű általános kockázatvállalási attitűdök mellett – magasabb IT-biztonsági kockázatvállalási hajlandósággal járt együtt.

Az eredmény különösen figyelemre méltó abból a szempontból, hogy az életkor hatása csak kontrollált modellben vált láthatóvá. Ez arra utal, hogy az életkor és az IT-biztonsági kockázatvállalás közötti kapcsolat nem közvetlen, hanem az általános kockázati dimenziókhoz viszonyított relatív pozíció mentén strukturálódik. Másképpen fogalmazva: az IT-domén nem redukálható, az általános kockázati attitűdök alapján előre nem jelezhető, mivel az életkor önálló, reziduális magyarázó tényezőként jelenik meg.

A H8 hipotézis ennek megfelelően empirikus alátámasztást nyert. Az életkor az általános kockázatvállalási dimenziók kontrollálása mellett is szignifikáns magyarázóerővel bír az IT-biztonsági kockázatvállalás modelljében, ami megerősíti az IT-domén részleges autonómiáját a kockázati döntéshozatal szerkezetében.

H9: A nem az általános kockázatvállalási dimenziók kontrollálása mellett is szignifikáns kapcsolatban áll az IT-biztonsági kockázatvállalással.

A kilencedik hipotézis a nem szerepét vizsgálta az IT-biztonsági kockázatvállalás magyarázatában, az általános kockázatvállalási dimenziók statisztikai kontrollja mellett. A kockázatpszichológiai szakirodalom számos területen dokumentál nemi különbségeket a kockázatvállalásban, ugyanakkor több empirikus vizsgálat rámutat arra, hogy ezek a különbségek részben az általános attitűdstruktúrára vezethetők vissza. A H9 célja annak tesztelése volt, hogy az IT-biztonsági kontextusban fennmarad-e az önálló nemi hatás, ha az észlelt haszon, az észlelt kockázat és a cselekvési valószínűség dimenziói kontrollálásra kerülnek.

A hierarchikus többszörös regressziós modell második lépésében a nem – binárisan kódolt változóként (1 = férfi, 2 = nő) – az általános kockázati dimenziókkal együtt került bevonásra. A teljes modell szignifikáns illeszkedést mutatott ($F(5, 766) = 137{,}20$; $p < 0{,}001$), és a függő változó varianciájának 47,2%-át magyarázta ($R^2 = 0{,}47$).

Az eredmények szerint a nem az általános kockázatvállalási dimenziók kontrollálása mellett is szignifikáns, pozitív kapcsolatban állt az IT-biztonsági kockázatvállalással ($\beta = 0{,}10$; $p < 0{,}001$). A kódolásból adódóan a pozitív regressziós együttható azt jelenti, hogy azonos kontrollváltozók mellett a női válaszadók magasabb IT-biztonsági kockázatvállalási értéket mutattak, mint a férfiak.

Ez az eredmény arra utal, hogy a nemi különbségek az IT-doménben nem redukálhatók pusztán az általános kockázati attitűdkülönbségekre. A demográfiai háttérváltozó reziduális hatása arra enged következtetni, hogy az IT-biztonsági döntések strukturálását olyan tényezők is

befolyásolhatják, mint a technológiai önbizalom, a digitális szocializáció mintázatai vagy az eltérő normatív értelmezési keretek.

A H9 hipotézis ennek megfelelően empirikus alátámasztást nyert. A nem önálló magyarázó tényezőként jelenik meg az IT-biztonsági kockázatvállalás modelljében, ami megerősíti, hogy az IT-domén részben demográfiai háttérváltozók által strukturált döntési térként értelmezhető.

17. táblázat A hipotézisek összefoglaló táblázata

Kód	**Hipotézis leírása**	**Hipotézis vizsgálat eredménye**
H1	A DOSPERT eredeti doménjei nem képesek szignifikáns mértékben előre jelezni az IT-biztonsági kockázati kérdésekre adott válaszokat.	Elfogadva
H2	Az IT-biztonsági domén észlelt kockázati szintje nem a legmagasabb a vizsgált kockázati domének között.	Elfogadva
H3	A különböző szakok hallgatói között szignifikáns különbség mutatható ki az IT-biztonsági kockázatok észlelésében.	Részben elfogadva (nem minden területen és szakon igazolódott konzisztensen)
H4	Az IT-biztonsági kockázatok magasabb észlelése pozitív kapcsolatban áll a biztonságtudatos viselkedési gyakorlatok alkalmazásával.	Elfogadva
H5	A technikai biztonságtudatosság egyes formái együtt járhatnak BYOD-kontextusban magasabb szervezeti kockázatvállalási hajlandósággal.	Részben elfogadva
H6	Az IT-biztonsági döntésekben az észlelt haszon standardizált regressziós súlya szignifikánsan meghaladja az észlelt kockázat abszolút értékű regressziós súlyát.	Elfogadva
H7	Az észlelt haszon–kockázat súlyozási aszimmetriája nem kizárólag IT-biztonsági sajátosság, más doménekben is kimutatható.	Elfogadva
H8	Az életkor az általános kockázatvállalási dimenziók kontrollálása mellett szignifikáns magyarázóerővel bír az IT-biztonsági kockázatvállalás tekintetében.	Elfogadva
H9	A nem az általános kockázatvállalási dimenziók kontrollálása mellett is szignifikáns kapcsolatban áll az IT-biztonsági kockázatvállalással.	Elfogadva

Forrás: saját szerkesztés a kutatási eredmények alapján

Összegzésképpen a kutatás rávilágított, hogy az IT-biztonsági kockázatvállalás egy autonóm, kontextusfüggő terület, ahol a döntéseket elsősorban a várt előnyök (például kényelem, gyorsaság) dominálják a kockázatészleléssel szemben.

3.4 Tézisek

T1: Az IT-biztonsági kockázatvállalás mint önálló konstrukció

Empirikusan kimutattam, hogy az IT-biztonsági kockázatvállalás nem írható le megfelelően a DOSPERT eredeti doménstruktúrájával, és a technikai képzés, valamint az általános kockázatvállalási dimenziók kontrollálása mellett is szignifikáns szerepet játszanak demográfiai tényezők (életkor, nem). Eredményeim alapján az IT-biztonsági kockázatvállalás részben autonóm, kontextus-specifikus konstrukcióként értelmezhető. [P4][P12][P14][P24][P25]

T2: Az IT-biztonsági kockázatok percepciós pozíciója

Igazoltam, hogy az IT-biztonsági kockázatok észlelt szintje nem a legmagasabb a vizsgált kockázati területek között, hanem inkább a középmezőnyben vagy annak alsó szegmensében helyezkedik el, ami a digitális kockázatok relatív percepciós alulsúlyozottságára utal. [P2][P5][P6][P8][P16][P17]

T3: Kockázatpercepció és biztonságtudatos viselkedés kapcsolata

Empirikusan alátámasztottam, hogy az IT-biztonsági kockázatok magasabb észlelése több esetben szignifikáns, irányhelyes kapcsolatban áll a biztonságtudatos viselkedési gyakorlatok alkalmazásával, ugyanakkor az összefüggések erőssége mérsékelt, ami az attitűd és viselkedés közötti kapcsolat részleges jellegét jelzi. [P3][P13][P15][P18][P19]

T4: A technikai kompetencia és a szervezeti kockázat viszonya

Kimutattam, hogy a technikai biztonságtudatosság bizonyos formái BYOD-kontextusban együtt járhatnak szervezeti szempontból kockázatos magatartással, ami a technikai kompetencia és a szervezeti szabálykövetés közötti potenciális strukturális feszültségre utal. [P20][P21][P22][P23]

T5: Haszon-domináns döntési architektúra az IT-biztonsági döntésekben

Igazoltam, hogy az IT-biztonsági döntésekben az észlelt haszon hatása szignifikánsan meghaladja az észlelt kockázat hatását, és ez a súlyozási aszimmetria nem kizárólag az IT-biztonsági domén sajátossága, hanem más kockázati területeken is strukturálisan megjelenik. [P1][P7][P9][P10][P11]

18. táblázat A téziseket megalapozó hipotézisek és empírikus magyarázatuk táblázata

Kapcsolódó hipotézis(ek)	**Tézis szövege**	**Empirikus magyarázat**
H1, H3, H8, H9	T1 – Az IT-biztonsági kockázatvállalás mint önálló konstrukció Empirikusan kimutattam, hogy az IT-biztonsági kockázatvállalás nem írható le megfelelően a DOSPERT eredeti doménstruktúrájával, és a technikai képzés, valamint az általános kockázatvállalási dimenziók kontrollálása mellett is szignifikáns szerepet játszanak demográfiai tényezők (életkor, nem). Eredményeim alapján az IT-biztonsági kockázatvállalás részben autonóm, kontextus-specifikus konstrukcióként értelmezhető.	A H1 vizsgálata során az IT-biztonsági terület elemeire futtatott többszörös regresszióelemzések alacsony determinációs együtthatókat eredményeztek, az eredeti DOSPERT-doménváltozók többsége nem bizonyult szignifikáns prediktornak, és a kimutatható gyenge kapcsolatok sem alkottak konzisztens mintázatot. Ez arra utal, hogy az IT-biztonsági döntések nem vezethetők vissza az eredeti doménstruktúrára. A H3 eredményei szerint a különböző szakok hallgatói között csak részleges és nem konzisztens különbségek mutatkoztak az IT-kockázatok észlelésében, vagyis a technikai vagy informatikai képzés önmagában nem determinál magasabb kockázati érzékenységet. A H8 és H9 hierarchikus regressziós eredményei azt mutatták, hogy az életkor és a nem az általános kockázatvállalási dimenziók kontrollálása mellett is szignifikáns önálló magyarázóerővel bírnak az IT-biztonsági kockázatvállalás tekintetében. Mindez együtt az IT-domén részleges autonómiáját támasztja alá.
H2	T2 – Az IT-biztonsági kockázatok percepciós pozíciója Igazoltam, hogy az IT-biztonsági kockázatok észlelt szintje nem a legmagasabb a vizsgált kockázati területek között, hanem inkább a középmezőnyben vagy annak alsó szegmensében helyezkedik el, ami a digitális kockázatok relatív percepciós alulsúlyozottságára utal.	A doménenként számított átlagok alapján az IT-biztonsági kockázatok észlelt szintje nem bizonyult a legmagasabbnak a vizsgált területek között. Az egyes IT-biztonsági elemek közül a jelszó vagy PIN mások előtti használata kapta a legmagasabb átlagértékeket, míg a nyílt WiFi-hálózathoz való csatlakozás a legalacsonyabb percepciós értéket mutatta, noha objektív információbiztonsági szempontból jelentős kockázatot hordoz. A teljes domén-összehasonlítás alapján az etikai és az egészség/biztonsági domén magasabb észlelt kockázati értékeket mutatott, mint az IT-domén, amely a középmezőnyben vagy annak alsó részében helyezkedett el. Ez a digitális kockázatok relatív percepciós alulsúlyozottságára utal.
H4	T3 – Kockázatpercepció és biztonságtudatos viselkedés kapcsolata Empirikusan alátámasztottam, hogy az IT-biztonsági kockázatok magasabb észlelése több esetben szignifikáns, irányhelyes kapcsolat-	A Spearman-féle rangkorrelációs elemzések több esetben szignifikáns, irányhelyes kapcsolatot tártak fel az észlelt IT-kockázat és a biztonságtudatos viselkedés között. A nyílt WiFi-hálózathoz való csatlakozás magasabb kockázatészlelése együtt járt a kétfaktoros hitelesítés gyakoribb használatával. A frissítések rendszeres telepítése és a nyílt WiFi-

Kapcsolódó hipotézis(ek)	Tézis szövege	Empirikus magyarázat
	ban áll a biztonságtudatos viselkedési gyakorlatok alkalmazásával, ugyanakkor az összefüggések erőssége mérsékelt, ami az attitűd és viselkedés közötti kapcsolat részleges jellegét jelzi.	használat között negatív kapcsolat mutatkozott, ami arra utal, hogy a magasabb biztonságtudatosság preventív viselkedéssel társul. Emellett a biztonságtudatos e-mail-csatolmánykezelés kisebb valószínűséggel járt együtt vállalati adatok privát e-mail címre történő továbbításával. Ugyanakkor az összefüggések többsége gyenge vagy közepes erősségű volt, ami azt jelzi, hogy a kockázatészlelés fontos, de nem kizárólagos magyarázó tényezője a viselkedésnek.
H5	T4 – A technikai kompetencia és a szervezeti kockázat viszonya Kimutattam, hogy a technikai biztonságtudatosság bizonyos formái BYOD-kontextusban együtt járhatnak szervezeti szempontból kockázatos magatartással, ami a technikai kompetencia és a szervezeti szabálykövetés közötti potenciális strukturális feszültségre utal.	A H5 vizsgálata azt mutatta, hogy a technikai biztonságtudatosság nem homogén konstrukció. A vállalati adatok saját tulajdonú eszközre történő másolása, mint BYOD-kontextusban értelmezett szervezeti kockázati magatartás gyenge pozitív kapcsolatot mutatott a rendszeres biztonsági frissítések telepítésével, ami arra utal, hogy a technikai kompetencia és az eszközhasználati magabiztosság bizonyos esetekben együtt járhat a szervezeti kontrollmechanizmusok részleges megkerülésével. Ugyanakkor a jelszókezelő használata gyenge negatív kapcsolatot mutatott a vállalati adatmásolással, vagyis a technikai biztonságtudatosság egyes formái kifejezetten védő jellegűek. Az eredmények alapján a technikai biztonságtudatosság, a szervezeti szabálykövetés és a normatív-etikai attitűd nem feltétlenül mozognak együtt.
H6, H7	T5 – Haszon-domináns döntési architektúra az IT-biztonsági döntésekben Igazoltam, hogy az IT-biztonsági döntésekben az észlelt haszon hatása szignifikánsan meghaladja az észlelt kockázat hatását, és ez a súlyozási aszimmetria nem kizárólag az IT-biztonsági domén sajátossága, hanem más kockázati területeken is strukturálisan megjelenik.	A H6 eredményei szerint az IT-biztonsági doménben a cselekvési valószínűség regressziós modelljében az észlelt haszon standardizált regressziós együtthatója lényegesen nagyobb volt, mint az észlelt kockázaté ($\beta = 0{,}679$ vs. $\beta = -0{,}125$; $R^2 = 0{,}541$), ami egyértelműen haszon-domináns döntési struktúrát jelez. A H7 ezt a mintázatot doménközi összehasonlításban is megerősítette: más vizsgált kockázati területen is kimutatható volt a haszon regressziós dominanciája (például az A-doménben $\beta = 0{,}522$ vs. $\beta = -0{,}212$; $R^2 = 0{,}377$), és a dominancia mértéke nem tért el szignifikánsan az IT-domén eredményétől. Az eredmények alapján a súlyozási aszimmetria nem kizárólag IT-biztonsági sajátosság, hanem szélesebb döntési mintázatként értelmezhető.

Forrás: saját szerkesztés a kutatási eredmények alapján

3.5 Alkalmazhatóság katonai és kritikus infrastruktúra környezetben

A dolgozat eddigi eredményei – különösen a mobileszközökhöz kapcsolódó humán kockázat észlelés és döntéstámogatási stratégia strukturálása – olyan mechanizmusokat fogalmaznak meg, amelyek több szinten is átültethetők katonai és kritikus infrastruktúra környezetbe. Bár primer adatgyűjtésem nem katonai mintán történt, az eredmények tematikus szerkezete lehetővé teszi a katonai alkalmazhatóság értelmes és tudományosan megalapozott kiterjesztését.

A 3.3–3.4 fejezetekben bemutatott empirikus kockázati dimenziók és stratégiák (ld. különösen az IT-kockázatészlelés tendenciáit) olyan általános viselkedési és stratégiai mintákat rajzolnak ki, amelyek kapcsolódási pontot jelentenek a katonai-műszaki döntéshozatali folyamatokkal. Ennek bemutatására az alábbiakban strukturált áttekintést adok.

3.5.1 Mobil digitális rendszerek és katonai kontextus

A mobileszközök növekvő szerepe a polgári és szervezeti működésben közismert, és a biztonsági kockázatok is egyre összetettebbé válnak [145] [146]. A dolgozat eredményei szerint – ahogyan azt a 3.4.1. alfejezetben is láttuk – a felhasználók hajlamosak alulértékelni a mobileszközök kockázatait a munkavégzés során, ami a katonai környezetben kritikus helyzetkép-pontosság és információbiztonság gyengüléséhez vezethet. A katonai műveleti környezetben a mobilitás nem pusztán kényelmi kérdés, hanem stratégiai komponens. A Secure Digital Military Mobility System fejlesztésére irányuló uniós kezdeményezés például kifejezetten hangsúlyozza a mobileszközök integrációjának és biztonsági kezelésének fontosságát katonai alkalmazásban [147]. Ez alátámasztja azt a feltevést, hogy az itt vizsgált kockázati struktúrák – bár civil mintán történtek – közvetlenül hasznosíthatók katonai digitális rendszerek fejlesztésében, feltéve, hogy a szervezeti és műveleti kontextus figyelembevételével adaptáljuk őket.

3.5.2 Kiberbiztonság és katonai műveleti döntéshozatal

A dolgozatban kimutatott humán kockázatészlelés mechanizmusai (3.4.2.) összefüggenek azzal a stratégiai problémával, amelyet a NATO tagállamok kiberbiztonsági képességeinek fejlesztése is tükröz [148]. A kibererők és a kibervédelem integrációja a katonai doktrínákba egyre inkább középpontba kerül, különösen a digitális kommunikációs rendszerek és hálózatok terén. A NATO Cyber Coalition 2025 gyakorlat e tekintetben olyan kihívásokat szimulál, amelyek a mobileszközök és a hálózati infrastruktúra biztonsági integritását vizsgálják [33]. Ez közvetetten alátámasztja, hogy a dolgozat döntéstámogatási és kockázati keretei relevánsak lehetnek a katonai kiberbiztonság operatív és stratégiai szintű vizsgálatában is. A fentiekből következik, hogy a dolgozatban alkalmazott kockázatmodellezés és humán tényezők figyelembevétele

támogathatja a katonai műveleti döntéshozatalt, különösen ott, ahol a mobilitással és digitális eszközhasználattal kapcsolatos kockázatok valós idejű döntési keretbe rendezése szükséges.

3.5.3 Technológiai trendek, hibrid fenyegetések és katonai IoT

A mobil kommunikációs technológiák (beleértve a 6G-t és a hálózati sebezhetőségeket) egyre nagyobb szerepet játszanak a katonai műveletekben – például a híradó- és információs rendszerek integrált komponenseiként [149] [150]. A dolgozat 3.2–3.3 fejezeteiben bemutatott IT-kockázati dimenziók és fenyegetési mintázatok a technológiai trendek fényében releváns fenyegetési forgatókönyvekké válhatnak olyan rendszerekben, ahol a kommunikációs csatornák és végponti eszközök kombinált biztonsága döntő fontosságú. A LoRaWAN és más IoT-alapú hálózatok katonai alkalmazására vonatkozó friss kutatások rámutatnak, hogy ezekben a környezetekben a hálózati sebezhetőségek – beleértve a végponti eszközöket – nem csupán elméleti kockázatok, hanem valós fenyegetési vektorok [151]. Hasonlóan, a katonai 5G-alapú hálózatok privát hitelesítési protokolljai is magas követelményeket támasztanak az eszköz- és felhasználókezelés biztonságával szemben [152]. Ez megerősíti azt a feltételezést, hogy az értekezésben definiált kockázati fogalmak és stratégiák adaptálhatók olyan katonai IoT- és hálózati kontextusokba, ahol a mobileszközök integrált komponensek, és ahol a hálózatbiztonság kritikus szerephez jut.

3.5.4 Kritikus infrastruktúrák, nemzetbiztonság és katonai kapcsolódás

A kritikus infrastruktúrák védelme és a nemzetbiztonsági szempontok a katonai stratégiai doktrínák fontos elemei. A polgári és katonai infrastruktúrák közötti konvergencia miatt a dolgozatban felvetett stratégiák – különösen a mobileszközök integrációjából eredő kockázatok kezelése – relevánsan alkalmazhatók a kritikus szektorokra is. Napjaink kibervédelmi trendjei és a közép- és kelet-európai infrastruktúra védelmi jelentések egyaránt hangsúlyozzák a digitális mobilitás és IoT-biztonság szerepét a kritikus rendszerekben [20]. Ez párhuzamba állítható azzal az eredménnyel, amelyet a 3.3.1 fejezetben fogalmaztam meg az IT-kockázat struktúrájáról: amely dimenziók kiemelt figyelmet érdemelnek egy szervezet biztonsági stratégiájában, azok a kritikus infrastruktúra operátoroknál és katonai támogatással működő védelmi láncoknál is kulcsfontosságúak.

3.5.5 Alkalmazhatóság, korlátok és továbblépési irányok

A dolgozat eredményei – különösen a mobileszközök humán kockázatészlelésére és a stratégiai döntéstámogatási keretekre vonatkozó elemzések – több ponton kapcsolódnak a katonai műszaki és biztonsági döntéshozatal kihívásaihoz. A friss katonai és hibrid fenyegetésekről szóló

szakirodalom [148] [149] alátámasztja, hogy a mobileszközök biztonsága és integrációja nem csak szervezeti, hanem stratégiai katonai probléma is.

Ugyanakkor fontos leszögezni a korlátokat:

- a primer adatgyűjtés nem katonai mintán alapult,
- a dolgozat strukturálása nem katonai doktrínaelemzésként indult,
- a konkrét műveleti modellek nem kerültek empirikusan validálásra.

Ennek ellenére a katonai alkalmazhatósági szempontú értelmezés támogathatja a dolgozat további tudományos és gyakorlati érvényesülését, különösen olyan kutatási projektben vagy haderő-biztonsági stratégiában, ahol a mobileszközök és kiberbiztonság integrált kezelése kiemelt stratégiai fontosságú.

3.6 Az eredmények hasznosítása, továbbfejlesztési lehetőségek, limitációk

A dolgozatban bemutatott empirikus vizsgálatok mintái felsőoktatási hallgatókból álltak, azonban az IT-biztonsági kockázatvállalás szerkezete és a percepciós döntési mechanizmusok nem korlátozódnak az egyetemi környezetre. A feltárt döntési mintázatok – különösen a haszondomináns súlyozási struktúra és a demográfiai tényezők reziduális hatása – közvetlen relevanciával bírnak a katonai és honvédelmi információbiztonsági rendszerek számára is.

A modern katonai működés egyre inkább hálózatközpontú, digitálisan integrált és mobileszközökre támaszkodó rendszerben zajlik. A saját tulajdonú vagy félig kontrollált mobileszközök használata, a hibrid kommunikációs csatornák, valamint a civil–katonai technológiai átjárhatóság olyan kockázati környezetet hoz létre, amelyben a humán döntési tényezők stratégiai jelentőségűvé válnak.

A kutatás egyik legfontosabb eredménye, hogy az IT-biztonsági döntésekben az észlelt haszon strukturálisan dominál az észlelt kockázattal szemben. Katonai kontextusban ez különösen kritikus, mivel az operatív hatékonyság, a gyors információáramlás és a kényelmi szempontok rövid távú előnyei könnyen felülírhatják a biztonsági kockázatok absztrakt, jövőbeni következményeit. A döntési architektúra haszon-orientált jellege arra utal, hogy a kizárólag veszélykommunikációra épülő biztonsági doktrína nem feltétlenül eredményez optimális viselkedési mintázatot.

A kutatás eredményei a katonai alkalmazás szempontjából az alábbi területeken hasznosíthatók:

- **Katonai információbiztonsági oktatás és kiképzés:** a képzési programokban a biztonságos viselkedéshez kapcsolódó operatív előnyök hangsúlyozása növelheti a szabálykövetés hatékonyságát.
- **Humán kockázatelemzés integrálása a védelmi kockázatmenedzsmentbe:** az életkor és nem önálló magyarázó szerepe alapján differenciált érzékenységi profilok alakíthatók ki.
- **BYOD-szerű katonai eszközhasználat szabályozása:** a technikai kontroll mellett szükséges a döntési percepciók strukturális figyelembevétele.
- **Kiberbiztonsági doktrínák finomítása:** a veszteségelkerülési modellek mellett a motivációs szerkezet haszonorientált komponenseit is be kell építeni.

A katonai szervezetekben a biztonság nem pusztán technológiai kérdés, hanem döntési és kulturális konstrukció is. A dolgozat eredményei arra utalnak, hogy a kockázati döntéshozatal nem kiegyensúlyozott nyereség–veszteség szempontok figyelembevételével működik, hanem az egyéni kockázatérzékelés alapján kerül kiválasztásra. Ennek figyelmen kívül hagyása stratégiai sérülékenységet eredményezhet.

Továbbfejlesztési lehetőségek katonai irányban

- **A kutatás megismétlése katonai mintán:** különböző szolgálati ágak és beosztási szintek összehasonlító vizsgálata.
- **Operatív környezetben végzett terepkutatás:** missziós vagy gyakorlati helyzetekben vizsgált döntési mintázatok.
- **Kísérleti kockázatkommunikációs modellek tesztelése:** haszonorientált vagy veszteségalapú biztonsági kommunikáció hatékonyságának összehasonlítása.
- **Kiberreziliencia-modell beépítése:** a kiberbiztonsági fenyegetettség-érzet egyéni különbségének beépítése katonai kockázatértékelési keretrendszerbe.
- **Adaptív döntéstámogató rendszer fejlesztése:** amely képes humán viselkedési profilok alapján differenciált biztonsági kontrollszinteket javasolni különböző helyzetekben.

A dolgozat eredményei hozzájárulnak annak megértéséhez, hogy a katonai információbiztonsági rendszerek sérülékenysége nem kizárólag technikai gyengeségekből fakad, hanem a

döntési súlyozás strukturális sajátosságaiból is. A haszon-domináns döntési szerkezet felismerése lehetőséget teremt olyan doktrinális és képzési beavatkozások kidolgozására, amelyek a motivációs mechanizmusokra építve növelik a kiberbiztonsági fegyelmet.

Limitációk

A kutatás kényelmi mintavétellel, egyetemi hallgatók bevonásával készült. Az eredmények értelmezésekor figyelembe kell venni, hogy a minta demográfiailag és végzettség tekintetében homogénebb a teljes magyar aktív korú lakosságnál.

Ugyanakkor a feltárt döntési mintázatok és a demográfiai tényezők hatásai olyan alapvető mechanizmusok, amelyek más (pl. katonai vagy vállalati) környezetben is értelmezhetőek és alkalmazhatóak.

3.7 Vezetői javaslattétel: BYOD biztonsági stratégiák a felhasználói viselkedés és kockázatészlelés tükrében

A problémafelvetés és a kutatás fókuszpontja

A saját tulajdonú mobileszközök munkacélú használata (BYOD) mára a modern vállalati működés elkerülhetetlen elemévé vált, amely jelentős rugalmasságot és költséghatékonyságot biztosít. Ugyanakkor a BYOD alapjaiban bontja meg a hagyományos vállalati infokommunikációs technológiák védelmét. A jelen doktori kutatás alaptézise, hogy az információbiztonsági incidensek túlnyomó többsége nem tisztán technológiai hiányosságokra, hanem a felhasználói döntési mechanizmusok és a szubjektív kockázatészlelés anomáliáira vezethető vissza. A technológiai (hard) kontrollok önmagukban elégtelenek; megértésük és hatékony alkalmazásuk elengedhetetlenül igényli a humán tényező (soft kontrollok) viselkedésalapú vizsgálatát.

A kutatás legfontosabb megállapításai (Vezetői szemmel)

Az elvégzett empirikus vizsgálat és a modellalkotás az alábbi, vállalati környezetben is kritikus jelentőségű eredményeket (téziseket) igazolta:

A "Biztonságtudatossági paradoxon" (Kiemelt eredmény): A kutatás rávilágított egy rendkívül veszélyes vállalati vakfoltra. A magasabb szintű technikai ismeretekkel rendelkező felhasználók (pl. mérnökök, erős IT-affinitású munkavállalók) a kontroll illúziója miatt hajlamosabbak nagyobb biztonsági kockázatot vállalni, mint a laikusok. Esetükben a hagyományos technikai tudás nem eredményez automatikusan óvatosabb magatartást, így a standard biztonsági oktatások náluk sokszor hatástalanok, vagy egyenesen hamis biztonságérzetet keltenek.

Haszon-domináns döntési architektúra: A dolgozat igazolta, hogy a BYOD eszközök használata során a felhasználók kognitív mérlegelésében súlyos aszimmetria áll fenn. A várt haszon (kényelem, gyorsaság, produktivitás) standardizált súlya többszörösen felülmúlja a vélt kockázatok (adatvesztés, lebukás) visszatartó erejét. Ha a biztonságos megoldás kényelmetlen, a munkavállaló szinte biztosan a kockázatosabb, de gyorsabb utat fogja választani (Shadow IT).

Az IT-kockázatvállalás mint specifikus terület: A munkavállalók az IT-biztonsági veszélyeket teljesen eltérően értékelik, mint a mindennapi élet (pl. pénzügyi vagy egészségügyi) kockázatait. Az életkor és a nem jelentős magyarázóerővel bír a kockázatvállalási hajlandóságban, ami indokolttá teszi a célcsoport-specifikus biztonsági megközelítéseket.

Stratégiai javaslatok a vállalati BYOD szabályozáshoz

A fenti tudományos eredmények alapján a szervezetek információbiztonsági vezetőinek (CISO) és döntéshozóinak az alábbi stratégiai irányelvek mentén érdemes újragondolniuk a BYOD szabályozást:

Felhasználói élmény (UX) alapú biztonságtervezés: Mivel a felhasználók döntéseit a haszon és a kényelem dominálja, a biztonsági kontrolloknak (pl. többfaktoros hitelesítés, VPN-ek) „láthatatlannak" és a lehető legkényelmesebbnek kell lenniük. A büntetésre és tiltásra épülő szabályozások helyett az „alapértelmezett biztonság" (security by default) elvét kell alkalmazni a BYOD környezetben.

Differenciált, viselkedésalapú edukáció: A biztonságtudatossági paradoxon miatt a vállalati oktatást át kell alakítani. A „kockázati bajnokokat" (magas technikai tudású, de kockázatkereső kollégákat) nem a spamek felismerésére kell tanítani, hanem a túlzott magabiztosság kognitív torzításaira és a szervezeti felelősségre. A képzéseket a munkavállaló valós IT-biztonsági kockázati profiljához kell igazítani.

Zero Trust Architecture (ZTA) integrációja a BYOD-ban: A magas egyéni kockázatvállalási hajlandóság miatt a szervezet nem bízhat meg vakon a felhasználó eszközében. A stratégia fókuszát az eszköz (MDM - Mobile Device Management) menedzseléséről át kell helyezni az adatok és az identitás védelmére (MAM - Mobile Application Management), valós idejű, viselkedésalapú anomália-elemzéssel (UEBA) kiegészítve.

Konklúzió

A doktori értekezés eredményei bizonyítják, hogy a sikeres BYOD stratégia nem csupán informatikai beruházás kérdése, hanem egy összetett szocio-technikai kihívás. A jövőben azok a

szervezetek lesznek képesek minimalizálni a kiberbiztonsági incidenseket, amelyek megértik a munkavállalóik „haszon-domináns” döntési logikáját, és a biztonsági szabályozásaikat képesek ehhez a pszichológiai valósághoz igazítani.

3.8 A fejezet összefoglalása

Az értekezés 3. fő fejezete a dolgozat gyakorlati eredményét adja, amelyben az elméleti háttér bemutatása és elemzése után ismertetem saját empirikus kutatásom, annak módszertanát, eredményeit és a felállított téziseket.

A kutatás módszertana és célkitűzése

A fejezet központi eleme kérdőíves vizsgálat, amely az egyetemi hallgatók (mint a jelen és a közeljövő munkavállalói) IT-biztonsági kockázatvállalási hajlandóságát mérte. A kutatás a nemzetközileg elismert DOSPERT-skálára (Domain-Specific Risk-Attitude Scale) épült, amelyet egy speciális, IT-biztonsági doménnel egészítettem ki.

A kutatás fő céljai a következők voltak:

Az IT-kockázatvállalási hajlandóság mérhetőségének és szerkezeti sajátosságainak feltárása.

Annak vizsgálata, hogy az IT-biztonsági döntések mennyire tekinthetők doménspecifikusnak (azaz elkülönülnek-e más élethelyzetek, pl. pénzügyi vagy etikai kockázatok döntési mechanizmusaitól). A biztonságtudatos viselkedés és a valós kockázatvállalás közötti összefüggések elemzése.

Legfontosabb eredmények és összefüggések

A fejezet részletesen elemzi a kilenc felállított hipotézis tesztelésének eredményeit, amelyek közül több alapvető jelentőségű a BYOD-stratégiák szempontjából: Az IT-biztonsági domén autonómiája (H1, H8, H9). Kimutattam, hogy az IT-biztonsági kockázatvállalás egy önálló, kontextusfüggő konstrukció. Az eredeti DOSPERT-domének nem tudták szignifikánsan előre jelezni az IT-biztonsági válaszokat. Érdekes eredmény, hogy az életkor és a nem (a nők javára) más tényezők kontrollálása mellett szignifikáns magyarázóerővel bír az IT-kockázatvállalásban. Haszon-domináns döntési architektúra (H6, H7): Az egyik legfontosabb eredmény, hogy a döntéshozatali folyamatban az észlelt haszon (kényelem, gyorsaság) súlya közel tízszerese (globálisan) vagy ötszöröse (IT-specifikusan) az észlelt kockázatnak. Ez azt jelenti, hogy a felhasználókat elsősorban az előnyök mozgatják a kockázatos viselkedés felé, és a veszélyek hangsúlyozása önmagában kevésbé hatékony.

A technikai kompetencia paradoxona (H3, H5): A kutatás cáfolta, hogy az informatikai képzettség egyértelműen magasabb kockázati érzékenységet jelentene. Sőt, bizonyos esetekben a technikai magabiztosság (pl. rendszerfrissítések naprakészsége) együtt járhat magasabb szervezeti kockázatvállalással (pl. vállalati adatok saját eszközre másolása), mivel a felhasználó bízik saját problémamegoldó képességében. A biztonságtudatosság többdimenziós jellege (H4): A biztonságtudatos gyakorlatok (pl. jelszókezelő használata) pozitív kapcsolatban állnak a kockázatészleléssel, de ez a kapcsolat nem lineáris minden területen.

Alkalmazhatóság katonai és kritikus környezetben

Kitérek dolgozatom e fejezetében arra is, hogy az eredmények különösen relevánsak a katonai és kritikus infrastruktúra szektorokban, ahol a hibrid fenyegetések és a katonai IoT eszközök elterjedése miatt a metaadat-kitettség és az egyéni döntések stratégiai súllyal bírnak. A humán tényező itt nem csupán hibaforrás, hanem a biztonsági architektúra strukturális komponense. Ismertettem a kutatásom limitációit.

Vezetői javaslattétel

A vezetői javaslattétel alfejezetben összefoglaltam eredményeimet vállalatvezetői szempontból és javaslatokat tettem egy BYOD szabályozás stratégiai kérdéseire.

Legfontosabb hivatkozások a fejezetben:

- Weber U. Elke, Blais Renée Ann, Betz E. Nancy (2002): A Domain-Specific Risk-Attitude Scale: Measuring Risk Perceptions and Risk Behaviors [27]
- Renn (2017): Risk Governance, Coping with Uncertainty in a Complex World. [12]
- ISO/IEC 27001: Information security, cybersecurity and privacy protection [135]

A 3. fejezet összegzéseként a megállapítom, hogy a BYOD-stratégia nem épülhet kizárólag technikai kontrollra (pl. MDM); szükség van a haszon-orientált döntési mechanizmusok figyelembevételére és a biztonsági kultúra célzott, generációs és doménspecifikus fejlesztésére. Valamint, hogy a szervezeteknek szükségük van az értekezésben bemutatott kutatásaim alapján olyan BYOD stratégiára, mely az alap stratégiákra (Tiltott, Tűrt, Esetileg szabályozott, írásban szabályozott, írásban szabályozott és aktívan támogatott) épít és figyelembe veszi az egyes felhasználók által a szervezetre jelentett BYOD kockázatot.

IRODALOMJEGYZÉK

1 LEE James, WARKENTIN Merrill, CROSSLER Robert E., OTONDO Robert F., Implications of Monitoring Mechanisms on Bring Your Own Device Adoption, Journal of Computer Information Systems , vol. 57, no. 4, pp. 309-318, 2017. ISSN:0887-4417 DOI:10.1080/08874417.2016.1184032 (Letöltve: 2023. február 7.)

2 WEEGER Andy, WANG Xuequn, GEWALD Heiko, It Consumerization: Byod-Program Acceptance and its Impact on Employer Attractiveness, Journal of Computer Information Systems , vol. 56, no. 1, pp. 1-10, 2016. ISSN:0887-4417 DOI:10.1080/08874417.2015.11645795 (Letöltve: 2023. február 7.)

3 KE Chih-Kun, LIN Zheng-Hua, An Approach for Secure Data Exchange: Experiments on Android-based Mobile Device, Scientia Iranica , vol. 22, no. 4, pp. 1586-1593, 2015. ISSN:1026-3098 https://web.archive.org/web/20240507071101/http://scientiairanica.sharif.edu/article_3736_5df2245ab8ec92e9cfc086d4cbd6df18.pdf (Letöltve: 2026. március 7.)

4 WANG Yu, LI Hanshang, LI Ting, Participant selection for data collection through device-to-device communications in mobile sensing, Personal and Ubiquitous Computing , vol. 21, no. 1, pp. 31-41, 2017. ISSN:1617-4909 DOI:10.1007/S00779-016-0974-0 (Letöltve: 2023. február 7.)

5 GLISSON William Bradley, STORER Tim, MAYALL Gavin, MOUG Iain, GRISPOS George, Electronic retention: what does your mobile phone reveal about you?, International Journal of Information Security , vol. 10, no. 6, pp. 337-349, 2011. ISSN:1615-5270 DOI:10.1007/S10207-011-0144-3 (Letöltve: 2023. február 7.)

6 MICHELBEGER Pál: Információ-, folyamat- és vállalatbiztonság;. Budapest, Magyarország Óbudai Egyetem, Keleti Károly Gazdasági Kar, 2022. ISBN 978-963-449-289-4

7 KESZTHELYI András, Paradigmaváltás - biztonság - emberi tényező, Taylor : gazdálkodás- és szervezéstudományi folyóirat , vol. 7, no. 1-2, pp. 406-412, 2015. ISSN:2062-1396 http://acta.bibl.u-szeged.hu/36354/1/vikek_018_019_406-412.pdf (Letöltve: 2023. február 7.)

8 MICHELBERGER Pál, LÁBODI Csaba, After Information Security – Before a Paradigm Change: A complex Enterprise Security Model, ACTA POLYTECHNICA HUNGARICA , vol. 9, no. 4, pp. 101-116, 2012. ISSN 1785-8860 http://acta.uni-obuda.hu//Michelberger_Labodi_36.pdf (Letöltve: 2022. december 29.)

9 MICHELBERGER Pál, KEMENDI Ágnes, Data, Information and IT Security - Software Support for Security Activities, Problems of Management in the 21st Century , pp. 108-124., 2020. ISSN 2029-6932 DOI:10.33225/pmc/20.15.108 (Letöltve: 2023. február 8.)

10 RAJNAI Zoltán, Információbiztonság tudatosság, Műszaki Tudományos Közlemények , no. 7., pp. 37-42., 2017. ISSN 2393-1280 DOI:10.33895/mtk-2017.07.02 (Letöltve: 2023. szepember 10.)

11 RENN Ortwin: "Concepts of risk : a classification" in *Social theories of risk*, KRIMSKY Sheldon, Ed., 1992 , pp. 53-79 ISBN:0-275-94168-X. DOI:10.18419/OPUS-7248 (Letöltve: 2023. február 8.)

12 RENN Ortwin: Risk Governance, Coping with Uncertainty in a Complex World;. London Routledge, 2017. ISBN: 978-1-84407-291-0

13 BLAIS Ann-Renée, WEBER U. Elke, A Domain-Specific Risk-Taking (DOSPERT) Scale for Adult Populations, vol. 1, pp. 33-47, 2006. ISSN:1930-2975 http://journal.sjdm.org/06005/jdm06005.htm (Letöltve: 2023. február 8.)

14 DISTERER Georg, KLEINER Carsten, BYOD Bring Your Own Device, Procedia Technology , vol. 9, pp. 43-53, 2013. ISSN 2212-0173 DOI:10.1016/J.PROTCY.2013.12.005 (Letöltve: 2022. szepember 12.)

15 ROSE Chris, BYOD: An Examination Of Bring Your Own Device In Business, Review of Business Information Systems (RBIS) , vol. 17, no. 2, pp. 65-70, 2013. ISSN:2157-9547 DOI:10.19030/RBIS.V17I2.7846 (Letöltve: 2023. január 17.)

16 OLALERE Morufu, ABDULLAH Taufik Mohd, MAHMOD Ramlan, ABDULLAH Azizol, Bring your own device: security challenges and a theoretical framework for two-factor authentication, International Journal of Computer Networks and Communications Security , vol. 4, no. 1, pp. 21-32, 2016. ISSN 2410-0595
http://psasir.upm.edu.my/id/eprint/55224/ (Letöltve: 2022. február 17.)

17 BAILLETTE Paméla, BARLETTE Yves, LECLERCQ-VANDELANNOITTE Aurélie, Bring your own device in organizations: Extending the reversed IT adoption logic to security paradoxes for CEOs and end users, International Journal of Information Management , vol. 43, pp. 76-84, 2018. ISSN:0268-4012
DOI:10.1016/J.IJINFOMGT.2018.07.007 (Letöltve: 2023. február 8.)

18 MIKE Nimród, KRÉN Enikő, KECSKEMÉTI Tamás, Wolf-proof brick house? Information security of SMEs in Hungary, Vezetéstudomány Budapest Management Review , vol. 54, no. 9, pp. 44-57, 2023.
https://journals.lib.uni-corvinus.hu/index.php/vezetestudomany/article/view/1070
DOI:10.14267/VEZTUD.2023.09.04 (Letöltve: 2024. április 10.)

19 KEMENDI Ágnes, MICHELBERGER Pál, MESJASZ-LECH Agata, ICT security in businesses – efficiency analysis, ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES , vol. 1, pp. 123-149, 2021. ISSN 2345-0282 (online)
DOI:10.9770/jesi.2021.9.1(8) (Letöltve: 2022. november 20.)

20 SILOBREAKER. (2025. július) Silobreaker supports NATO CCDCOE with release of new report on cybersecurity threats to maritime port infrastructure.
https://www.silobreaker.com/news/2025/07/nato-ccdcoe-releases-new-report-on-cybersecurity-threats-to-maritime-port-infrastructure/
(Letöltve: 2025. november 10.)

21 MICHELBERGER Pál, HORVÁTH Zsolt, Biztonságorientált folyamatmenedzsment, INTERNATIONAL JOURNAL OF ENGINEERING AND MANAGEMENT SCIENCES / MŰSZAKI ÉS MENEDZSMENT TUDOMÁNYI KÖZLEMÉNYEK , pp. 344-364., 2017. ISSN: 2498-700X
DOI:10.21791/IJEMS.2017.4.28. (Letöltve: 2019. oktober 3.)

22 VARGA Dóra, Az adatvédelem és a munkáltatói ellenőrzés kérdései a XXI. századi munkaviszonyok tükrében, Miskolci Jogtudó , pp. 81–89, 2019. ISSN 2630-9505 https://jogtudo.uni-miskolc.hu/files/4159/MJ2019iss1art9Varga.pdf (Letöltve: 2020. oktober 29.)

23 BRAUNSTEIN Christopher J, Mobile Device Management, Army Communicator , vol. 37, no. 2, pp. 28-30, 2012. ISSN:0362-5745 https://cybercoe.army.mil/AC/2012/Vol37/No2/Summer_2012_Edition.pdf (Letöltve: 2019. április 29.)

24 Logicalis. (2015) The Shadow IT Phenomenon - CIOs respond with internal service provider transformation. http://web.archive.org/web/20170622020039/https://www.logicalis.com/globalassets/group/cio-survey/cio-survey-2015_final3.pdf (Letöltve: 2023. február 8 (archive.org-on archívált változaton keresztül).)

25 VANDELANNOITTE Aurélie Leclercq, Managing BYOD: how do organizations incorporate user-driven IT innovations?, Information Technology & People , vol. 28, no. 1, pp. 2-33, 2015. ISSN: 0959-3845 DOI:10.1108/ITP-11-2012-0129 (Letöltve: 2023. február 8.)

26 PARSONS Kathryn, MCCORMAC Agata, BUTAVICIUS Marcus A., PATTINSON Malcolm Robert, JERRAM Cate, Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q), Computers & Security , vol. 42, pp. 165-176, 2014. ISSN:0167-4048 DOI:10.1016/J.COSE.2013.12.003 (Letöltve: 2024. március 12.)

27 WEBER U. Elke, BLAIS Renée Ann, BETZ E. Nancy, A Domain-Specific Risk-Attitude Scale: Measuring Risk Perceptions and Risk Behaviors, Journal of Behavioral Decision Making Volume , vol. 15, no. 4, pp. 263-290, 2002. ISSN:1099-0771 DOI:10.1002/BDM.414 (Letöltve: 2023. február 8.)

28 KRISTÓF Csaba. (2013. szeptember) A BYOD jogi útvesztői. http://bitport.hu/vezinfo/a-byod-jogi-utvesztoi (Letöltve: 2022. december 27.)

29 KRISTÓF Csaba. (2013. június) A britek a biztonságtudatosság növelésére költenek. http://bitport.hu/biztonsag/a-britek-koeltenek-biztonsagtudatossag-noevelesere (Letöltve: 2022. december 27.)

30 SCHOPP Attila, VASVÁRI György. (2012. február) Tudatos biztonság. https://itbusiness.hu/technology/aktualis-lapszam/focus/tudatos-biztonsag/ (Letöltve: 2022. december 27.)

31 HOFSTEDE Geert: Culture's Consequences: comparing values, behaviors, institutions, and organizations across nations (2nd ed.);. Thousand Oaks, CA SAGE Publications, 2001. ISBN:978-0-8039-7323-7

32 HOFSTEDE H. Geert, HOFSTEDE Jan Gert, MINKOV Michael: Cultures and Organizations, Software of the mind. Intercultural Cooperation and Its Importance for survival;. McGraw-Hill, 2010. ISBN: 978-0-07-166418-9

33 NATO. (2025. december) NATO Cyber Coalition 2025: Advancing Cyber Defence and Strengthening Alliance Resilience. https://www.act.nato.int/article/cyber-coalition-2025/ (Letöltve: 2026. január 17.)

34 European Network and Information Security Agency. (2013) Top Ten Smartphone Risks. https://web.archive.org/web/20120527090937/http://www.enisa.europa.eu/activities/application-security/smartphone-security-1/top-ten-risks (Letöltve: 2022. december 27.)

35 NOBLE M. Stephanie, HAYTKO L. Diana, PHI Joanna, What drives college-age Generation Y consumers?, Journal of Business Research , vol. 62, no. 6, pp. 617-628, 2009. ISSN:0148-2963 DOI:10.1016/J.JBUSRES.2008.01.020 (Letöltve: 2023. február 8.)

36 JONES L Jami, Who are Millennials? And what they want from libraries, bookstores, and librarians, 2008: IASL Conference Proceedings (Berkeley, USA): World Class Learning and Literacy through School Libraries , 2008. ISSN 2562-8372 DOI:10.29173/iasl7976 (Letöltve: 2022. december 28.)

37 PARDUE T. Karen, MORGAN Patricia, MILLENNIALS CONSIDERED: A NEW GENERATION New Approaches, and Implications for Nursing Education, Nursing education perspectives , vol. 29, no. 2, pp. 74-79, 2008. ISSN:1536-5026 DOI:10.1097/00024776-200803000-00007 (Letöltve: 2023. február 8.)

38 PRENSKY Marc, Digital Natives, Digital Immigrants, On the Horizon , vol. 9, no. 5, 2001. ISSN:1074-8121
DOI:10.1108/10748120110424816 (Letöltve: 2023. február 8.)

39 PERILLO Suzanne, "Reaching Generation Y To Be or Not to Be – Relevant" , AASN Conference 2007 - The Wired Generation: Faith, Learning and Community with Generation Y.
https://web.archive.org/web/20080719195606/http://aasn.edu.au/zone_files/AASN_Conference_2007/dr_s_perillo_gen_y.pdf (Letöltve: 2023. február 8 (archive.org-on archívált változaton keresztül).)

40 LAZÁNYI Kornélia, A társas támogatás szerepe egy individualista társadalomban, A Virtuális Intézet Közép-Európa Kutatására közleményei , vol. 4, no. 2, pp. 51-58, 2012. ISSN:2062-1396
http://acta.bibl.u-szeged.hu/30184/ (Letöltve: 2023. február 8.)

41 KOVÁCS Kármen, A divatterjedés és a divattermékek fogyasztását befolyásoló tényezők empirikus vizsgálata a hazai fiatalok körében, Marketing & Menedzsment , vol. 43, no. 1, pp. 62-71, 2009. ISSN:1219-0349
https://journals.lib.pte.hu/index.php/mm/article/view/769 (Letöltve: 2023. február 8.)

42 PRZYBYLSKI K. Andrew, MURAYAMA Kou, DEHAAN R. Cody, GLADWELL Valerie, Motivational, emotional, and behavioral correlates of fear of missing out, Computers in Human Behavior , vol. 29, no. 4, pp. 1841-1848, 2013. ISSN: 1873-7692 DOI:10.1016/J.CHB.2013.02.014 (Letöltve: 2023. február 8.)

43 SHAW R. Susan, FAIRHURST David, Engaging a new generation of graduates, Journal of Education and Training , vol. 50, no. 5, pp. 366-378, 2008. ISSN:2330-9709 DOI:10.1108/00400910810889057 (Letöltve: 2016. május 27.)

44 TWENGE M. Jean: Generation Me: Why Today's Young Americans Are More Confident, Assertive, Entitled--and More Miserable Than Ever Before;. Free Press, 2007. ISBN:9780743276986

45 MI Jia, NESTA Frederick, Marketing library services to the Net Generation, Library Management , vol. 27, pp. 411-422, 2006. ISSN:0143-5124 DOI:10.1108/01435120610702404 (Letöltve: 2023. február 8.)

46 BROOK Chris. (2020) The ultimate guide to BYOD security: overcoming challenges, creating effective policies, and mitigating risks to maximize benefits. https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating
(Letöltve: 2022. december 27.)

47 Pew Research Center. (2014. február) Emerging Nations Embrace Internet, Mobile Technology, Cell Phones Nearly Ubiquitous in Many Countries. https://www.pewresearch.org/global/2014/02/13/emerging-nations-embrace-internet-mobile-technology/ (Letöltve: 2022. december 27.)

48 CHEN Baiyun, SEILHAMER Ryan, BENNETT Luke, BAUER Sue. (2015. június) Students' Mobile Learning Practices in Higher Education: A Multi-Year Study. https://er.educause.edu/articles/2015/6/students-mobile-learning-practices-in-higher-education-a-multiyear-study (Letöltve: 2022. december 27.)

49 JOHNSON Larry et al.: NMC Horizon Report: 2016 Higher Education Edition;. The New Media Consortium, 2016. ISBN:978-0-9968527-5-3 https://www.learntechlib.org/p/171478/ (Letöltve: 2023. február 8.)

50 SONG Yanjie, SUN Daner, JONG Siu-yung: "Enhancing students’ science learning in a seamless inquiry-based learning environment leveraged by BYOD (Bring your own device)" in *Proceedings of the Workshop on Computer-Based Learning Environments for Deep Learning in Inquiry and Problem-Solving Contexts*. Singapore: The International Conference of the Learning Sciences (ICLS), 2016 , pp. 37 - 43. https://aims.cuhk.edu.hk/converis/portal/detail/Publication/35629123
(Letöltve: 2017. szeptember 10.)

51 HAYWOOD D et al.: Student Mobility in a Digital World. Final Report of the Victorious Project;. European Commission E-Learning Programme, 2007. ISBN: 978-0-9555414-1-4

52 Voxburner: UK Youth Trends Report;. London Voxburner / The Student Beans Insight Agency, 2016.
http://www.voxburner.com/reports/
(Letöltve: 2025. szeptember 1.)

53 MANDIC Dorottya, KISS Gábor, RAJNAI Zoltán: "Password Usage among Users of Smart Devices in Hungary and Serbia" in *18th IEEE International Symposium on Applied Computational Intelligence and Informatics SACI 2024 Proceedings*, ANIKÓ Szakál, Ed. New York, USA: Institute of Electrical and Electronics Engineers (IEEE), 2024 , pp. 309-313. https://ieeexplore.ieee.org/document/10619863
DOI:10.1109/SACI60582.2024.10619863 (Letöltve: 2025. oktober 12.)

54 GAGANIS Chrysovalantis, HASAN Iftekhar, PAPADIMITRI Panagiota, TASIOU Menelaos, National culture and risk-taking: Evidence from the insurance industry, Journal of Business Research , vol. 97, pp. 104-116, 2019. ISSN:0148-2963 DOI:10.1016/J.JBUSRES.2018.12.037 (Letöltve: 2022. március 12.)

55 LI Kai, GRIFFIN Dale W., YUE Heng, ZHAO Longka, How Does Culture Influence Corporate Risk-Taking?, Journal of Corporate Finance , vol. 23, pp. 1-22, 2013. ISSN:0929-1199 DOI:10.1016/J.JCORPFIN.2013.07.008 (Letöltve: 2016. április 20.)

56 HOFSTEDE Geert, Insurance as a product of national values, The Geneva Papers on Risk and Insurance - Issues and Practice , vol. 20, no. 4, pp. 423-429, 1995. ISSN:1018-5895 DOI:10.1057/GPP.1995.36 (Letöltve: 2016. március 20.)

57 DA VEIGA Adele, ELOFF Jan, A framework and assessment instrument for information security culture, Computers & Security , vol. 29, no. 2, pp. 196-207, 2010 március. ISSN:0167-4048 DOI:10.1016/j.cose.2009.09.002 (Letöltve: 2016. március 10.)

58 LAZÁNYI Kornélia, A biztonsági kultúra szerepe a vezetői döntések támogatásában = THE ROLE OF SAFETY CULTURE IN SUPPORTING THE LEADERS' DECISION MAKING, TAYLOR: GAZDÁLKODÁS- ÉS SZERVEZÉSTUDOMÁNYI FOLYÓIRAT: A VIRTUÁLIS INTÉZET KÖZÉP-EURÓPA KUTATÁSÁRA KÖZLEMÉNYEI , vol. 8, no. 1, pp. 143-150, 2016. ISSN:2064-4361 https://ojs.bibl.u-szeged.hu/index.php/taylor/article/view/12993/12849 (Letöltve: 2023. február 8.)

59 MICHELBERGER Pál, LÁBODI Csaba: "Vállalati információbiztonság szervezése" in *Vállalkozásfejlesztés a XXI. században II.*, NAGY Imre Zoltán, Ed. Budapest, Magyarország: Óbudai Egyetem, 2013 , pp. 241-302 ISBN 978-615-5018-33-6. http://kgk.uni-obuda.hu/sites/default/files/10_Michelberger_Labodi.pdf (Letöltve: 2022. december 29.)

60 SZABÓ Attila, A biztonság szemüvegén keresztül, JövőKép , pp. 36-37, 2014. ISSN:2061-5035 http://docplayer.hu/docview/25/5700143/#file=/storage/25/5700143/5700143.pdf (Letöltve: 2015. szepember 10.)

61 KESZTHELYI András: "Some Special Fields of Data Security" in *Symposium for Young Researchers 2007: Proceedings*. Budapest: Óbudai Egyetem, 2007 , pp. 91-97 ISBN: 978-963-7154-64-5. https://kgk.uni-obuda.hu/sites/default/files/Keszthelyi_Andras.pdf (Letöltve: 2015. január 10.)

62 SÁNDOR Barnabás, RAJNAI Zoltán, Cyber Security Analysis of Smart Buildings from a Cyber Security Architecture Point of View, Interdisciplinary Description of Complex Systems , vol. 21, no. 2, pp. 141-147, 2023. https://www.indecs.eu/2023/indecs2023-pp141-147.pdf DOI:10.7906/indecs.21.2.2 (Letöltve: 2024. február 10.)

63 BLIZZARD Sonia, Coming full circle: are there benefits to BYOD?, Computer Fraud & Security , vol. 2015, no. 2, pp. 18-20, 2015. ISSN:1361-3723 DOI:10.1016/S1361-3723(15)30010-5 (Letöltve: 2018. oktober 10.)

64 HOVAV Anat, PUTRI Frida Ferdani, This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy, Pervasive and Mobile Computing , vol. 32, pp. 35-49, 2016. ISSN:1574-1192 DOI:10.1016/J.PMCJ.2016.06.007 (Letöltve: 2018. február 10.)

65 ZAHADAT Nima, BLESSNER Paul, BLACKBURN Timothy, OLSON Bill A., BYOD security engineering, Computers & Security , vol. 55, pp. 81-99, 2015. ISSN:0167-4048 DOI:10.1016/J.COSE.2015.06.011 (Letöltve: 2016. február 17.)

66 VIGNESH U., ASHA S., Modifying Security Policies Towards BYOD, Procedia Computer Science , vol. 50, pp. 511-516, 2015. ISSN:1877-0509 DOI:10.1016/J.PROCS.2015.04.023 (Letöltve: 2016. február 10.)

67 DOWNER Kathleen, BHATTACHARYA Maumita, "BYOD Security: A New Business Challenge" in *2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)*, 2015 , pp. 1128-1133. ISBN: 978-1-5090-1893-2 DOI:10.1109/SMARTCITY.2015.221 (Letöltve: 2016. február 10.)

68 Macmillan Dictionary. BYOD ABBREVIATION. https://www.macmillandictionary.com/dictionary/british/byod (Letöltve: 2022. december 27.)

69 BUDAI Balázs Benjámin: A közigazgatás újragondolása [Digitális kiadás.];. Budapest Akadémiai Kiadó, 2017. ISBN 978-963-454-065-6

70 BAILLETTE Paméla, BARLETTE Yves, BYOD-related innovations and organizational change for entrepreneurs and their employees in SMEs, Journal of Organizational Change Management , vol. 31, no. 4, pp. 839-851, 2018. ISSN:0953-4814 DOI:10.1108/JOCM-03-2017-0044 (Letöltve: 2023. február 8.)

71 JOBBÁGY Szabolcs, A negyedik generációs hadviselés infokommunikációs aspektusai - Fogalmi kitekintő, Hadmérnök , vol. 12, no. 1, pp. 203-213, 2017. ISSN:1788-1919 http://hadmernok.hu/171_16_jobbagy.pdf (Letöltve: 2022. február 17.)

72 ALBERTS David S. , GARSTKA John, STEIN Frederick P.: Network centric warfare: Developing and leveraging information superiority;. CCRP, 1999. ISBN: 978-1-57906-019-0 https://apps.dtic.mil/sti/tr/pdf/ADA406255.pdf (Letöltve: 2022. szepember 26.)

73 NATO, "NATO 2030: United for a New Era. Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General," Brussels, 2020. https://s.rfi.fr/media/display/7260c324-3550-11eb-8090-005056bff430/201125%20Nato%202030.pdf (Letöltve: 2026. január 10.)

74 RID Thomas, Cyber War Will Not Take Place, Journal of Strategic Studies , vol. 35, pp. 5-32, 2012. DOI:10.1080/01402390.2011.608939 (Letöltve: 2025. szepember 12.)

75 REASON James: Human Error;. Cambridge Cambridge University Press., 1991. ISBN: 978-1-139-06236-7

76 DHINGRA Madhavi, Legal Issues in Secure Implementation of Bring Your Own Device (BYOD), Procedia Computer Science , vol. 78, pp. 179-184, 2016. ISSN:1877-0509 DOI:10.1016/J.PROCS.2016.02.030 (Letöltve: 2017. február 2.)

77 Information Security Buzz. (2016. február) Top 10 Hacking Methods. https://informationsecuritybuzz.com/study-research/top-10-hacking-methods/ (Letöltve: 2022. december 27.)

78 HARRIS Mark A., PATTEN Karen P., Mobile device security considerations for small- and medium-sized enterprise business mobility, Information Management & Computer Security , vol. 22, no. 1, pp. 97-114, 2014. ISSN:0968-5227 DOI:10.1108/IMCS-03-2013-0019 (Letöltve: 2016. február 10.)

79 KOH Eun Byol: "A Study on Security Threats and Dynamic Access Control Technology for BYOD, Smart-work Environment" in *Proceedings of the International Multi Conference of Engineers and Computer Scientists*. Hong Kong, 2014 , pp. 12–14 ISSN:2078-0966. http://www.iaeng.org/publication/IMECS2014/IMECS2014_pp634-639.pdf (Letöltve: 2019. február 15.)

80 HASSAN Mohammad Khaled Al, BYOD Technological: Next Generation Business Development Programs for Future Accelerations, Innovations and Employee Happiness, International Journal of Computer Applications , vol. 165, no. 10, pp. 4-14, 2017. ISSN:0975-8887 DOI:10.5120/ijca2017913929 (Letöltve: 2018. február 8.)

81 TOPERESU B-Abee, BELLE Jean-Paul Van, Organisational Capabilities Required for Enabling Employee Mobility through Bring- Your-Own-Device Concept, Business Systems Research , vol. 8, no. 1, pp. 17-29, 2017. ISSN:1847-9375 DOI:10.1515/BSRJ-2017-0002 (Letöltve: 2018. március 10.)

82 DAS Amit, KHAN Habib Ullah, Security behaviors of smartphone users, Information and Computer Security , vol. 24, no. 1, pp. 116-134, 2016. ISSN:2056-4961 DOI:10.1108/ICS-04-2015-0018 (Letöltve: 2019. február 3.)

83 KADENA Esmeralda, KOVÁCS Tibor, The need for BYOD security strategy, Hadmérnök , vol. 12 (4), pp. 138-145, 2017 december. ISSN:1788-1929 http://hadmernok.hu/174_14_kadena.pdf (Letöltve: 2023. február 8.)

84 TOKUYOSHI Brian, The security implications of BYOD, Network Security , vol. 2013, no. 4, pp. 12-13, 2013. ISSN:1353-4858
DOI:10.1016/S1353-4858(13)70050-3 (Letöltve: 2017. február 3.)

85 DOMBORA Sándor, MICHELBERGER Pál, Információbiztonság szerepe az üzleti folyamatokban, INTERNATIONAL JOURNAL OF ENGINEERING AND MANAGEMENT SCIENCES / MŰSZAKI ÉS MENEDZSMENT TUDOMÁNYI KÖZLEMÉNYEK , 2016. ISSN: 2498-700X
https://ojs.lib.unideb.hu/IJEMS/article/view/4807/4540
DOI:10.21791/IJEMS.2016.1.17. (Letöltve: 2017. február 10.)

86 LECLERCQ - VANDELANNOITTE Aurélie, Managing BYOD: how do organizations incorporate user-driven IT innovations?, Information Technology & People , vol. 28, no. 1, pp. 2-33, 2015. ISSN:0959-3845
DOI:10.1108/ITP-11-2012-0129 (Letöltve: 2016. február 16.)

87 MICHELBERGER P., HORVÁTH J., BEINSCHRÓTH G.K., The Employe - An Information Security Risk, ACTA OECONOMICA UNIVERSITATIS SELYE , vol. 2, no. 1, pp. 187-200, 2013. ISSN 2644-5212
http://acta.fei.ujs.sk/uploads/papers/finalpdf/AOUS_2(1)_from22to22.pdf
(Letöltve: 2022. december 27.)

88 EM360 Tech. (2018. március) Top 10 companies supporting bring-your-own-device culture. https://em360tech.com/tech-news/top-ten/top-10-companies-supporting-bring-device-culture/ (Letöltve: 2022. december 27.)

89 GARETH James, Smartphone risk: Malicious threats to Smartphones, Network Security archive , vol. 2004, no. 8, pp. 5-7, 2004. ISSN:1353-4858 DOI:10.1016/S1353-4858(04)00115-1 (Letöltve: 2023. február 8.)

90 PROTALINSKI Emil. (2014. március) F-Secure: Android accounted for 97% of all mobile malware in 2013, but only 0.1% of those were on Google Play. http://thenextweb.com/google/2014/03/04/f-secure-android-accounted-97-mobile-malware-2013-0-1-google-play/ (Letöltve: 2022. december 27.)

91 Kaspersky lab. (2014. április) IT threat evolution Q1 2014. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08081202/q1-it-threats-en.pdf (Letöltve: 2022. december 27.)

92 CVE Details. Android Vulnerability Statistics. https://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224 (Letöltve: 2022. december 27.)

93 SHINDER Littlejohn Debra. (2014. szeptember) iOS 8 fixes 53 security flaws in iPhone and iPad. https://techtalk.gfi.com/ios-8-fixes-53-security-flaws-in-iphone-and-ipad/ (Letöltve: 2022. december 27.)

94 CVE Details. Iphone Os Vulnerability Statistics. https://www.cvedetails.com/product/15556/Apple-Iphone-Os.html?vendor_id=49 (Letöltve: 2022. december 27.)

95 Kaspersky. (2025. szepember) Kaspersky report: Attacks on smartphones increased in the first half of 2025. https://www.kaspersky.com/about/press-releases/kaspersky-report-attacks-on-smartphones-increased-in-the-first-half-of-2025 (Letöltve: 2026. január 17.)

96 Zimperium. (2024) 2024 Global Mobilethreat Report. https://lp.zimperium.com/hubfs/Reports/Global%20Mobile%20Threat%20Report%202024%20FINAL%20(1).pdf (Letöltve: 2025. május 10.)

97 Lookout. (2024) Mobile Threat Landscape Report Q3 2024. https://www.lookout.com/threat-intelligence/report/q3-2024-mobile-landscape-threat-report-copy (Letöltve: 2025. február 10.)

98 Verizon. (2025) 2024 MobileSecurity Index. https://www.verizon.com/business/resources/T6bb/reports/2024-mobile-security-index.pdf (Letöltve: 2025. február 10.)

99 itsecurityguru. (2020. oktober) 8 Phones left in each London taxi each year, leads to security concerns. https://www.itsecurityguru.org/2014/10/06/8-phones-left-london-taxi-year-leads-security-concerns/ (Letöltve: 2022. november 16.)

100 LAZÁNYI Kornélia, A biztonsági kultúra, TAYLOR:GAZDÁLKODÁS- ÉS SZERVEZÉSTUDOMÁNYI FOLYÓIRAT: A VIRTUÁLIS INTÉZET KÖZÉP-EURÓPA KUTATÁSÁRA KÖZLEMÉNYEI , vol. 7, no. 1-2, pp. 398-405, 2015. ISSN:2064-4361 http://vikek.eu/wp-content/uploads/2015/10/TAYLOR_2015-nyomdai.pdf (Letöltve: 2023. február 8.)

101 MICHELBERGER Pál: "Risk Management for Business Trust" in *MEB 2014 : Management, Enterprise and Benchmarking in the 21st Century*, MICHELBERGER Pál, Ed. Budapest, Magyarország: Óbudai Egyetem, Keleti Károly Gazdasági Kar, 2014 , pp. 401-413. ISBN:978-615-5460-06-7. http://kgk.uni-obuda.hu/sites/default/files/28_Michelberger.pdf (Letöltve: 2015. január 17.)

102 KESZTHELYI András, About passwords, Acta Polytechnica Hungarica , vol. 10, no. 6, pp. 99-118, 2013. ISSN:1785-8860 DOI:10.12700/APH.10.06.2013.6.6 (Letöltve: 2015. január 17.)

103 WÓJTOWICZ Adam, JOACHIMIAK Krzysztof, Model for adaptable context-based biometric authentication for mobile devices, Personal and Ubiquitous Computing , vol. 20, no. 2, pp. 195-207, 2016. ISSN:1617-4909
DOI:10.1007/S00779-016-0905-0 (Letöltve: 2018. szepember 3.)

104 STAPOR Piotr Paweł, LASKOWSKI Dariusz Andrzej, Bring Your Own Device - providing reliable model of data access, Journal of Konbin , vol. 39, no. 1, pp. 41-56, 2016. ISSN:1895-8281
DOI:10.1515/JOK-2016-0031 (Letöltve: 2017. február 12.)

105 HOLLÓ Dóra, Hol a határ? Magánszféra kontra munkahely a digitális korban, Detektor plusz , no. 3, p. 35, 2015. ISSN:1217-9175
http://hplaw.hu/wp-content/uploads/2015/07/Detektor_2015_3_Holloestsai.pdf
(Letöltve: 2022. december 27.)

106 2012. I. törvény, 8. §.

107 FISHER Warren, ALLEN Charlotte, Road Warriors and Information Systems Security: Risks and Recommendations, Journal of Management Information and Decision Sciences , vol. 18, no. 1, p. 84, 2015. ISSN:1532-5806
http://faculty.sfasu.edu/fisherwarre/Road_Warrior_Fisher_Allen_JMIDS.pdf
(Letöltve: 2016. február 1.)

108 KESZTHELYI András: "Netháborúk kora" in *Új kihívások a tudományban és az oktatásban - Gazdaságtudományi szekció : Zborník medzinárodnej vedeckej konferencie Univerzity J. Selyeho – 2013 "Nové výzvy vo vede a vo vzdelávaní" Sekcia ekonomických vied*, GYÖRGY Juhász et al., Eds. Komárom, Magyarország : Selye János Egyetem, 2013 , pp. 149-170 ISBN:978-80-8122-074-6. (Letöltve: 2015. január 17.)

109 RSA Security Inc. (2007. december) The Confessions Survey: Office Workers Reveal Everyday Behavior That Places Sensitive Information at Risk. https://web.archive.org/web/20081121114611/http://www.rsa.com/company/news/releases/pdfs/RSA-insider-confessions.pdf (Letöltve: 2022. december 27.)

110 NELSON Joanne. (2015. november) CXO Unplugged. http://cxounplugged.com/2015/11/shadow-it-is-a-reality-for-most-cios/
(Letöltve: 2020. november 17.)

111 STUART Andrew, The dangers of file sync and sharing services, Computer Fraud & Security , vol. 2016, no. 11, pp. 10-12, 2016. ISSN:1361-3723 DOI:10.1016/S1361-3723(16)30090-2 (Letöltve: 2018. január 17.)

112 BROWNE Sean, LANG Michael, GOLDEN William, "Contextualising the insider threat: a mixed method study" , vol. WISP 2016 Proceedings, 13, 2016. https://aisel.aisnet.org/wisp2016/13/ (Letöltve: 2022. december 27.)

113 HANDEL Mark J., POLTROCK Steven, "Working around official applications: experiences from a large engineering project" in *Proceedings of the ACM 2011 conference on Computer supported cooperative work*, 2011 , pp. 309-312. ISBN: 978-1-4503-0556-3 DOI:10.1145/1958824.1958870 (Letöltve: 2016. február 10.)

114 GALLATTO Sara, CHEN Weifeng: "Security Management of Bring-Your-Own-Devices" in *Proceedings of the International Conference on Security and Management (SAM 2014)*, DAIMI Kevin, ARABNIA R. Hamid, Eds.: CSREA Press, 2015 , pp. 303-310 ISBN:978-1-60132-285-2.
http://worldcomp-proceedings.com/proc/p2014/SAM9733.pdf (Letöltve: 2019. február 10.)

115 KOO Chulmo, CHUNG Namho, KIM Hee Woong, Examining explorative and exploitative uses of smartphones: a user competence perspective, Information Technology & People , vol. 28, no. 1, pp. 133-162, 2015. ISSN:0959-3845 DOI:10.1108/ITP-04-2013-0063 (Letöltve: 2016. február 10.)

116 WALLI R. Stephen, The Arrival of the Mobile Internet Thanks to the Economics of Open Source Software, Open Source Business Resource , 2009 január. ISSN:1913-6102 http://timreview.ca/article/221 (Letöltve: 2015. január 10.)

117 LAZÁNYI Kornélia, Szervezeti biztonság és a munkahelyi stress kapcsolata, TAYLOR: GAZDÁLKODÁS- ÉS SZERVEZÉSTUDOMÁNYI FOLYÓIRAT: A VIRTUÁLIS INTÉZET KÖZÉP-EURÓPA KUTATÁSÁRA KÖZLEMÉNYEI , vol. 8, no. 5, pp. 24-31, 2016. ISSN:2064-4361
http://vikek.eu/wp-content/uploads/2016/10/Taylor2016.5.sz%C3%A1mNo26.pdf (Letöltve: 2023. február 8.)

118 Check Point Software Technologies Ltd. (2017. március) Preinstalled Malware Targeting Mobile Users. https://blog.checkpoint.com/2017/03/10/preinstalled-malware-targeting-mobile-users/ (Letöltve: 2022. december 27.)

119 Dr.Web. (2018. március) Doctor Web: over 40 models of Android devices delivered already infected from the manufacturers. https://news.drweb.com/show/?i=11749 (Letöltve: 2022. december 27.)

120 WALLS Jason, CHOO Kim-Kwang Raymond: "A Study of the Effectiveness Abs Reliability of Android Free Anti-Mobile Malware Apps" in *Mobile Security and Privacy*.: Syngress, 2017 , pp. 167-203 ISBN:978-0-12-804629-6. DOI:10.1016/B978-0-12-804629-6.00008-0 (Letöltve: 2018. február 16.)

121 JIA Yunhan Jack, CHEN Qi Alfred, LIN Yikai, KONG Chao, MAO Z. Morley: "Open Doors for Bob and Mallory: Open Port Usage in Android Apps and Security Implications" in *2nd IEEE European Symposium on Security and Privacy*.: University of Michigan, 2017 , pp. 190-203 ISBN:978-1-5090-5763-4. DOI:10.1109/EuroSP.2017.44 (Letöltve: 2018. február 10.)

122 ELAHI Haroon, WANG Guojun, LI Xu: "Smartphone Bloatware: An Overlooked Privacy Problem" in *Security, Privacy, and Anonymity in Computation, Communication, and Storage. SpaCCS 2017. Lecture Notes in Computer Science*.: Springer, Cham, 2017 , pp. 169-185 ISBN:978-3-319-72389-1. DOI:10.1007/978-3-319-72389-1_15 (Letöltve: 2018. február 7.)

123 LESWING Kif. (2017. Október) Apple gave Uber's app 'unprecedented' access to sensitive Apple features that can record iPhone screens. https://www.businessinsider.com/uber-iphone-app-secret-access-sensitive-apple-features-2017-10 (Letöltve: 2022. december 27.)

124 GIBBS Samuel. (2017. augusztus) Game of Thrones secrets revealed as HBO Twitter accounts hacked. https://www.theguardian.com/media/2017/aug/17/game-of-thrones-secrets-revealed-as-hbo-twitter-accounts-hacked (Letöltve: 2022. december 27.)

125 HERN Alex. (2018. január) Fitness tracking app Strava gives away location of secret US army bases. https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases (Letöltve: 2022. december 27.)

126 Kaspersky. (2018) Skygofree: highly advanced, powerful Android surveillance software active since 2014. https://www.kaspersky.com/about/press-releases/2018_skygofree-highly-advanced-powerful-android-surveillance-software-active-since-2014 (Letöltve: 2022. december 27.)

127 BUCHKA Nikita, KIVVA Anton, GALOV Dmitry. (2017. december) Jack of all trades. https://securelist.com/jack-of-all-trades/83470/ (Letöltve: 2022. december 27.)

128 YUKSEL Asim S., ZAIM Abdul H., AYDIN Muhammed A., A Comprehensive Analysis of Android Security and Proposed Solutions, International Journal of Computer Network and Information Security , vol. 6, no. 12, pp. 9-20, 2014. ISSN:2074-9104 DOI:10.5815/IJCNIS.2014.12.02 (Letöltve: 2015. február 10.)

129 RUSER Nathan. (2018. Január) Strava released their global heatmap. https://twitter.com/Nrg8000/status/957318498102865920 (Letöltve: 2022. december 27.)

130 LAIGNEE Barron, U.S. Soldiers are Accidentally Revealing Sensitive Locations by Mapping Their Exercise Routes., Time , 2018 január. https://time.com/5122495/strava-heatmap-military-bases/ (Letöltve: 2022. december 27.)

131 SZOLDRA Paul, A Russian Soldier's Instagram Posts May Be The Clearest Indication Of Moscow's Involvement In East Ukraine, Business Insider , 2014 július. https://www.businessinsider.com/russian-soldier-ukraine-2014-7 (Letöltve: 2022. december 27.)

132 BODNÁR Ádám. (2011. május) Nem sokat törődtek az Android biztonságával. https://www.hwsw.hu/hirek/46730/google-android-okostelefon-biztonsag-linux-dalvik.html (Letöltve: 2022. december 27.)

133 Computer Laboratory, University of Cambridge. (2015) AndroidVulnerabilities.org. http://androidvulnerabilities.org/ (Letöltve: 2022. december 27.)

134 PulseSecure. (2015) 2015 Mobile Threat Report. https://www.pulsesecure.net/download/pages/2819/PulseSecure_MobilityReport.pdf (Letöltve: 2022. november 28.)

135 International Organization for Standardization, Information technology — Security techniques — Information security management systems — Requirements (ISO/IEC 27001:2022), 2022.

136 International Organization for Standardization, Risk management — Guidelines (ISO 31000:2018),2018.

137 FORD Glenn. (2014. január) BYOD Demand and Information Security. http://cybersecurity-hq.blogspot.com/2014/02/byod-consumer-demand-and-information.html (Letöltve: 2022. december 27.)

138 CSERCSA Klaudia, RAJNAI Zoltán, Adatvédelem és információbiztonság: az online térben fellelhető veszélyforrások, adathalászati módszerek (social engineering), Biztonságtudományi Szemle , vol. 7., no. 2., 2025. DOI:10.12700/btsz.2025.7.2.49 (Letöltve: 2025. november 9.)

139 2012. I. törvény, Munka Törvénykönyve (VIII. fejezet 51. §).

140 HOLLÓ Dóra. (2014. február) BYOD: céges és privát adatok egy dobozban. https://computerworld.hu/uzlet/byod-ceges-es-privat-adatok-egy-dobozban-144359.html (Letöltve: 2022. december 27.)

141 MICHELBERGER Pál, BEKE Éva, Stratégiai döntéseknél alkalmazható összesített kockázati mutatószámok meghatározása: Egy döntéstámogató módszer alkalmazási feltételei, BELÜGYI SZEMLE: A BELÜGYMINISZTÉRIUM SZAKMAI TUDOMÁNYOS FOLYÓIRATA , pp. 13-24., 2020. ISSN 2677-1632 http://real.mtak.hu/112744/1/Michelberger-BekeBelugyiSzemle2020.evi7.szam13-24.pdf (Letöltve: 2021. február 10.)

142 Oxford Economics, SAMSUNG. (2022. április) Maximizing Mobile Value To BYOD or not to BYOD? https://image-us.samsung.com/SamsungUS/samsungbusiness/short-form/maximizing-mobile-value-2022/Maximizing_Mobile_Value_2022-Final.pdf (Letöltve: 2022. december 27.)

143 MAYNARD Bright Harold: Industrial Engineering Handbook;. New York McGraw-Hill, 1971. ISBN:978-0-7041-0844-8

144 BRADLEY Loucks, J., Macaulay, J., Medcalf, R., Buckalew, L., J.. (2012) BYOD: A Global Perspective, Harnessing Employee-Led Innovation. http://www.cisco.com/web/about/ac79/docs/re/BYOD_Horizons-Global.pdf (Letöltve: 2022. december 27.)

145 IVANTI. (2025. oktober) Ivanti Report Reveals Only One in Three Organizations Have Implemented Zero Trust Network Access for Remote Workers. https://www.ivanti.com/company/announcements/2025/ivanti-report-reveals-only-one-in-three-organizations-have-implemented-zero-trust-network-access-for-remote-workers (Letöltve: 2025. november 7.)

146 TABALIPA Alexander, Bridging the Mobile Trust Gap: A Zero Trust Framework for Consumer-Facing Applications, SSRN , 2025. https://ssrn.com/abstract=5398024 DOI:10.48550/arXiv.2508.16662 (Letöltve: 2025. november 7.)

147 EU Funding Portal. (2026) Call for proposals to support the development of secure digital military mobility system. https://eufundingportal.eu/call-for-proposals-to-support-the-development-of-secure-digital-military-mobility-system/ (Letöltve: 2026. január 7.)

148 OLECH Aleksander, STRUCL Damjan: The evolution of cyber forces in NATO countries;. Tallin NATO Cooperative Cyber Defence Centre of Excellence, 2025. https://ccdcoe.org/uploads/2025/07/The_evolution_of_cyber_forces_in_NATO_countries.pdf (Letöltve: 2026. január 7.)

149 HOLZAPFEL Jens. (2025) The Swedish Institute of International Affairs. https://www.ui.se/globalassets/ui.se-eng/publications/ui-publications/2025/final-layout-ui-brief-no.-5-2025.pdf (Letöltve: 2026. január 7.)

150 BAYLISS DANIEL Lucia Angelo, Martin-Blanco Alvaro, Reding Dale F., Regan Laura A., Wells Bryan De, Science & Technology Trends: 2023-2043 Vol. 1, STO-OCS-001 , 2023. https://www.sto.nato.int/document/science-technology-trends-2023-2043-vol-1/ (Letöltve: 2026. január 7.)

151 DERACHE Georges et al., LoRaWAN attack in military use case, 2024. DOI:10.48550/arXiv.2412.18447 (Letöltve: 2026. január 7.)

152 LUTZ Isabella, HILL Ava, VALENTI Matthew, Privacy-Preserving Authentication for Secure Military 5G Networks, 2025. DOI:10.1109/MILCOM64451.2025.11310655 (Letöltve: 2026. január 7.)

TÁBLÁZATJEGYZÉK

ÁBRAJEGYZÉK

PUBLIKÁCIÓK

A doktori értekezéshez kapcsolódó publikációk

[P1] FEHÉR-POLGÁR, P., & MICHELBERGER, P. (2018). A sajáttulajdonú mobil eszközök információbiztonsági kockázatai: The information security risks of the BYOD. International Journal of Engineering and Management Sciences, 3(4), 176–185. ISSN: 2498-700X. https://doi.org/10.21791/IJEMS.2018.4.16.

[P2] FEHÉR-POLGÁR, P. (2018). BYOD, hozd magaddal a saját biztonsági kockázataid. In P. FEHÉR-POLGÁR (Szerk.), Kutatók éjszakája – Fiatal kutatók előadásai 2018 (p. 9). Óbudai Egyetem Keleti Károly Gazdasági Kar. ISBN: 978-963-449-102-6.

[P3] FEHÉR-POLGÁR, P., & NÉMETH, Z. (2016). Safety consciousness of the mobile phone users. In A. SZAKÁL (Szerk.), Proceedings of the 11th IEEE International Symposium on Applied Computational Intelligence and Informatics (SACI 2016) (pp. 345–348). IEEE. ISBN: 978-1-5090-2380-6. https://doi.org/10.1109/SACI.2016.7507399

[P4] FEHÉR-POLGÁR, P. (2015). Felsőoktatásban tanuló hallgatók biztonságtudatossága. Taylor: Gazdálkodás- és Szervezéstudományi Folyóirat, 7(3-4), 15–21. ISSN: 2676-8917.

[P5] FEHÉR-POLGÁR, P. (2015). A biztonságot veszélyeztető tényezőkkel kapcsolatos attitűdök vizsgálata egyetemi hallgatókon. Taylor: Gazdálkodás- és Szervezéstudományi Folyóirat, 7(1-2), 413–419. ISSN: 2676-8917.

[P6] FEHÉR-POLGÁR, P. (2015). Safety conscious of the students in higher education. In G. KRISTÓVÁ, P. SCHMIDT, J. BRIXOVÁ, & M. SZIVOSOVÁ (Szerk.), Trends and innovations in e-business, education and security: Proceedings of the Fourth International Scientific Videoconference of Scientists and PhD. students or candidates (pp. 8–16). Ekonomická Univerzita v Bratislave. ISBN: 978-80-225-3987-6.

[P7] FEHÉR-POLGÁR, P. (2014). Saját tulajdonú mobilinformatikai eszközök vállalati használatának jogi kérdései. In P. RÁCZ (Szerk.), IESB 2014: Nemzetközi Gépész és Biztonságtechnikai Szimpózium. Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar. ISBN: 978-615-5460-08-1.

[P8] FEHÉR-POLGÁR, P. (2014). Data security of mobile phones, from the aspect of university students. In P. MICHELBERGER (Szerk.), MEB 2014: Management, Enterprise and Benchmarking in the 21st Century (pp. 393–400). Óbudai Egyetem Keleti Károly Gazdasági Kar. ISBN: 978-615-5460-06-7.

[P9] MICHELBERGER, P., & FEHÉR-POLGÁR, P. (2020). BYOD security strategy (Aspects of a managerial decision). Journal of Security and Sustainability Issues, 9(4), 1135–1143. ISSN: 2029-7025. https://doi.org/10.9770/jssi.2020.9.4(1)

[P10] FEHÉR-POLGÁR, P., & MICHELBERGER, P. (2019). The information security risks of the BYOD, from theoretical point of view. In 2019 IEEE 17th International Symposium on Intelligent Systems and Informatics (SISY) (pp. 83–88). IEEE. https://doi.org/10.1109/SISY47553.2019.9111514

[P11] FEHÉR-POLGÁR, P. (2019). Managerial decision options about BYOD with the consideration of shadow IT. In P. SZIKORA & P. FEHÉR-POLGÁR (Szerk.), 17th International Conference on Management, Enterprise, Benchmarking. Proceedings (MEB 2019) (pp. 28–34). Óbuda University Keleti Károly Faculty of Business and Management. ISBN: 978-963-449-127-9.

[P12] FEHÉR-POLGÁR, P. (2020). Examination of IT risk-taking with modified DOSPERT questionnaire among university students. In A. KESZTHELYI, P. SZIKORA, & P. FEHÉR-POLGÁR (Szerk.), 18th International Conference on Management, Enterprise, Benchmarking. Proceedings (MEB 2020) (pp. 48–56). Óbudai Egyetem Keleti Károly Gazdasági Kar. ISBN: 978-963-449-223-8.

[P13] EISEMANN, G., & FEHÉR-POLGÁR, P. (2020). Safety consciousness in future employees. Macrotheme Review: A Multidisciplinary Journal of Global Macro Trends, 9(1), 74–84. ISSN: 2379-9765.

[P14] FEHÉR-POLGÁR, P. (2021). Measuring safetyconsciousness. In A. KELEMEN-ERDŐS, P. FEHÉR-POLGÁR, & A. POPOVICS (Szerk.), FIKUSZ 2021 XVI. International Conference Proceedings (pp. 22–27). Óbudai Egyetem, Keleti Károly Gazdasági Kar. ISBN: 978-963-449-274-0.

[P15] FEHÉR-POLGÁR, P. (2022). Can be the DOSPERT questioner used for measuring IT risk taking. In Á. CSISZÁRIK-KOCSIR, A. POPOVICS, & P. FEHÉR-POLGÁR (Szerk.), FIKUSZ 2022 XVII. International Conference Proceedings (pp. 637–645). Óbudai Egyetem. ISBN: 978-963-449-305-1.

[P16] FEHÉR-POLGÁR, P. (2022). Results upon two samples of university students on safety consciousness in smartphone usage. In Á. CSISZÁRIK-KOCSIR, A. POPOVICS, & P. FEHÉR-POLGÁR (Szerk.), FIKUSZ 2022 XVII. International Conference Proceedings (pp. 123–128). Óbudai Egyetem. ISBN: 978-963-449-305-1.

[P17] FEHÉR-POLGÁR, P. (2023). Testing ICT security risk attitude questions on a small scale level for future use. In M. GARAI-FODOR, Á. CSISZÁRIK-KOCSIR, A. POPOVICS, & T. EDŐCS (Szerk.), XVII. FIKUSZ 2023 International Conference: Proceedings (pp. 362–368). Óbuda University Keleti Károly Faculty of Business and Management. ISBN: 978-963-449-341-9.

[P18] FEHÉR-POLGÁR, P. (2023). Usage of self-assessment questionnaires in safety and security sciences - a literature review. In M. GARAI-FODOR, Á. CSISZÁRIK-KOCSIR, A. POPOVICS, & T. EDŐCS (Szerk.), XVII. FIKUSZ 2023 International Conference: Proceedings (pp. 268–272). Óbuda University Keleti Károly Faculty of Business and Management. ISBN: 978-963-449-341-9.

[P19] FEHÉR-POLGÁR, P. (2023). Alkalmazható-e a DOSPERT kérdőív informatikai kockázatvállalási hajlandóság mérésére? In P. SZIKORA (Szerk.), Társadalom, Informatika és Gazdaság Kutatócsoport Konferencia kiadvány: TIGKONF 2023 (pp. 132–141). Óbudai Egyetem, Keleti Károly Gazdasági Kar. ISBN: 978-963-449-342-6.

[P20] FEHÉR-POLGÁR, P. (2024). IT biztonságtudatosság fontossága. In P. SZIKORA (Szerk.), Társadalom, Informatika és Gazdaság Kutatócsoport Konferencia kiadvány: TIGKONF 2024 (pp. 106–111). Óbudai Egyetem, Keleti Károly Gazdasági Kar. ISBN: 978-963-449-370-9.

[P21] SZIKORA, P., & FEHÉR-POLGÁR, P. (2025). Kiberbiztonsági és felhasználói kihívások a digitális korban: párhuzamok a BYOD és az önvezető autók között. In P. SZIKORA (Szerk.), Társadalom, Informatika és Gazdaság Kutatócsoport Konferencia kiadvány: TIGKONF 2025 (pp. 69–76). Óbudai Egyetem, Keleti Károly Gazdasági Kar. ISBN: 978-963-449-407-2.

[P22] SZIKORA, P., & FEHÉR-POLGÁR, P. (2025). Cybersecurity and user challenges in the digital age: parallels between BYOD and self-driving cars. In P. SZIKORA & A. KESZTHELYI (Szerk.), 23rd International Conference on Management, Enterprise, Benchmarking. Proceedings III. (MEB 2025) (pp. 173–179). Óbuda University Keleti Károly Faculty of Business and Management. ISBN: 978-963-449-386-0.

[P23] FEHÉR-POLGÁR, P., & SZIKORA, P. Domain-Specific Risk Perception in IT Security Decisions: Empirical Examination of the Modified Domain-Specific Risk-Taking (DOSPERT) Framework. (2026). The Eurasia Proceedings of Educational and Social Sciences, 48, 1-7. https://doi.org/10.55549/epess.1006

[P24] FEHÉR-POLGÁR, P., & SZIKORA, P. (in press). Demographic differences in IT security risk-taking: Implications for targeted training and prevention.

[P25] FEHÉR-POLGÁR, P. & SZIKORA, P. (in press). Cross-domain asymmetry in risk–benefit weighting: Evidence for benefit-dominant decision architecture in IT security contexts.

További tudományos közlemények

[P26] HOLICZA, P., & FEHÉR-POLGÁR, P. (2017). The role of IT in international student mobility: The Y-generation case. In A. SZAKÁL (Szerk.), IEEE 15th International Symposium on Intelligent Systems and Informatics: SISY 2017 (pp. 147–150). IEEE. ISSN: 1949-0488. https://doi.org/10.1109/SISY.2017.8080542

[P27] THINH, D. V., & FEHÉR-POLGÁR, P. (2016). Culture and environmental awareness, a study on Hungarian higher education students. In I. MIHAJLOVIĆ et al. (Szerk.), Environmental awareness as a universal European value. University of Belgrade, Technical Faculty in Bor, Engineering Management Department. ISBN: 978-86-6305-044-0. http://media.sjm06.com/2016/02/Monograph-Environmental-awareness-as-a-universal-European-Value.pdf

[P28] ROQUE, J., DE MIRANDA, J. L., & FEHÉR-POLGÁR, P. (2019). Risk mitigation and preventing medicines shortages. In J. L. DE MIRANDA, H. JENZER, & A. P. BARBOSA-POVOA (Szerk.), Pharmaceutical supply chains - Medicines shortages (Chapter 6, pp. 103–109). Springer International Publishing. ISBN: 978-3-030-15398-4. https://doi.org/10.1007/978-3-030-15398-4_6

[P29] LAZÁNYI, K., FEHÉR-POLGÁR, P., & VIDA, I. (2020). Identification of the most important European productivity factors through the dimension reduction. Ekonomicko-manazerske spektrum / Economic and Managerial Spectrum, 14(1), 77–86. ISSN: 2585-7258. https://doi.org/10.26552/ems.2020.1.77-86

[P30] FODOR, N., & FEHÉR-POLGÁR, P. (2022). E-document, or the human factor in the security of electronic storage of personal documents. In Á. CSISZÁRIK-KOCSIR, A. POPOVICS, & P. FEHÉR-POLGÁR (Szerk.), FIKUSZ 2022 XVII. International Conference Proceedings (pp. 637–645). Óbudai Egyetem. ISBN: 978-963-449-305-1.

[P31] BERNÁTH, Á., & FEHÉR-POLGÁR, P. (2023). Adatgyűjtési módszerek jogi szabályozása és a velük kapcsolatos biztonságtudatosság. In P. SZIKORA (Szerk.), Társadalom, Informatika és Gazdaság Kutatócsoport Konferencia kiadvány: TIGKONF 2023 (pp. 153–169). Óbudai Egyetem, Keleti Károly Gazdasági Kar. ISBN: 978-963-449-342-6.

[P32] FEHÉR-POLGÁR, P. (2024). Artificial intelligence as an innovative tool for e-commerce. In M. GARAI-FODOR, Á. CSISZÁRIK-KOCSIR, A. POPOVICS, & T. EDŐCS (Szerk.), XIX. FIKUSZ 2024 International Conference Proceedings (pp. 87–91). Óbuda University Keleti Károly Faculty of Business and Management. ISBN: 978-963-449-416-4.

[P33] FEHÉR-POLGÁR, P. (2024). Az e-kereskedelem legfontosabb IT biztonsági kihívásai irodalomkutatás alapján. In P. SZIKORA (Szerk.), Társadalom, Informatika és Gazdaság Kutatócsoport Konferencia kiadvány: TIGKONF 2024 (pp. 30–36). Óbudai Egyetem, Keleti Károly Gazdasági Kar. ISBN: 978-963-449-370-9.

[P34] SZIKORA, P., & FEHÉR-POLGÁR, P. (2025). Az önvezető járművek társadalmi elfogadását befolyásoló technológiai bizalom és kockázatészlelés vizsgálata. In J. VARGA, Á. CSISZÁRIK-KOCSIR, & M. GARAI-FODOR (Szerk.), Vállalkozásfejlesztés a XXI. században III. kötet: Generációs attitűdök, szervezeti kihívások és technológiai megújulás a vállalkozásfejlesztésben (pp. 240–253). Óbudai Egyetem, Keleti Károly Gazdasági Kar. ISBN: 978-963-449-387-7.

[P35] FEHÉR-POLGÁR, P. (2025). Autonomous vehicles at the intersection of people, technology, and law: Social acceptance, testing, liability, and human factors. In M. GARAI-FODOR, Á. CSISZÁRIK-KOCSIR, A. POPOVICS, & T. EDŐCS (Szerk.), XX. FIKUSZ 2025 International Conference: Proceedings (pp. 107–121). Óbuda University Keleti Károly Faculty of Business and Management.

[P36] FEHÉR-POLGÁR, P. (2025). Autonóm járművek az ember, a technika és a jog metszéspontján: Társadalmi elfogadás, tesztelés, felelősség és humán tényezők. In P. SZIKORA (Szerk.), Társadalom, Informatika és Gazdaság Kutatócsoport Konferencia kiadvány: TIGKONF 2025 (pp. 25–39). Óbudai Egyetem, Keleti Károly Gazdasági Kar. ISBN: 978-963-449-407-2.

[P37] SZIKORA, P., & FEHÉR-POLGÁR, P. (2026). Technological trust and social risk perception in the acceptance of self-driving cars. In A. SZAKÁL (Szerk.), IEEE 24th World Symposium on Applied Machine Intelligence and Informatics (SAMI 2026) (pp. 187–192). Institute of Electrical and Electronics Engineers (IEEE).

Oktatási művek

[P38] FEHÉR-POLGÁR, P. (2019). A magyar B2C e-kereskedelem jelene. In P. FEHÉR-POLGÁR (Szerk.), Esettanulmány kötet (pp. 27–36). Óbudai Egyetem, Keleti Károly Gazdasági Kar. ISBN: 978-963-449-155-2.

Konferencia absztrakt publikációk

[P39] DUONG, T., & FEHÉR-POLGÁR, P. (2016). Culture and environmental awareness, a study on Hungarian higher education students. In Ž. ŽIVKOVIĆ & P. ĐORĐEVIĆ (Szerk.), Book of abstracts of 12th International May Conference on Strategic Management – IMKSM2016 (p. 151). University of Belgrade.

[P40] FEHÉR-POLGÁR, P. (2018). BYOD, hozd magaddal a saját biztonsági kockázataid. In K. LAZÁNYI (Szerk.), Kutatók éjszakája - Fiatal kutatók előadásai: Absztrakt kötet (p. 8). Óbudai Egyetem, Keleti Károly Gazdasági Kar.

[P41] FEHÉR-POLGÁR, P. (2019). Managerial decision options about BYOD with the consideration of shadow IT. In P. SZIKORA & P. FEHÉR-POLGÁR (Szerk.), 17th International Conference on Management, Enterprise, Benchmarking. Abstract Booklet (MEB 2019) (p. 38). Óbuda University Keleti Károly Faculty of Business and Management.

[P42] FEHÉR-POLGÁR. (2020). Examination of IT risk-taking with modified DOSPERT questionnaire among university students. In A. KESZTHELYI, P. SZIKORA, & P. FEHÉR-POLGÁR (Szerk.), 18th International Conference on Management, Enterprise, Benchmarking. Abstract Booklet (MEB 2020) (p. 41). Óbudai Egyetem, Keleti Károly Gazdasági Kar.

[P43] FEHÉR-POLGÁR, P. (2021). Measuring safety consciousness. In A. KELEMEN-ERDOS, A. POPOVICS, & P. FEHER-POLGAR (Szerk.), Aniko Kelemen-Erdos. XVI. FIKUSZ 2021 International Conference: Abstract Book. (p. 23). Óbudai Egyetem, Keleti Károly Gazdasági Kar. ISBN: 978-963-449-271-9.

[P44] FEHÉR-POLGÁR, P. (2021). Security questions of Covid-19 and the home office – Bring your own device in the home office world too! In P. FEHÉR-POLGÁR, A. KESZTHELYI, & P. SZIKORA (Szerk.), MEB — 19th International Conference on Management, Enterprise, Benchmarking. Abstract Booklet (MEB 2021). Óbuda University Keleti Károly Faculty of Business and Management.

[P45] FEHÉR-POLGÁR, P. (2022). Results upon two samples of university students on safety consciosness in smartphone usage. In A. CSISZARIK-KOCSIR, A. POPOVICS, & P. FEHER-POLGAR (Szerk.), XVII. FIKUSZ 2022 International Conference: Abstract Book (p. 22). Óbudai Egyetem.

[P46] FEHÉR-POLGÁR, P. (2022). Az okoseszközökkel kapcsolatos biztonságtudatosság fontossága. In P. FEHÉR-POLGÁR, P. SZIKORA, & A. KESZTHELYI (Szerk.), 20th InternationalConference on Management, Enterprise, Benchmarking. Abstract Booklet (MEB 2022) (p. 61). Óbudai Egyetem, Keleti Károly Gazdasági Kar.

[P47] FEHÉR-POLGÁR, P. (2022). Safety consciousness in a group of university students on smartphone usage. In P. FEHÉR-POLGÁR, P. SZIKORA, & A. KESZTHELYI (Szerk.), 20th International Conference on Management, Enterprise, Benchmarking. Abstract Booklet (MEB 2022) (p. 42). Óbudai Egyetem, Keleti Károly Gazdasági Kar.

[P48] FEHÉR-POLGÁR, P. (2023). Usage of self-assessment questionnaires in safety and security sciences - a literature review. In A. KESZTHELYI & P. SZIKORA (Szerk.), 21th International Conference on Management, Enterprise and Benchmarking. Abstract Booklet (MEB 2023) (p. 54). Óbudai Egyetem, Keleti Károly Gazdasági Kar.

[P49] FEHÉR-POLGÁR, P. (2024). Artificial intelligence as an innovative tool for e-commerce. In M. GARAI-FODOR, Á. CSISZÁRIK-KOCSIR, A. POPOVICS, & T. EDŐCS (Szerk.), XIX. FIKUSZ 2024 International Conference: FIKUSZ '24 Symposium for Young Researchers: Abstract Book (p. 45). Óbudai Egyetem, Keleti Károly Gazdasági Kar.

[P50] FEHÉR-POLGÁR, P. (2024). Biztonságtudatossági elvárások a gyakorlatban a B2C E-kereskedelem példáján keresztül. In A. KESZTHELYI & P. SZIKORA (Szerk.), 22nd International Conference on Management, Enterprise and Benchmarking. Abstract Booklet. MEB 2024. (p. 81). Óbuda University Keleti Károly Faculty of Business and Management.

[P51] FEHÉR-POLGÁR, P. (2025). Recent incidents in Smart Phone security and concerns for BYOD. In A. KESZTHELYI & P. SZIKORA (Szerk.), 23rd International Conference on Management, Enterprise and Benchmarking. Abstract Booklet. MEB 2025 (p. 80). Óbuda University Keleti Károly Faculty of Business and Management.

FÜGGELÉK

1. számú függelék Kutatási kérdések, a hozzájuk kapcsolódó hipotézis(ek), a megfogalmazott tézisek és azok empirikus magyarázata

Kutatási kérdés	Kapcsolódó hipotézis(ek)	Tézis szövege	Empirikus magyarázat
C1: Az IT-biztonsági kockázatvállalás mint önálló, doménspecifikus konstrukció azonosítása és mérési kereteinek validálása	H1: A DOSPERT eredeti doménjei nem képesek szignifikáns mértékben előre jelez-ni az IT-biztonsági kockázati kérdésekre adott válaszokat. H3: A különböző szakok hallgatói között szignifikáns különbség mutatható ki az IT-biztonsági kockázatok észlelésében. H8: Az életkor az általános kockázatvállalási dimenziók kontrollálása mellett szignifikáns magyarázóerővel bír az IT-biztonsági kockázatvállalás tekintetében. H9: A nem az általános kockázatvállalási dimenziók kontrollálása mellett is szignifikáns kapcsolatban áll az IT-biztonsági kockázatvállalással.	T1: Az IT-biztonsági kockázatvállalás mint önálló konstrukció Empirikusan kimutattam, hogy az IT-biztonsági kockázatvállalás nem írható le megfelelően a DOSPERT eredeti doménstruktúrájával, és a technikai képzés, valamint az általános kockázatvállalási dimenziók kontrollálása mellett is szignifikáns szerepet játszanak demográfiai tényezők (életkor, nem). Eredményeim alapján az IT-biztonsági kockázatvállalás részben autonóm, kontextus-specifikus konstrukcióként értelmezhető.	A H1 vizsgálata során az IT-biztonsági elemekre futtatott többszörös regresszióelemzések alacsony determinációs együtthatókat eredményeztek, az eredeti DOSPERT-doménváltozók többsége nem bizonyult szignifikáns prediktornak, és a kimutatható gyenge kapcsolatok sem alkottak konzisztens mintázatot. Ez arra utal, hogy az IT-biztonsági döntések nem vezethetők vissza az eredeti doménstruktúrára. A H3 eredményei szerint a különböző szakok hallgatói között csak részleges és nem konzisztens különbségek mutatkoztak az IT-kockázatok észlelésében, vagyis a technikai vagy informatikai képzés önmagában nem determinál magasabb kockázati érzékenységet. A H8 és H9 hierarchikus regressziós eredményei azt mutatták, hogy az életkor és a nem az általános kockázatvállalási dimenziók kontrollálása mellett is szignifikáns önálló magyarázóerővel bírnak az IT-biztonsági kockázatvállalás tekintetében. Mindez együtt az IT-domén részleges autonómiáját támasztja alá.

Kutatási kérdés	Kapcsolódó hipotézis(ek)	Tézis szövege	Empirikus magyarázat
C2: Az IT-biztonsági kockázatok percepciós helyzetének meghatározása és rendszerezése a BYOD-környezetben	H2: Az IT-biztonsági domén észlelt kockázati szintje nem a legmagasabb a vizsgált kockázati domének között.	T2: Az IT-biztonsági kockázatok percepciós pozíciója Igazoltam, hogy az IT-biztonsági kockázatok észlelt szintje nem a legmagasabb a vizsgált kockázati területek között, hanem inkább a középmezőnyben vagy annak alsó szegmensében helyezkedik el, ami a digitális kockázatok relatív percepciós alulsúlyozottságára utal.	A doménenként számított átlagok alapján az IT-biztonsági kockázatok észlelt szintje nem bizonyult a legmagasabbnak a vizsgált területek között. Az egyes IT-biztonsági elemek közül a jelszó vagy PIN mások előtti használata kapta a legmagasabb átlagértékeket, míg a nyílt WiFi-hálózathoz való csatlakozás a legalacsonyabb percepciós értéket mutatta, noha objektív információbiztonsági szempontból jelentős kockázatot hordoz. A teljes domén-összehasonlítás alapján az etikai és az egészség/biztonsági domén magasabb észlelt kockázati értékeket mutatott, mint az IT-domén, amely a középmezőnyben vagy annak alsó részében helyezkedett el. Ez a digitális kockázatok relatív percepciós alulsúlyozottságára utal.
C3: A szubjektív kockázatpercepció és a biztonságtudatos felhasználói viselkedés közötti összefüggések feltárása	H4: Az IT-biztonsági kockázatok magasabb észlelése pozitív kapcsolatban áll a biztonságtudatos viselkedési gyakorlatok alkalmazásával.	T3: Kockázatpercepció és biztonságtudatos viselkedés kapcsolata Empirikusan alátámasztottam, hogy az IT-biztonsági kockázatok magasabb észlelése több esetben szignifikáns, irányhelyes kapcsolatban áll a biztonságtudatos viselkedési gyakorlatok alkalmazásával, ugyanakkor az összefüggések erőssége mérsékelt, ami az attitűd és viselkedés közötti kapcsolat részleges jellegét jelzi.	A Spearman-féle rangkorrelációs elemzések több esetben szignifikáns, irányhelyes kapcsolatot tártak fel az észlelt IT-kockázat és a biztonságtudatos viselkedés között. A nyílt WiFi-hálózathoz való csatlakozás magasabb kockázatészlelése együtt járt a kétfaktoros hitelesítés gyakoribb használatával. A frissítések rendszeres telepítése és a nyílt WiFi-használat között negatív kapcsolat mutatkozott, ami arra utal, hogy a magasabb biztonságtudatosság preventív viselkedéssel társul. Emellett a biztonságtudatos e-mail-csatolmánykezelés kisebb valószínűséggel járt együtt vállalati adatok privát e-mail címre történő továbbításával. Ugyanakkor az összefüggések többsége gyenge vagy közepes erősségű volt, ami azt jelzi, hogy a kockázatészlelés fontos, de nem kizárólagos magyarázó tényezője a viselkedésnek.

Kutatási kérdés	Kapcsolódó hipotézis(ek)	Tézis szövege	Empirikus magyarázat
C4: A technikai biztonságtudatosság és a szervezeti kockázatvállalás ellentmondásainak (biztonságtudatossági paradoxon) elemzése	H5: A technikai biztonságtudatosság egyes formái együtt járhatnak BYOD-kontextusban magasabb szervezeti kockázatvállalási hajlandósággal.	T4: A technikai kompetencia és a szervezeti kockázat viszonya Kimutattam, hogy a technikai biztonságtudatosság bizonyos formái BYOD-kontextusban együtt járhatnak szervezeti szempontból kockázatos magatartással, ami a technikai kompetencia és a szervezeti szabálykövetés közötti potenciális strukturális feszültségre utal.	A H5 vizsgálata azt mutatta, hogy a technikai biztonságtudatosság nem homogén konstrukció. A vállalati adatok saját tulajdonú eszközre történő másolása, mint BYOD-kontextusban értelmezett szervezeti kockázati magatartás gyenge pozitív kapcsolatot mutatott a rendszeres biztonsági frissítések telepítésével, ami arra utal, hogy a technikai kompetencia és az eszközhasználati magabiztosság bizonyos esetekben együtt járhat a szervezeti kontrollmechanizmusok részleges megkerülésével. Ugyanakkor a jelszókezelő használata gyenge negatív kapcsolatot mutatott a vállalati adatmásolással, vagyis a technikai biztonságtudatosság egyes formái kifejezetten védő jellegűek. Az eredmények alapján a technikai biztonságtudatosság, a szervezeti szabálykövetés és a normatív-etikai attitűd nem feltétlenül mozognak együtt.
C5: A haszon-domináns döntési mechanizmusok feltárása és a BYOD döntéstámogató stratégiai alapjainak kidolgozása	H6: Az IT-biztonsági döntésekben az észlelt haszon standardizált regressziós súlya szignifikánsan meghaladja az észlelt kockázat abszolút értékű regressziós súlyát. H7: Az észlelt haszon–kockázat súlyozási aszimmetriája nem kizárólag IT-biztonsági sajátosság, más doménekben is kimutatható.	T5: Haszon-domináns döntési architektúra az IT-biztonsági döntésekben Igazoltam, hogy az IT-biztonsági döntésekben az észlelt haszon hatása szignifikánsan meghaladja az észlelt kockázat hatását, és ez a súlyozási aszimmetria nem kizárólag az IT-biztonsági domén sajátossága, hanem más kockázati területeken is strukturálisan megjelenik.	A H6 eredményei szerint az IT-biztonsági doménben a cselekvési valószínűség regressziós modelljében az észlelt haszon standardizált regressziós együtthatója lényegesen nagyobb volt, mint az észlelt kockázaté ($\beta = 0{,}679$ vs. $\beta = -0{,}125$; $R^2 = 0{,}541$), ami egyértelműen haszon-domináns döntési struktúrát jelez. A H7 ezt a mintázatot doménközi összehasonlításban is megerősítette: más vizsgált kockázati területen is kimutatható volt a haszon regressziós dominanciája (például az A-doménben $\beta = 0{,}522$ vs. $\beta = -0{,}212$; $R^2 = 0{,}377$), és a dominancia mértéke nem tért el szignifikánsan az IT-domén eredményétől. Az eredmények alapján a súlyozási aszimmetria nem kizárólag IT-biztonsági sajátosság, hanem szélesebb döntési mintázatként értelmezhető.

KÖSZÖNETNYILVÁNÍTÁS

Szeretném megköszönni mindazoknak a segítségét, akik támogattak a doktori értekezésem elkészítésében.

Külön köszönettel tartozom témavezetőmnek, Prof. Dr. Michelberger Pálnak a munkám során nyújtott folyamatos, kitartó és iránymutató támogatásáért. Külön köszönöm azt a bizalmat és szakmai iránymutatást, amely a több mint 15 éves, oktatásban és kutatásban eltöltött közös munkánkat végig kísérte, és amely nélkül ez a dolgozat nem születhetett volna meg.

Köszönöm jelenlegi és korábbi vezetőimnek, főnökeimnek a támogató hozzáállásukat. Ugyancsak hálás vagyok közvetlen kollégáimnak és a társterületeken dolgozó munkatársaknak a mindennapi segítségért és az inspiráló szakmai beszélgetésekért, amelyek hozzájárultak a nyugodt kutatómunkához.

Szeretném megköszönni az Óbudai Egyetem Biztonságtudományi Doktori Iskola korábbi és jelenlegi munkatársainak a munkámat segítő szakmai és adminisztratív támogatást, biztatást, lehetőségeket. Valamint doktorandusz társaimnak a hasznos tanácsokat és az együttgondolkodást!

Végül, de nem utolsósorban köszönöm feleségemnek, Daragó Anitának a rengeteg türelmet, a kitartó biztatást. Nélküle ez a munka nem jöhetett volna létre.