ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS

BAK DORINA GERDA

A felhőhasználat információbiztonsági aspektusai a kkv-knál

Témavezető: Dr. habil Reicher Regina Zsuzsánna

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2025.09.08

Nyilvános védés teljes bizottsága:

Elnök:
Prof. Dr. Michelberger Pál
Titkár:
Dr. Szilágyi Győző Attila
Tagok:
Dr. Majláth Melinda
Prof. Dr. Tick Andrea
Dr. habil. Deák Zsuzsanna
Bírálók:
Dr. habil Kiss Gábor
Dr. Bács Zoltán György

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 **Bak Dorina Gerda** kijelentem, hogy **A felhőhasználat információbiztonsági aspektusai a kkv-knál** 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, 2025.09.08.

.....

Bak Dorina Gerda

Tartalomjegyzék

Bevezetés

1. 1. A tudományos probléma megfogalmazás

A hazai kis- és középvállalkozások (kkv) közel felénél hiányos vagy nem megfelelő a digitális jelenlét, sok kkv nem rendelkezik saját honlappal vagy webáruházzal, illetve, ha van is, azt nem frissítik rendszeresen, derül ki az Eurostat digitális intenzitás felméréséből c. További problémát jelent, hogy a közösségi média felületeken sincsenek jelen. Az alacsony szintű digitalizáltságát mutatja, hogy nehezen, vagy egyáltalán nem megoldható a kkv-nál a megfelelő digitális infrastruktúra kialakítása a dolgozók otthonról történő munkavégzéséhez, mert nem rendelkeznek a szükséges informatikai háttérrel. Szerb és munkatársai [4] a Global Entrepreneurship Index (GEI) pilléreit vizsgálva arra jutottak, hogy magyarországi kis- és középvállalkozások (kkv) számára a termékinnováció és a versenyelőny hiánya jelenti a legnagyobb gondot.

A digitális infrastruktúra kialakításához stratégiaváltásra van szükség [5, 6]. A kkv-k korlátozott erőforrásokkal rendelkeznek, különösen az emberi és pénzügyi tőke tekintetében, így egy hosszabb távú stratégiák kidolgozására nem marad kapacitás [7]. A kkv-k számára kihívást jelent a meglévő rendszerek integrálása, a szállítói kockázatok kezelése és az ügyfelek bizalmának fenntartása, miközben igyekeznek az információbiztonság és a kiberbiztonság fenntartására [8]. A kkv-kat érintő kiberbiztonsági trendek közé tartozik az intelligens szoftvercsomagok és a felhőszolgáltatások egyre szélesebb körű alkalmazása, a kapcsolódó költségek és a szakképzett személyzet szükségessége ellenére [9, 10]. A kkv-k azonban gyakran alábecsülik a kiberbiztonsági fenyegetéseket, ami fokozott sebezhetőséghez és kockázatokhoz vezet [9]. A kihívások ellenére egyes tanulmányok szerint az információbiztonsági kérdések pozitívan kapcsolódnak a vállalatokon belüli digitalizációs folyamathoz [11]. Ez az ellentmondás rávilágít a biztonsági aggályok és a kkv-k digitális bevezetése közötti kapcsolat összetett jellegére. Annak ellenére, hogy felhőhasználat előnyös a kkv-k számára, többek között a működési hatékonyság és az innováció javulását segítheti [12], de a biztonsági kihívások jelentősen befolyásolhatják a bevezetését és használatát. E problémák kezelése érdekében a kkv-knak olyan stratégiákat kell elfogadniuk, mint a robusztus hozzáférés-ellenőrzés, a fenyegetések folyamatos nyomon követése, az alkalmazottak képzése, az irányítási keretrendszereknek való megfelelés és az adatok titkosítása [8]. A felhőszolgáltatásoknak a kkv-k egyedi

igényeihez való igazítása és a biztonságos integrációra vonatkozó átfogó ütemterv kidolgozása kulcsfontosságú a digitális infrastruktúra kialakításához [12].

A felhő meghatározásához az Egyesült Államok National Institute of Standards and Technology's [13] definícióját veszem alapul. Azaz a felhőt egy olyan modellnek tekintem, aminek a segítségével bárhonnan, bármikor és kényelmesen hozzáférhetünk a különböző és testre szabható digitális erőforrásokhoz, mindezt könnyedén és akár a szolgáltató közbenjárása nélkül [13].

1. 2. Célkitűzés(ek)

A szakirodalomelemzéseim során azt tapasztaltam, hogy a hazai kis- és középvállalkozások által használt felhő területén több kutatási hiányosságot is fel lehet fedezni a szakirodalom területén. Ilyen hiányosságnak tekinthető a felhő alkalmazásának akadályai, a szolgáltatáshoz kapcsolódó biztonsági és adatvédelmi kérdések, a szolgáltatás által milyen gazdasági előnyök realizálhatók a vállalat számára, milyen technikai/technológiai kihívásokkal kell a vállalatnak szembenéznie a szolgáltatás implementálása során, de megemlíthető még az adatvédelemre vonatkozó előírások és szabályok köre is [14].

Kutatásom céljaként fogalmazható meg azoknak a tényezőknek a feltérképezése, amelyekkel a magyarországi kkv-kat alacsony információbiztonsági tudás és információbiztonsági tudatosság mellett, ösztönözni lehet a nagyobb mértékű felhőszolgáltatás tudatos és biztonságos használatára, továbbá a kkv-k versenyképességének növelése a felhő igénybevétele révén, miközben az információbiztonság is nő. Ehhez fel kell tárni és azonosítani kell azokat a bizonytalanságot, visszatartó tényezőket, melyek elhárítására törekedni kell.

Ebből adódóan a következő kutatási célok (C) indukálták a munkásságom:

C1: A kutatás célja feltárni, hogy a kis- és középvállalkozások (kkv-k) milyen gazdasági, technológiai, szervezeti, kulturális és bizalmi tényezőket vesznek figyelembe a felhőszolgáltatások igénybevétele során, és ezek hogyan hatnak a döntéshozatali folyamatokra.

C2: A cél annak vizsgálata, hogy milyen értelmezési keretek és prioritások mentén jelenik meg az információbiztonság a kkv-k és a felhőszolgáltatók körében, különös tekintettel a kihívásokra, érintettekre és szervezeti megközelítésekre.

C2a: A kutatás célja annak feltérképezése, hogy a felhőszolgáltatók és a kkv-k miként értelmezik a felhőtechnológiát, milyen akadályokat és előnyöket látnak benne, milyen kihívásokkal szembesülnek, és milyen belső vagy külső motivációk befolyásolják a bevezetését és használatát.

C2b: A cél az, hogy azonosítsam és feltérképezzem azokat a strukturális és tematikus kapcsolatokat, amelyek az információbiztonság különböző aspektusai (pl. szervezeti működés, tudás, attitűd, szabályozás) között fennállnak a kkv-kon belül, kvalitatív kódhálózat alapján.

C3: A kutatás célja feltárni, hogy milyen viszonyrendszerek és kapcsolati hálók rajzolódnak ki a felhőtechnológia bevezetését és használatát befolyásoló különböző tényezők között, a kvalitatív adatelemzés során létrejött kódok hálózati összefüggései alapján.

C4: A cél az interjúalanyok felhőszolgáltatásokkal kapcsolatos érzelmi viszonyulásainak feltérképezése, különös figyelemmel az ambivalens attitűdökre, félelmek és motivációk együttes jelenlétére, valamint ezek kapcsolatára a döntési és bevezetési folyamatokkal.

1. 3. A téma kutatásának kérdései és feltevései

A kutatás kvalitatív megközelítésen alapult, amely lehetővé tette a vizsgált jelenség mélyrehatóbb és kontextusfüggőbb elemzését. A kvalitatív kutatás választása indokolt volt, mivel a cél nem statisztikai összefüggések számszerűsítése, hanem a résztvevők tapasztalatainak, nézőpontjainak és percepcióinak feltárása volt [15, 16]. Ennek megfelelően a kutatás nem hipotézisek igazolására vagy cáfolására épült, hanem exploratív módon megfogalmazott feltevések mentén zajlott, amelyek rugalmasabb keretet biztosítottak az adatok értelmezéséhez [17]. Ez a megközelítés különösen alkalmas olyan témák esetében, ahol a jelenségek komplexitása és szubjektív jellege miatt a strukturált kvantitatív módszerek korlátozott érvényességgel alkalmazhatók [18]. Ennek megfelelően az alábbi kutatási kérdéseket és feltételezéseket fogalmaztam meg:

Kutatási kérdés 1: Milyen tényezők befolyásolják a felhőszolgáltatás használatát a kkv-k esetében?

Kutatási kérdés 2a: Hogyan látják a felhőszolgáltatók és a kkv-k az információbiztonságot?

Kutatási kérdés 2b: Hogyan látják a felhőszolgáltatók és a kkv-k a felhőt?

Kutatási kérdés 3a: Milyen összefüggések fedezhetők fel a kkv-knál az információbiztonságot befolyásoló tényezők között?

Kutatási kérdés 3b: Milyen összefüggések fedezhetők fel a kkv-knál a felhőt befolyásoló tényezők között?

Kutatási kérdés 4: Milyen érzelmi mintázatok jelennek meg a felhőszolgáltatásokkal kapcsolatos interjúkban?

Feltételezés 1: Nem csak gazdasági tényezők befolyásolják a felhőszolgáltatás használatát.

Feltételezés 2: Az interjúk alapján a kis- és középvállalkozások, valamint a szolgáltatók vonatkozásában tartalmi hasonlóságok és eltérések azonosíthatók az információbiztonság és a felhőszolgáltatások megjelenéséhez kapcsolódó kódok értelmezési dimenzióiban.

Feltételezés 2a: Az interjúk alapján a kis- és középvállalkozások, valamint a szolgáltatók vonatkozásában tartalmi hasonlóságok és eltérések azonosíthatók az információbiztonság megjelenéséhez kapcsolódó kódok értelmezési dimenzióiban (kihívás, stakeholderek és szervezet).

Feltételezés 2b: Az interjúk alapján a kis- és középvállalkozások, valamint a szolgáltatók vonatkozásában tartalmi hasonlóságok és eltérések azonosíthatók a felhőszolgáltatások megjelenéséhez kapcsolódó kódok értelmezési dimenzióiban (akadály, előny, kihívás és motiváció).

Feltételezés 3: A kkv-knál meghatározhatók a kódok hálózatával az információbiztonságot és a felhő megjelenését, használatát befolyásoló tényezők.

Feltételezés 3a: A kkv-knál meghatározhatók a kódok hálózatával az információbiztonságot befolyásoló tényezők.

Feltételezés 3b: A kkv-knál meghatározhatók a kódok hálózatával a felhő megjelenését, használatát befolyásoló tényezők.

Feltételezés 4: Az interjúalanyok gyakran kettős érzelmi viszonyulással élnek (egyszerre vonzó és félelmetes a technológia).

N	Kutatási kérdés	Előfeltevés	Módszertan
1	Milyen tényezők befolyásolják a felhőszolgáltatás használatát a kkv-k esetében?	Nem csak gazdasági tényezők befolyásolják a felhőszolgáltatás használatát.	kódolás
2	Hogyan látják a felhőszolgáltatók és a kkv-k …	Az interjúk alapján a kis- és középvállalkozások, valamint a szolgáltatók vonatkozásában tartalmi hasonlóságok és eltérések azonosíthatók az információbiztonság és a felhőszolgáltatások megjelenéséhez kapcsolódó kódok értelmezési dimenzióiban.	kódgyakoriság
2a	… az információbiztonságot?	Az interjúk alapján a kis- és középvállalkozások, valamint a szolgáltatók vonatkozásában tartalmi hasonlóságok és eltérések azonosíthatók az információbiztonság megjelenéséhez kapcsolódó kódok értelmezési dimenzióiban.	
2b	… a felhőt?	Az interjúk alapján a kis- és középvállalkozások, valamint a szolgáltatók vonatkozásában tartalmi hasonlóságok és eltérések azonosíthatók a felhőszolgáltatások megjelenéséhez kapcsolódó kódok értelmezési dimenzióiban.	
3	Milyen összefüggések fedezhetők fel a kkv-knál …	A kkv-knál meghatározhatók a kódok hálózatával az információbiztonságot és a felhő megjelenését, használatát befolyásoló tényezők**.**	kontextus elemzés - kódhálózat
3a	… az információbiztonságot befolyásoló tényezők között?	A kkv-knál meghatározhatók a kódok hálózatával az információbiztonságot befolyásoló tényezők.	
3b	… a felhőt befolyásoló tényezők között?	A kkv-knál meghatározhatók a kódok hálózatával a felhő megjelenését, használatát befolyásoló tényezők.	
4	Milyen érzelmi mintázatok jelennek meg a felhőszolgáltatásokkal kapcsolatos interjúkban?	Az interjúalanyok gyakran kettős érzelmi viszonyulással élnek (egyszerre vonzó és félelmetes a technológia).	sentiment

1. ábra A kutatási kérdések és feltételezések összefoglalása (Saját szerkesztés)

Feltételezéseimhez kapcsolódóan kiemelendő, hogy mivel a magyar gazdaságpolitikában döntő szerepe van a kkv-k versenyképességének, ezért a felhő megfelelő implementációja és hatékony használta kulcsfontosságú az ország számára. Ugyanakkor a téma növekvő népszerűsége ellenére sem találtam a felhőszolgáltatásra vonatkozó akár a bevezetésre, akár a használathoz kapcsolódó jó gyakorlatokról, elemzésekről szóló friss vizsgalati eredményt. Ezen kívül a humán tényező a felhőszolgáltatás implementációjában játszott szerepének feltárása lehetőséget biztosít többek között a versenyképesség növelésében, támogatásában és a munkafolyamatok (át)tervezéséhez.

2. Kutatási módszerek

2. 1. Kvalitatív kutatás indokoltsága

A kvalitatív módszerek, különösen a félig strukturált interjúk, különösen hatékonyak a kkv-k véleményének, előnyeinek, hátrányainak és észleléseinek kutatásában a felhőszolgáltatásokkal kapcsolatban. Ezek a módszerek lehetővé teszik a kutatók számára, hogy mélyen belemerüljenek a résztvevők tapasztalataiba és gondolatiba, és olyan betekintést nyújtsanak, amely pusztán kvantitatív módszerekkel nem lenne elérhető.

A félig strukturált interjúk előnye, hogy az előre elkészített kérdéseket ötvözik azzal a rugalmassággal, hogy a résztvevők válaszait alapul véve mélyebben is feltárhatók a témák. Ez az alkalmazkodóképesség elengedhetetlen a kkv-k felhőszolgáltatásokkal kapcsolatos összetett és gyakran árnyalt nézőpontjainak megértéséhez [19]. Lehetővé teszik olyan témák feltárását, mint a relatív előnyök, a bizonytalanság, a kompatibilitás és más, a felhőszolgáltatások bevezetését befolyásoló tényezők [20]. A félig strukturált interjúk rugalmasságot biztosítanak, lehetővé téve az interjúvezető számára, hogy további információkat kérjen, ha egy adott pont érdekesnek tűnik, vagy tisztázást igényel. Ez a rugalmasság kulcsfontosságú a kkv-k eltérő nézőpontjainak és egyedi körülményeinek megértéséhez [21]. Ezenkívül a félig strukturált interjúk segítségével azonosíthatók azok a konkrét kihívások és aggályok, amelyekkel a kkv-k a felhőszolgáltatásokkal kapcsolatban szembesülnek, például a biztonsági és adatvédelmi kérdések, az interoperabilitási problémák és a befektetés egyértelmű megtérülésének bizonyításának nehézsége [22]. Ezeknek a kérdéseknek a feltárásával a kutatók célzott ajánlásokat tudnak tenni a kkv-k számára szabott felhőszolgáltatások bevezetési stratégiáinak javítására, figyelembe véve azok egyedi igényeit és jellemzőit [23].

Ezenkívül ezek az interjúk lehetővé teszik, hogy a kutató megértse a kkv-k felhőszolgáltatásokkal kapcsolatos döntéshozatali folyamatainak bonyolultságát. Ez a megértés tájékoztathatja a szolgáltatókat arról, hogyan tudják jobban testre szabni kínálatukat és támogatásukat a kkv-k speciális igényeinek kielégítése érdekében, ezáltal javítva a felhőtechnológiák általános bevezetését és kihasználtságát [24](Faruque et al., 2024). Az interjúk révén közvetlen kapcsolatba kerülhetünk a kkv-k tulajdonosaival és vezetőivel, ami lehetővé teszi a kutatók számára a felhőszolgáltatások használatával kapcsolatos döntések technológiai, szervezeti és környezeti tényezőinek mélyebb

megértését [25]. Végül a félig strukturált interjúk használata átfogó képet nyújt, amely támogatja a hatékony keretrendszerek és stratégiák kidolgozását, amelyeket a kkv-k alkalmazhatnak a felhőszolgáltatások sikeres integrálása érdekében működésükbe.

A fókuszcsoportos interjúkkal szemben azért döntöttem az egyéni interjúk mellett az IT és vezető beosztásban dolgozókkal, valamint a felhőszolgáltatást nyújtó vállalatok képviselőivel, mert egyrészt a fókuszcsoportos interjúkhoz képest strukturált válaszok alkotják az interjúk végtermékét, amiknek a kódolása és elemzése könnyebb, másrészt a csoportnormák sem torzítják a válaszokat [26, 27].

2. 2. Grounded Theory módszertan

A Grounded Theory (megalapozott elmélet, GT) ideális a kvalitatív kutatáshoz, mivel szisztematikusan közelíti meg az adatokból történő elméletépítést, és szigorú keretet biztosít a kvalitatív információk elemzéséhez [28]. A GT módszertana egy kvalitatív kutatási megközelítés, amely az adatokból indul ki az elméletalkotáshoz, nem pedig előzetesen meghatározott hipotézisekre támaszkodik. Ez a megközelítés különösen hatékony az olyan kutatási helyzetekben, ahol a téma kevéssé feltárt, vagy az előzetes tudás nem nyújthat kielégítő keretet a vizsgált jelenség megértéséhez [29]. A GT-n belül a konstruktivista irányzat – amely Kathy Charmaz [30] nevéhez fűződik, és az eredeti Glaser és Strauss-féle [31] GT-t továbbfejlesztése– kiemeli a kutató és a résztvevők közötti dinamikus kapcsolatot, valamint a jelentések közös konstrukcióját. A módszer lényege, hogy a módszer és a kutatás az interjúalanyokkal való folyamatos interakció során fejlődik és változik [32]. Ez a megközelítés különösen hasznos volt számomra, mivel arra ösztönzött, hogy a kutatás során kritikai kérdéseket tegyek fel, és megvizsgáljam az adatokat és elemzéseiket [33]. A gyakorlati megjelenése az iteratív megközelítésnek a folyamatban a következő: Először interjúkat készítettem a kkv-ban dolgozó emberekkel a munkájuk kihívásairól. Az első interjúk során megemlített (további) tényezők alapján a következő interjúkban jobban rákérdeztem az említett tényezőkre, kapcsolódó mintákra, és ennek megfelelően alakítottam az interjúkat.

Kutató munkám során összegyűjtöttem és szintetizáltam a témában keletkezett nemzetközi és hazai szakirodalmat. A GT kvalitatív kutatási módszertanra építve félig strukturált szakértői interjúkat készítettem hazai kis- és közepesvállalatok IT üzemeltetőivel, munkatársaival, illetve HR vezetőivel és munkatársaival, valamint hazai

felhőszolgáltatást nyújtó vállalkozások IT szakembereivel és munkatársaival. Egy adatelemző szoftver, az ATLAS.ti alkalmazásával különböző elemzéseket folytattam.

A kvalitatív interjúk mélyebb értelmezése érdekében az elemzést szentimentelemzéssel egészítettem ki, amely lehetővé tette a válaszok mögött meghúzódó attitűdök és érzelmi tónusok feltárását is.

Ez a megközelítés lehetővé teszi az interjúk során elhangzott vélemények és érzelmek mélyebb, árnyaltabb értelmezését. A manuális módszer előnye, hogy figyelembe veszi a kontextust és a hangnemet is, amelyek automatizált rendszerekkel nehezen értelmezhetők. Míg a kódolás elsősorban az interjúk tartalmának kategorizálására és strukturálására szolgál, a szentiment elemzés az elhangzottak érzelmi töltetét, azaz hangnemét vizsgálja. A kódolás során azonosítottam és rendszereztem a kulcsfontosságú témákat és fogalmakat, míg a szentiment elemzés során az ezekhez kapcsolódó attitűdöket és érzelmeket tárom fel, tehát kiegészíti a kódolást, mélyebb betekintést nyújtva a résztvevők véleményébe. A szentimentelemzést a felhőszolgáltatók és a kkv-k vezetőinek a felhővel kapcsolatos általános hozzáállásának és megítélésének felmérésére használtam. Ennek segítségével feltárhattam a felhőhasználat szubjektív aspektusaiba és azonosíthattam a döntéshozatali folyamatokat befolyásoló akadályokat, aggodalmakat és pozitív mozgatórugókat.

Ezek alapján a jelen disszertáció az alábbi kutatási fejezetekre tagolható:

- Kutatás módszertan (2 fejezet)
- Szakirodalmi áttekintés, ahol bemutatom:
    - A vizsgálat tárgyát képező kkv-k helyzetét (3. 1 fejezet)
    - Az információbiztonság és a biztonságtudatosság alapjainak megismerése (3. 2. fejezet)
    - A kibertér és a kiberbiztonság (3. 3 fejezet)
    - A felhőalapú szolgáltatások bemutatása (3. 4. fejezet)
- Kutatás bemutatása (4. fejezet)
- Kutatás eredményei, illetve új tudományos eredmények bemutatása (5-6 fejezet)
- Következtetések és ajánlások (7-8. fejezet)

3. Szakirodalmi áttekintés

3. 1. A kis és középvállalkozások digitalízációja

A kkv-k több okból is döntő szerepet játszanak a globális, az uniós és az országos szintű gazdaságokban. Globális szinten a kkv-kat a gazdasági növekedés, az innováció, a foglalkoztatás és a társadalmi integráció kulcsfontosságú hajtóerejének ismerik el [34]. Jelentősen hozzájárulnak a munkahelyteremtéshez és a jólét megteremtéséhez, de a használatuknak akadályai is vannak [35]. Az Európai Unióban (EU) a kkv-k a gazdasági növekedés és a foglalkoztatás létfontosságú tényezői. Az EU-ban több mint 20 millió kkv működik és döntő szerepet játszanak a regionális bruttó hazai termék (GDP) növelésében [34, 36, 37]. A kutatások jelentős összefüggést mutattak ki a kkv-k szolgáltatási ágazatban való foglalkoztatása és az EU teljes foglalkoztatottsága között, kiemelve jelentőségüket a munkahelyteremtésben és a munkanélküliség csökkentésében, még a kevésbé kedvező makrogazdasági feltételek mellett is [38]. Magyarországon a vállalkozások 99 %-a kis és középvállalkozás [39], mindemellett pedig a foglalkoztatottak mintegy kétharmada ebben a szektorban dolgozik [40].

A kkv-k kulcsfontosságú szerepet játszanak a digitális megoldások elfogadásában és bevezetésében, ami létfontosságú a fenntartható és versenyképes tudásalapú gazdaságok kiépítéséhez [41]. A kkv-knak elemezniük kell a digitalizáció jelenlegi állapotát, és azonosítaniuk kell a fejlesztendő területeket [42]. Fontolóra kell venniük a digitális technológiákba, például okostelefonokba, felhőbe, mesterséges intelligenciába, robotikai rendszerekbe való beruházást is, hogy fejlesszék képességeiket és folyamataikat [43].

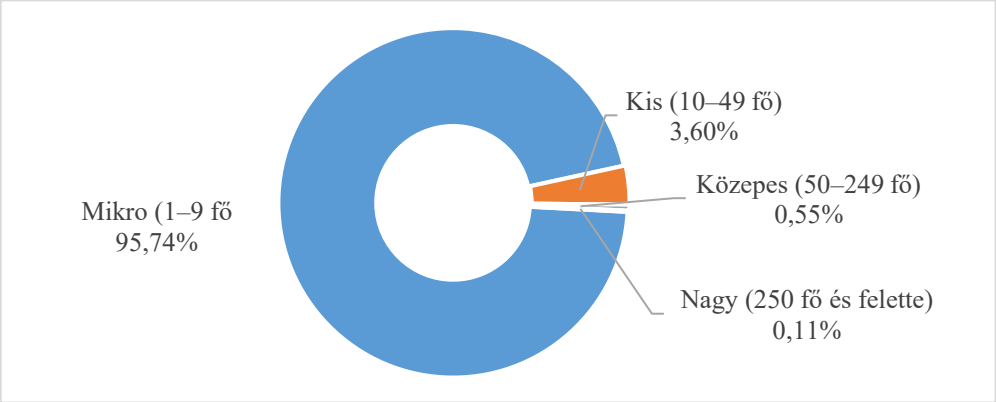
Az EU-ban és Magyarországon működő kkv-k teljesítménykritériumai jelentős eltéréseket mutatnak, elsősorban a különböző gazdasági, társadalmi és szabályozási környezet miatt. Ezek az eltérések fontosak az erőforrások elosztásának megértése szempontjából, beleértve az információbiztonságra fordított erőforrásokat is. Az EU-ban a kkv-k teljesítményét elsősorban az általuk generált hozzáadott érték alapján értékelik, amely az összes vállalkozás által generált hozzáadott értékhez való hozzájárulásukat jelenti. Ezt a teljesítményt különböző gazdasági és társadalmi tényezők befolyásolják, többek között a pénzügyi forrásokhoz való hozzáférés és a szabályozási keretekhez, például az általános adatvédelmi rendelethez (GDPR) való alkalmazkodási képesség [44, 45]. A GDPR szigorú adatvédelmi követelményeket ír elő, amelyek jelentős kiigazításokat tesznek szükségessé a kkv-k információbiztonsági gyakorlatában, ami

erőforrás-igényes lehet. A magyar kkv-k jelentősebb akadályokkal szembesülhetnek a hitelekhez való hozzáférésben, ami hatással lehet általános teljesítményükre és technológiai és információbiztonsági erőforrásokba való befektetési képességükre. Ezen túlmenően, az EU digitális évtizedre vonatkozó politikai programjában vázolt digitális és fenntartható átalakulások integrációja az EU-n belül eltérő mértékű, a digitális és fenntartható technológiák bevezetésének aránya széles skálán mozog [46]. Ezeknek a különbségeknek a jelentősége az információbiztonsági erőforrásokra gyakorolt hatásukban rejlik. Az EU-ban a GDPR-hez hasonló szabályozásoknak való megfelelés megköveteli a kkv-któl, hogy fejlett információbiztonsági intézkedésekbe fektessenek be, amelyek magukban foglalhatják a nyílt forráskódú biztonsági információ- és eseménykezelő (Security information and event management – SIEM) rendszereket is a kiberfenyegetések enyhítése érdekében [47]. Ez ellentétben áll a magyar kkv-kkal, amelyek pénzügyi korlátok miatt inkább a költséghatékonyabb megoldásokat részesíthetik előnyben. Az EU-ban és hazánkban egyaránt elengedhetetlen a hatékony információbiztonsági menedzsment a kkv-k sikeréhez, amelynek kulcsfontosságú elemei a biztonsági ellenőrzések és a menedzsment támogatás [48]. Az ezekkel a kihívásokkal való megbirkózás képessége nemcsak a szabályoknak való megfelelést és a kockázatkezelést befolyásolja, hanem a kkv-k általános versenyképességét és az európai piacba való integrációját is.

A kiberbiztonság és az információbiztonság tekintetében a kkv-k a korlátozott erőforrásaik és szakértelmük miatt egyedülálló kihívásokkal szembesülnek [47, 49]. Kibervédelmi stratégiájuk kritikus összetevőjeként a kiberbiztonsági tudatosságot kell előtérbe helyezniük [49]. Egy robusztus SIEM rendszer bevezetése alapvető fontosságú a biztonsági incidensek nyomon követése, észlelése és az azokra való reagálás szempontjából. A nyílt forráskódú SIEM-megoldások költséghatékonyságuk és hozzáférhetőségük miatt különösen előnyösek lehetnek a kkv-k számára [47].

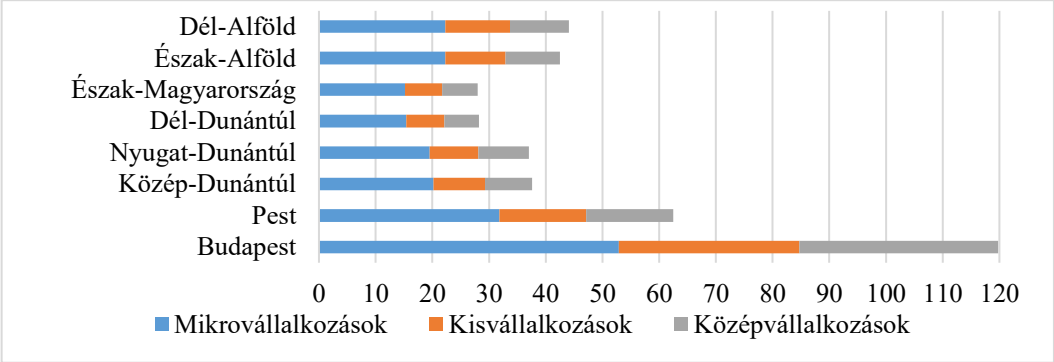
A kkv-k előnyei a nagyvállalatokkal szemben, hogy rugalmasak, dinamikusak, szorosan együttműködnek másokkal és kevésbé bürokratikusak, mint a nagyobb szervezetek [50]. Kisebb méretük nagyobb rugalmasságot, a külső fenyegetésekre és lehetőségekre való gyors reagálást, hatékony belső kommunikációt és interaktív vezetési stílust tesz lehetővé [51]. Azonban a méretükből adódóan korlátozottabbak az

Magyarországon több mint 960.000 kkv működik. A kkv szektort tovább bontva látható, hogy a mikro, vagyis a 9 vagy annál kevesebb embert foglalkoztató vállalkozások dominálnak (95,74%), illetve a foglalkoztatottak számának növekedésévvel egyre kevesebb a vállalkozás.



2. ábra A magyar vállalkozások megoszlása méret szerint 2024-ben. Forrás: [52] (saját szerkesztés)

A 3. ábra a hazai kkv szektor régiókra vetített eloszlását mutatja be. Ahogy az várható volt az előző adatok függvényében, mind a hét régióban, illetve Budapesten is a mikrovállalkozások vannak többségben, valamint a fővárosban és Pest megyében nagyobb mértékben koncentrálódnak a kkv-k, mint a többi régióban. Az is leolvasható, hogy az észak-magyarországi és dél-dunántúli régióban működik a legkevesebb számban kkv méretű vállalkozás.



3. ábra A magyar vállalkozások megoszlása régiók szerint 2023-ban. Forrás: [53] (saját szerkesztés)

A digitális technológiák széles körű alkalmazása negatívan befolyásolja a kkv-k környezeti innovációját, míg a konkrét digitális technológiák mélyreható alkalmazása pozitívan hat rá [54]. Az olyan belső tényezők, mint az informatikai irányítási gyakorlat, az informatikai tervezés és az informatikai vezetés jelentősen befolyásolják az informatikai sikert a kkv-kban [55].

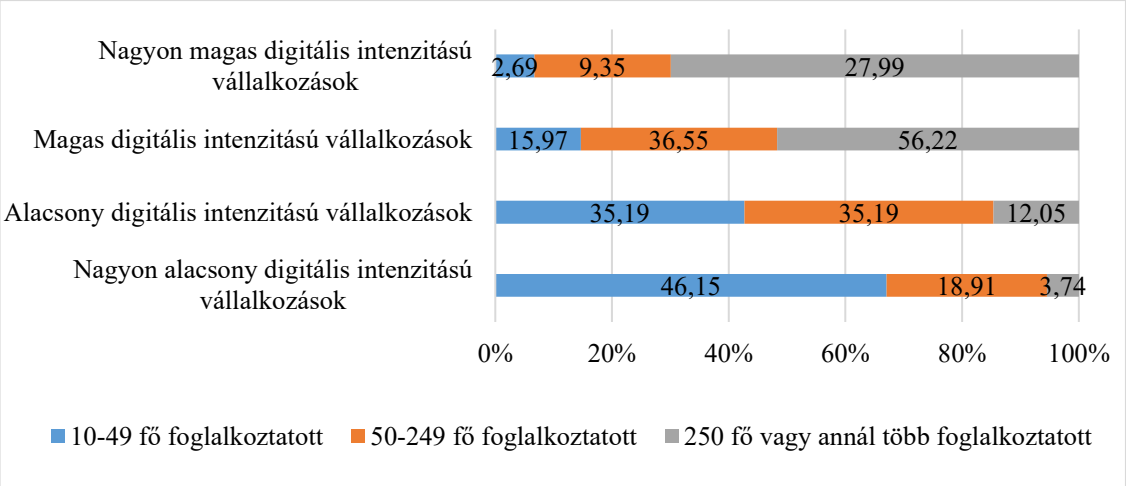
A digitális infrastruktúra kiépítése pénzügyi korlátok fékezik [56, 57]. A kockázatkezelési folyamatokat bevezetését a kockázatkezelési eszközök és technikák ismeretének hiánya is gátolja [58]. Gyakori probléma, hogy részben használják csak ki a technológia adta lehetőségeket [59], illetve az nem hangolják össze az üzleti modellt az új eszközökhöz és a megváltozott működési környezethez [60, 61]. Ebből következik egy újabb kihívás, méghozzá megtérülés hiánya, elmaradása [62]. Habár a digitális infrastruktúra kialakítása kulcsfontosságú a kkv-k számára versenyképességük növelése és a nemzetközi piacokhoz való hozzáférés szempontjából, sokuknak nehézséget okoz a gyorsan változó technológiák sebességével való megbirkózás [56, 63]. Ezt súlyosbítja a kkv-tulajdonosok és alkalmazottak technikai készségeinek és ismereteinek hiánya [56].

A kkv-k technológiai és biztonsági kihívással, kockázattal is szembesülnek, amelyek jelentősen befolyásolják üzleti tevékenységüket. A kiberbiztonsági fenyegetések komoly kihívást jelentenek a kkv-k számára. Ezek közé tartoznak a kibertámadások, vírusok, jelszótámadások, pszichológiai manipuláció (social enginering) és adathalász támadások [64, 65]. Az internetre csatlakoztatott eszközök és a felhőszolgáltatások növekvő használata különböző biztonsági kockázatoknak teszi ki a kkv-kat [9]. Ezek a fenyegetések adatszerzésekhez, pénzügyi veszteségekhez és hírnévkárosodáshoz vezethetnek, és potenciálisan a kkv-k létét is veszélyeztethetik [66, 67].

Az emberi tényezők is döntő szerepet játszanak a kkv-k kiberbiztonsági kockázataiban. Tanulmányok kimutatták, hogy a sikeres kibertámadások 95%-át emberi hiba okozza, és ezek többsége belső fenyegetés [65, 66]. Ez rávilágít a munkavállalók kiberbiztonsági gyakorlatokkal kapcsolatos tudatosságának és képzésének fontosságára. A kkv-kra szabott megfelelő kockázatkezelési keretrendszerek hiánya szintén jelentős kihívást jelent. Bár léteznek olyan bevett keretrendszerek, mint a NIST, ezek gyakran túl absztraktak vagy összetettek ahhoz, hogy a kkv-k hatékonyan alkalmazhassák őket [68]. A kockázatkezelési képességek e hiányossága miatt a kkv-k kiszolgáltatottá válnak a különböző működési kockázatoknak és bizonytalanságoknak, ami potenciálisan csökkenti a termelékenységet, növeli a költségeket és csökkenti a nyereséget [69].

Az EU Digital Intensity Indexe (DII) alapján hazánkban nagyon alacsony a vállalatok digitalizáltsága, azaz a vállalatok több mint fele többnyire csak egy egyszerű honlappal és számítógépekkel rendelkezik [70], további és komplexebb technológiai megoldásokkal azonban nem. Ezt mutatja a 4. ábra is. Az indexből az is kiderül, hogy az 50-249 főt

foglalkoztató kkv-k 81,09%-a rendelkezik legalább alapszintű digitális intenzitással, a 250 főt vagy több munkavállalót alkalmazó vállalkozások esetében ez az arány 96,26 %, míg a 9 vagy kevesebb fővel rendelkező vállalkozásoknál ez a szám 53,85 %. A magyarországi vállalkozások digitális intenzitását a 4 szemlélteti. A 3. ábráról is leolvasható, hogy az 50-249 főt foglalkoztató vállalkozások esetében az alacsony és a magas digitális intenzitás aránya közel 55 – 45 % a magas javára, míg a kisebb vállalkozásoknál ez az arány 80 – 20 % az alacsony javára, a nagy vállalatok esetében pedig 15 – 85 %-ról beszélünk a magas javára. Ezek az értékek az EU átlagnál a következők: kis vállalkozások esetében 70-30 %, középvállalkozásoknál 40 – 60 %, nagyvállalatoknál pedig 15 – 85 % az alacsony és magas intenzitás tekintetében. A számokat nézve megállapítható, hogy az EU átlaghoz képest is rosszabb helyzetben vannak a magyar vállalkozások.



4. ábra A magyarországi vállalkozások digitális intenzitása. Forrás:[71]. (saját szerkesztés)

A digitális technológiák adaptálásának folyamatát a vállalkozás mérete, a foglalkoztatottak száma, vagy akár a vállalkozás kora is befolyásolhatja. Love és munkatársai [72] arról számoltak be, hogy a különböző szervezeti típusok jelentősen különböznek a beruházások tekintetében, de ezt nem befolyásolja az éves árbevétel vagy az alkalmazottak száma. Acar és munkatársai [73] szerint azonban a kkv-k alkalmazottainak és forgalmának növekedésével intenzívebben használják az ezeket az eszközöket. A bevezetés valószínűségét növelő egyéb befolyásoló tényezők közé tartozik az is, hogy a kis- és középvállalkozások felismerték ezek kritikus szerepét az innovációban [74]. Egyéb befolyásoló tényezők közé tartozik az emberi erőforrás digitális készsége, a vállalat döntéshozatali folyamata, és a szervezetek egymásközti kutatás-fejlesztési együttműködés [75]. Az OECD felmérése is azt mutatja, hogy az

utóbbi évek fejlődése ellenére a kkv-k továbbra is lemaradásban vannak a digitális technológiák alkalmazásában. Ezt mutatja az is, hogy Magyarországon, Törökországban és Lengyelországban is a kkv-kat alapul véve a számítógéppel rendelkező alkalmazottak aránya átlagosan 40%, ezzel szemben a skandináv országokban ez az arány 80%-ot meghaladhatja [76].

A kkv szektor hazánkban is jelentős a gazdaságot tekintve, legyen szó foglalkoztatásról, hozzáadott értékről vagy a vállalkozások számát nézve. Azonban mégis ez az a szektor, amelyik a leginkább elhanyagolt, hátrányban van. A kkv szektor hátrányát mutatja a vállalatok digitalizáltságának alacsony szintje is. A digitalizáció kkv-kat is érintő előnye ellenére a Digitális gazdaság és társadalom index (DESI) 2020 adatai szerint a kkv-k szinte valamennyi digitális technológia alkalmazásában elmaradnak a nagyobb vállalkozásoktól, annak ellenére, hogy ugyanolyan arányban csatlakoznak az internethez. A legnagyobb lemaradás a belső szervezeti folyamatok digitalizálása terén mutatkozik, ahol a legnagyobb hatékonyságnövekedés érhető el [77]. Ehhez szorosan kapcsolódik a munkavállalók digitális képességeinek, tudásának növelése és fejlesztése is [78].

A sikeres működés érdekében a kkv-knak átfogó megközelítést kell alkalmazniuk a a kiberbiztonság terén. Ez magában foglalja az ISO 27001:2022 információbiztonsági irányítási szabvány bevezetését, amely egyértelmű előnyöket mutatott a kkv-k információbiztonsági robusztusságának és az alkalmazottak biztonságtudatosságának növelésében [79].

3. 2. Információbiztonság - biztonságtudatosság

A megváltozott munkakörnyezet azonban rákényszeríti a munkavállalókat arra, hogy készségeiket a folyamatosan változó piaci változásokhoz igazítsák [80-82]. A szükséges készségeknek nemcsak azt kell lehetővé tenniük, hogy a munkavállalók hatékonyan használják a digitális technológiákat, hanem azt is, hogy a munkát egy technológiában gazdag környezetben végezzék [81, 83]. A megváltozott munkakörülményekhez való alkalmazkodás nehézséget jelenthet az idősebb munkavállalók számára, mivel az életkor előrehaladtával nő a technológiával szemben támasztott aggodalmuk, szorongásuk, és általában kevésbé bíznak saját számítógépes tudásukban, mint fiatalabb munkatársaik [84, 85]. Ezt nehezíti még a generációk közötti különbségek megjelenése is. A legfiatalabb generáció, viszont nehezen találják meg a közös hangot az idősebb munkatársakkal, és akadályokat képez az idősebb munkatársakkal való csapatmunkában

[86, 87]. Az ellentéthez hozzájárul az is, hogy a fiatalabb munkavállalók együtt nőttek fel az ezekkel a technológiákkal, és őket nevezik digitális bennszülötteknek, míg az úgynevezett digitális bevándorlóknak, akik felnőttkorukban találkoztak az internettel és a számítógéppel, nekik alkalmazkodniuk kellett ezek munkahelyi használatához [88].

Az információbiztonsággal kapcsolatos pozitív hírek, események és tevékenységek pozitív és szignifikáns hatással vannak a digitális infrastruktúrába beruházó vállalatok részvényárfolyamára is [89]. Az előnyök mellett kockázatok és hátrányok is vannak. Az egyik ilyen az automatizáció és robotizáció térnyerése a munkaerőpiacon [90]. Az automatizált munkafolyamatok és a robotok általi feladatvégzés ellenérzést vált ki a munkavállalókban, mivel úgy érzik, hogy a gépek elveszik a munkájukat, és emiatt kiszorulnak a munkaerőpiacról. Míg a vállalatok számára előnyösebb és kiszámíthatóbb az emberi munkaerő gépekkel való helyettesítése, addig a munkavállalók folyamatos tanulási kényszerrel és ellenérzéssel szembesülnek [91, 92].

A digitális kor vívmányai lehetővé teszik az információk gyors megszerzését és cseréjét a felhasználók számára, de az új eszközök birtoklása nem garantálja azok helyes használatát [93], Megfelelő tudás és óvatosság hiányában védtelenek a kibertámadásokkal szemben [94]. Az új technológiák mindennapokba és munka világába való beépülése új készségeket, képességeket és ismereteket igényel, hogy az új eszközöket és szolgáltatásokat hatékonyan alkalmazhassuk. Ehhez úgynevezett digitális intelligenciára [95] van szükség [96], amelynek fontosságát több tényező támasztja alá. Egyre több nemzetközi szervezet és ország fejleszt erre irányuló programokat [82, 97, 98], és az online oktatások, valamint az otthoni munkavégzés egyre népszerűbbé válnak [99, 100]. A biztonságtudatosság szükségességét tovább erősítik a munkahelyi elvárások [101, 102], amelyeket a munkavállalókkal szemben támasztanak [103, 104], de az iskolapadban megszerzett tudás gyakran nem egyezik meg a munkahelyen elvárt készségekkel és képességekkel [105, 106]. A Covid-19 miatt bekövetkezett kötelező átállás az offline térből az online térbe csak még intenzívebbé tette ezt a folyamatot [107]. Ezek az új képességek és ismeretek gyakran hamarabb jelennek meg az egyének oldalán, mint a vállalatoknál, és gyakran használat közben sajátítódnak el, felületesek, és hiányzik mögülük az összefüggések ismerete és megértése. A digitális infrastruktúra [108] korunk alapja és az innováció motorja [109], de az egész életen át tartó tanulás [110] talán még soha nem volt ilyen fontos a tudásalapú társadalom fejlődése és az innovációk gyors átvétele szempontjából. Annak ellenére, hogy egyre inkább elismerik a digitalizációhoz

kapcsolódó kompetenciák elsajátításának fontosságát [111-113], és a digitális kompetenciák szakirodalma közel 20 éves múltra tekint vissza [114], a mai napig nem született egységes definíció rá [115, 116].

Az információbiztonság és az emberi viselkedés összefüggnek egymással, és jelentős hatással vannak egymásra [117]. Az emberi viselkedés egyaránt növelheti és alááshatja az információbiztonságot [83, 118]. Ezért fontos, hogy a szervezetek figyelembe vegyék az emberi viselkedést az információbiztonsági irányelvek és eljárások kidolgozásakor és végrehajtásakor. Az információbiztonsággal kapcsolatos kutatások nagy része a technológiai megoldásokra összpontosít, míg az emberi tényezők és különösen az emberi hibák vizsgálata viszonylag kevés figyelmet kapott [119]. Az emberi hibát nem szándékos, véletlen cselekedetként definiálják, amely káros hatással van az információbiztonságra [120]. A kutatások szerint az információbiztonsági incidensek jelentős részéért – 42% és 90% közötti arányban – emberi hibák felelősek [121-124]. Az emberi tényezők figyelmen kívül hagyása a biztonsági rendszerek sérülékenységéhez vezethet [125, 126], különösen, mivel a belső szereplők által okozott incidensek a legnehezebben megelőzhetők [127]. A komplex szociotechnikai rendszerekben az emberi viselkedés megbízhatóságának integrálása komoly kihívást jelent. A stressz, a képzés hiánya és a rosszul kialakított folyamatok gyakran vezetnek hibákhoz [128]. A kockázatkezelési megközelítések hasznosak az elfogadható kockázati szintek fenntartásában, azonban nem alkalmasak a komplex emberi tényezők kezelésére [129]. Az emberi viselkedés megértését célzó kutatások alacsony száma miatt további empirikus vizsgálatok szükségesek [130, 131]. Az emberi tényező figyelembevétele és az emberi viselkedés megváltoztatására irányuló új beavatkozások kidolgozása alapvető fontosságú az információbiztonság javítása érdekében [128].

Az információbiztonság és az emberi viselkedés összefüggnek egymással, és jelentős hatással vannak egymásra [117]. Az információbiztonság az érzékeny információk, adatok és rendszerek védelme és biztonsága érdekében hozott intézkedésekre utal, amelyek célja a jogosulatlan hozzáférés, felhasználás, nyilvánosságra hozatal, módosítás vagy megsemmisítés elleni védelem. Az emberi viselkedés másrészt az egyének és csoportok által hozott olyan cselekvésekre és döntésekre utal, amelyek hatással lehetnek az információk biztonságára. Az emberi viselkedés egyaránt növelheti és alááshatja az információbiztonságot [83, 118].

A biztonságtudatosság meghatározása nehézségekbe ütközik, melyet egyrészt a megfoghatatlansága, meghatározhatatlansága ad, másrészt pedig a transzdiszciplináris természete, mely a területet övező széles körű kutatások is alátámasztanak [132]. A biztonságtudatosság egyes definíciói az egyén kognitív tudatállapotának figyelembevétele mellett - mint például az észlelés és helyzetfelismerés - reagálási jellemzőket is tartalmaznak, azaz az e tudatállapot létrehozására alkalmazott eljárásokat, folyamatokat [133-135]. Kevés olyan definíció létezik, amely a tudatosságot elkülöníti egy bizonyos típusú tevékenységtől [136]. Bár a biztonság és az adatvédelem kiemelkedő szerepet játszik az információs rendszerekkel kapcsolatos kutatásokban [137], az emberi aspektusra vonatkozó kutatások, mint például az információbiztonság vezetői megközelítése [138, 139], az információbiztonsági tudatosság [138, 140], valamint az emberi tényezők és a vezérigazgatók szerepe [141, 142] csak az utóbbi néhány évben kerültek a tudományos kutatások középpontjába. A definíciók sokszínűségét a 1. táblázat mutatja be.

Thompson és munkatársai [143] azt vizsgálták, hogy van-e különbség az otthoni és a mobil eszközök esetén alkalmazott biztonsági megoldások között. Megállapították, hogy az észlelt sebezhetőség, az énhatékonyság és a válaszadási költség mind fontos tényezők abban, hogy a felhasználó milyen biztonsági megközelítéssel használja az egyes digitális eszközöket, míg a fenyegetés észlelt súlyossága csak a mobileszközök biztonsági törekvéseiben játszott szerepet. A tapasztalat megváltoztatja, hogyan értékelik az emberek a sebezhetőségüket, ellensúlyozva a sebezhetőség alábecsülésére való hajlamot [118, 144]. szándék és a viselkedés közötti kapcsolatban a szokás mérséklő tényező lehet [145]. Az otthoni számítógépes biztonsági viselkedések stabilabbnak és rögzültebbnek tűnnek, mint a mobileszközökhöz kapcsolódó biztonsági viselkedések [146, 147]. A biztonságtudatosságra, valamint a hozzátartozó definíciókra ez szintén igaz. A 1. táblázat A biztonságtudatosság meghatározásai a különböző szakirodalmakban. (Saját szerkesztés)

1. táblázat A biztonságtudatosság meghatározásai a különböző szakirodalmakban. (Saját szerkesztés)

ezt hivatott szemléltetni. A biztonságtudatosság vizsgálatára irányuló kutatások két fő szálon mozognak. Az egyik irány, mint általános, tudást, ismeretet, következmények ismeretét, az egyén szerepét, jelentőségét érti alatta. Ezzel szemben a másik oldal a fenyegetések ismerete, valamint a fenyegetésekkel való megküzdés, fenyegetések értékelése, gyakorlatibb folyamatokat, reakciókat ért a fogalom alatt.

Szerző(k)	Biztonságtudatosság meghatározása
Albrechtsen [148]	Az, hogy az egyének milyen mértékben értik meg az információbiztonság fontosságát; a szervezet által megkövetelt biztonsági szint és az egyéni biztonsági felelősség.
Boss, Kirsch, Angermeier, Shingler and Boss [149]	Az általános tudatosság, amely a vállalati előírások, policyk meghatározásától, betartásától/betartatásától, illetve a büntetés-jutalmazás rendszerétől függ.
Bulgurcu, Cavusoglu and Benbasat [133]	A munkavállaló általános ismeretei az információbiztonságról és a szervezet információbiztonsági politikájáról, valamint az információbiztonsággal kapcsolatos lehetséges problémák és azok következményeinek ismerete, megértése.
D'Arcy, Herath and Shoss [126], D'Arcy, Hovav and Galletta [134], Crossler [150], Burns, Posey, Roberts and Benjamin Lowry [151]	A fenyegetettséggel való megküzdés, illetve a fenyegetések értékelése, ezek ismerete.
Kritzinger and Smith [152]	Az információbiztonsági tudatosság annak biztosítását jelenti, hogy egy szervezet minden alkalmazottja tisztában legyen a szerepével és felelősségével a velük dolgozó információk biztonsága terén.
Liang and Xue [153]	A tudatosság az egyének fenyegetésekről és a védelmi intézkedések elérhetőségéről alkotott elképzeléseire összpontosít, beleértve az információbiztonsági politika elérhetőségét is.
Pahnila, Siponen and Mahmood [154]	A biztonsági politikák és irányelvek ismerete. A biztonsági fenyegetések, valamint azok súlyosságának és gyorsaságának ismerete. A megküzdéssel és a fenyegetések értékelésével való hallgatólagos kapcsolat.
Rhee, Ryu and Kim [155]	Az információbiztonság tudatossága a különböző információbiztonsági fenyegetések megértésének és a fenyegetésekkel kapcsolatos sebezhetőség érzékelése.
Siponen and Vance [156]	Az információbiztonsági irányelvek és azok megsértésének tudatossága.
Woon, Tan and Low [157]	A tudatosságot egy adott témával kapcsolatos tudásként fogalmazták meg.

1. táblázat A biztonságtudatosság meghatározásai a különböző szakirodalmakban. (Saját szerkesztés)

A dolgozat szempontjából a fentiek alapján a biztonságtudatosság az egyén azon képességeinek összességének tekintem, amely révén felismeri az információbiztonság jelentőségét, megérti a fenyegetéseket, és érzékeli a rendszerek vagy saját viselkedése által jelentett sebezhetőségeket.

A személyes adatok biztonságának megsértése, különösen az érzékeny adatok esetében, az elmúlt években rendszeresen előforduló jelenséggé vált. Ezeket az incidenseket rosszindulatú kiberszereplők hajtják végre, akik különféle eszközökkel támadják a szervezetek információs rendszereit az információk kiszivárogtatása céljából [158]. A biztonsági incidensek elkövetői egyre inkább tudatában vannak annak, hogy az emberi tényezők – legyen szó tévedésről vagy viselkedésről, magatartásról – az információbiztonsági struktúra gyenge pontját jelenthetik [80]. Ez egyértelműen jelzi, hogy minden hatékony információbiztonsági rendszer ereje azok kezében van, akik azt használják, és nem csupán a technológiában rejlik. A bekövetkezett támadások jelentős

része (közel 90%) emberi hibára vezethető vissza [159]. A technológia gyakran olyan gyenge és sebezhető, mint az azt fejlesztő és/vagy működtető emberek (munkaerő), valamint a használatára tervezett és strukturált folyamatok [160]. Ezért az emberi viselkedés továbbra is kritikus jelentőségű. A kutatások azt mutatják, hogy a szervezetek által elkövetett információsértések fő típusa bizonyos mértékig az emberi erőforrások kihasználásához kapcsolódik, legyen az hiba vagy felhasználói magatartás [159, 161, 162]. A kutatások azt is kimutatták, hogy a szervezetek gyakran figyelmen kívül hagyják az emberi tényezőket, mint a biztonsági rések egyik fő okát, és inkább a technológiai ellenőrzésekre és megoldásokra összpontosítanak [163]. Az információbiztonság és az ember közötti elválaszthatatlan kapcsolatot nem lehet figyelmen kívül hagyni. Amikor az információbiztonsági rendszerek értékelésére kerül sor, a szervezetek többnyire a rendszer technológiai aspektusát értékelik, és nagyon kevés vagy semmilyen értékelést nem végeznek az emberi tényezőkről, amelyek nagymértékben befolyásolhatják a biztonsági rendszer sebezhetőségét [164]. Az adatok vagy információk védelme nagymértékben függ az információbiztonsági tervtől, amely a technológiai ellenőrzések szokásos gyakorlatán túl figyelmet fordít az emberi tényezőkre, a felhasználói viselkedés és szokások ellenőrzésére, formálására [165, 166].

Bak és Kelemen-Erdős [118] a kutatásukban rámutattak arra, hogy az általuk megkérdezettek biztonságtudatossága nem megfelelő szintű, még akkor sem, ha eltérő mértékű ismeretekkel rendelkeznek a kibertámadások módjairól és következményeiről. A felhasználók hajlamosak alábecsülni saját sebezhetőségüket, és gyakran az az illúziójuk, hogy nem lehetnek célpontok. Nemzetközi tanulmányok hangsúlyozzák, hogy a fenyegetések ismerete önmagában nem elegendő: a biztonságtudatos viselkedéshez elengedhetetlen a védelmi eszközök alkalmazásának képessége és a szabályok mögötti okok megértése [167, 168]. A kutatás során megállapították, hogy a kiberbiztonsággal kapcsolatos személyes tapasztalatok jelentős hatást gyakorolnak a biztonságtudatosságra.

A biztonságtudatossággal foglalkozó szakirodalmat áttekintve az látható, hogy az egyén biztonságtudatossága több tényező függvénye, melyek kultúránként, régiónként más képet mutathat. Ezek a befolyásoló tényezők körébe tartoznak a különböző szociodemografikus jellemzők, például a megkérdezett neme, kora, az iskolai végzettsége, vagy a jövedelme, lakhely típusa [131]. Más kutatások szerint az életkor, az egyén iparág szerint munkahelye és az iskolázottsági szintje nagyban befolyásolja azt, hogy az egyén mennyire van tisztában a munkahelye által alkalmazott

információbiztonsági előírásokkal, belső szabályokkal, illetve azokat mennyire tartja be [169]. Ezzel egybe cseng az is, miszerint azok, akik ismerik a vállalati szintű hivatalos információbiztonsági szabályokat, azok magasabb szintű információbiztonság tudatosságról tesznek bizonyságot [170]. Érdemes megemlíteni, hogy például az egyének neme sok kutatásban egymásnak ellentmondó eredményeket hoz, lehet befolyásoló és nem befolyásoló tényező is. Erre jó példa, hogy míg Hajli és Lin [171] szerint a nők nagyobb kontrolt gyakorolnak az információmegosztási hajlandóságuk felett a közösségi média oldalakon történő megosztások esetében, addig Anwar és munkatársai [172] a nemek tekintetében nem talált szignifikáns különbséget a kockázatérzékelést illetően. A személyiségjegyekhez kapcsolódóan Hadlington és Parson [173] kapcsolatot talált az egyén személyisége és a munkahelyi információbiztonsági intézkedések között, vagyis az a személy, akinek a munkahelyén magasabb szintű biztonsági intézkedések, védelem van érvényben, azok kockázatvállalóbbak, hiszen úgy vélik, ha rá is kattintanak egy kéretlen emailre, a szervezet védelmi rendszere majd megvédi. Ha az egyén kevéssé elkötelezett a munkahelye és a szervezete iránt, vagy úgy érzi, hogy csak korlátozottan tudja ellenőrizni a munkáját, akkor kisebb valószínűséggel fog részt venni a hatékony információbiztonságban **[140]**. A szakirodalomban összefoglalóan security-related stress (SRS) vagyis biztonsághoz kapcsolódó stresszhatásokként nevezett jelenség például csökkenti a vállalat információbiztonsági kultúra iránti elköteleződést és növeli a nemkívánatos viselkedést [126]. Zwilling és munkatársai [174] négy országra (Lengyelország, Izrael, Törökország és Szlovénia) kiterjedő felmérése szerint, akik magasabb kiberbiztonsági tudással rendelkeznek, azaz tudatában vannak a rájuk leselkedő online veszélyekre, azoknak magasabb a kiberbiztonsági tudatossága. A megkérdezettek kiberbiztonsági tudatosságára pozitív befolyással volt a kiberbiztonsági képzésen való részvétel és a témában kapott oktatás, képzés is, ami rávilágít ezeknek a programoknak a tudatosításban való szerepére. A felhasználók biztonságtudatossága kapcsán a közösségi média oldalakat tekintve Zolait és munkatársai [175] azt találták, hogy a felhasználók biztonsági aggályai, ismeretei és biztonságtudatossága erősen befolyásolja a felhasználói attitűdöt, valamint a felhasználó azon szándékát, hogy a közösségi média oldalak használata során biztonságosan viselkedjen. A közösségi média felületek a szervezetek számára az egyik legnagyobb kihívást jelentik az információ kiszivárogtatások szempontjából, mivel széles körben elterjedtek és OSINT (open-source intelligence - nyílt forrású hírszerzés) szempontból közkedvelt forrás [176, 177]. A közösségi média felületek mellett a munkavállalók is információbiztonsági fenyegetést

jelentenek a vállalatra [178]. A munkavállalók szándékos vagy nem szándékos adatmegosztása akár a céges, akár a privát adatokat tekintve célponttá teszi őket a social engineering támadásoknak, amely támadások általában nehezen felderíthetők, a szellemi tulajdon vagy bizalmas információk megszerzését, ipari kémkedést és a vállalati hálózatok szabotálását célozzák [179, 180]. A támadók különböző forrásokból, többek között közösségi médiaplatformokról, keresőmotorokból, fórumokról és archivált weboldalakról passzívan gyűjthetnek információkat a célpontjukról, és ezeket az adatokat felhasználhatják arra, hogy más kulcsfontosságú személyekkel való interakciók révén további információkat szerezzenek [181]. Bár a szervezetek nem tudják teljes mértékben megakadályozni, hogy az alkalmazottak információkat osszanak meg, vagy leállítsák a kapcsolódó OSINT-folyamatokat [182], oktathatják és tájékoztathatják munkatársaikat az információmegosztás negatív következményeiről. Ez a megközelítés segíthet korlátozni az érzékeny információk nyilvánosságra hozatalát [183], növelheti a felderítési erőfeszítések nehézségeit, és következésképpen csökkentheti a támadás valószínűségét. Bár az elmúlt években több kutatás is megerősítette, hogy az emberi tényezőre vezethető vissza a hibák bekövetkezésének nagy része, ennek ellenére a szervezetek továbbra is a technológiai infrastruktúra területére összpontosítják IT (és kiberbiztonsági) beruházásaikat [184, 185]. Az információbiztonság terén nyilvánvaló hiányosság tapasztalható a szervezetek körében, amelyek csak a biztonság technológiai szempontjait veszik figyelembe, és lemondanak az emberi szempontokról.

3. 3. Kiberbiztonság

A kiberbiztonság kifejezést gyakran felváltva használják az információbiztonsággal, és bár a kiberbiztonság és az információbiztonság között jelentős átfedés van, a két fogalom nem teljesen összeegyeztethető [186]. A kiberbiztonság és az internetbiztonság olyan, mint egy érem két oldala. Más szakemberek azonban úgy vélik, hogy a kiberbiztonság az internetbiztonság egy része vagy alterülete [187]. A kiberbiztonság esetében az ember a kibertámadások potenciális célpontjaként jelenik meg, vagy akár akaratlanul is egy kibertámadás részesévé válik [186]. A legtöbb vállalat nem fektet be vagy nem elegendő mértékben a kiberbiztonsági oktatásba. Ha az oktatást az alkalmazottak és rendszereik veszélyeztetésének kockázatát csökkentő módszerként határozzák meg, akkor azt többnyire tudatosságnövelő kampányok révén teszik [188].

A kiberbiztonság terén a *Global Cybersecurity Index* (GCI) kínál átfogó képet. A 2024-es jelentés szerint Magyarország a Tier 2 – Advancing (score of 85–95) klaszterbe tartozik a 88,73 ponttal a maximális 100 pontból, míg a globális átlag pontszám 65,7. A jelentés alapján a technikai intézkedések terén van leginkább szükség fejlesztésre, míg a jogi, szervezeti, kapacitásbővítési és együttműködési intézkedések terén kedvező eredmények születtek. A Tier 1 – Role-modelling (score of 95–100), vagyis a felmérésben a legjobbak közé tartozó országok között olyanokat találunk, mint Ausztrália, (96,24 pont), Japán (97,58 pont), Szerbia (96,82 pont), de idetartozik még míg az Egyesült Királyság (100 pont) és az Amerikai Egyesült Államok (99,86 pont) is [189]. Egy másik releváns mutató az *IMD World Digital Competitiveness* (WDC), amely az országok digitális technológiák iránti nyitottságát és alkalmazkodóképességét vizsgálja. A WDC három fő tényezőt értékel: tudás, technológia és jövőbeli felkészültség. A legfrissebb jelentés alapján, amely 67 országot elemzett, Magyarország a 53. helyen áll. A mutató szerint technológia és a tudás területén mutatkozik elmaradás. Szingapúr vezeti a rangsort, a második helyezett Svájc, míg az EU tagállamai közül Dánia kiemelkedő helyet foglal el (3. hely) [190]. Habár már a 2000-es évek elején, illetve a (digitális) technológia fejlődése kapcsán léteztek a kibertámadások és a hacker tevékenységek, valamint fontosnak tekintették ellenük a védekezést, egészen 2007-ig váratott magára az áttörés, ugyanis ekkor történt orosz-észt incidens [191]. Napjainkban a kibertér, a kiberbiztonság és a kiberbűnözés témakörei egyre nagyobb figyelmet kapnak mind nemzetközi szervezetek, mind nemzetállamok részéről. Ezt alátámasztják a vezető hatalmak kibertérre vonatkozó intézkedései, a kiberhadviseléssel kapcsolatos kutatások és fejlesztések számának növekedése, valamint az olyan kezdeményezések, mint az Európai Kiberbiztonsági Hónap [192]. A vállalatok szerepe sem elhanyagolható: az Accenture „Securing the Digital Economy” című felmérése szerint napjainkban a vállalatok 100%-a támaszkodik a digitális eszközökre az üzleti tevékenysége során, míg tíz évvel ezelőtt ez az arány mindössze 25% volt [193].

A társadalom növekvő mértékű függősége az új technológiáktól az elmúlt években azt eredményezte, hogy exponenciális mértékben nőttek a különböző biztonsági incidensek [194] (jogosulatlan hozzáférések/ unauthorized accesses [195], a rosszindulatú szoftver/malware támadások, a zero-day támadások, az adatszivárgás/data breach-ek, a szolgáltatás megtagadása/denial of service (DoS) [118], a pszichológiai manipuláció/social engineering vagy az adathalászat/phishing [89, 196]). 2010-ben közel

50 millió rosszindulatú program volt ismert a biztonsági szakemberek számára. 2012-re ezek száma megduplázódott 100 millió körül, 2019-ben pedig már több mint 900 millió rosszindulatú programra nőtt az adatbázis, és ez a szám a németországi AV-TEST intézet statisztikái szerint valószínűleg tovább fog nőni [197].

A kiberbiztonság olyan technológiák és folyamatok összessége, amelyek célja a számítógépek, hálózatok, programok és adatok védelme a támadástól, károsodástól vagy jogosulatlan hozzáféréstől [198]. Az elmúlt fél évszázad során a digitális technológiai ipar [108] nagymértékben fejlődött, amely mindenütt jelen van és szorosan integrálódott modern társadalmunkba. Így az a kibertámadásoktól való védelem az elmúlt években nagymértékben foglalkoztatta a biztonságpolitikai döntéshozókat [199-201]. A kiberbiztonsághoz több szempont is kapcsolódik: az digitális eszközök védelmét szolgáló intézkedések; a benne lévő adatok és információk, valamint azok feldolgozása és továbbítása; a rendszerek kapcsolódó virtuális és fizikai elemei; az ezen intézkedések alkalmazásából eredő védelem mértéke; és végül a kapcsolódó szakmai terület [191].

A kiberbiztonság arra törekszik, hogy biztosítsa a szervezet és a felhasználó eszközei biztonsági tulajdonságainak elérését és fenntartását a kiberkörnyezet releváns biztonsági kockázataival szemben. Az általános biztonsági célkitűzések a következőket foglalják magukban: bizalmasság (confidentiality), sértetlenség (integrity) és rendelkezésre állás (availability) (CIA elv) [202, 203]. Ez részletebben a következő, a 2. táblázat CIA elv esetei (saját szerkesztés)

pedig gyakorlati példákon keresztül szemlélteti a CIA elvet:

- A bizalmasság olyan tulajdonság, amely megakadályozza az információkhoz való hozzáférést és azok illetéktelen személyek, szervezetek vagy rendszerek számára történő használatát.
- A sértetlenség az információ jogosulatlan módosításának vagy megsemmisítésének megakadályozására szolgáló tulajdonság.
- A rendelkezésre állás olyan tulajdonság, amely az információs eszközökhöz és rendszerekhez való bármikor bárhonnan megbízható hozzáférést biztosítja az arra jogosultak számára.

	Rendelkezésre állás	**Bizalmasság**	**Sértetlenség**
Hardver	Ellopják, elérhetetlenné válik	-	-
Szoftver	Törlődik, hozzáférés megtagadás	Másolat készül	Módosult - hibás lefutás
Adat, információ	Törlődik, hozzáférés megtagadás	Jogosulatlan hozzáférés, szivárogtatás	Módosul, kicserélődik, sérül

Kommunikációs csatorna	Sérül, törlődik, elérhetetlenné válik	Jogosulatlan hozzáférés	Módosul, késik, eltérítik, kicserélődik, sérül

2. táblázat CIA elv esetei (saját szerkesztés)

A CIA-elv, vagyis az előbb említett három tényező az információbiztonság és a személyes adatok védelme szempontjából is releváns, bár a dimenziók hangsúlyai némileg eltérnek egymástól.

A kkv-kat érintő fő információbiztonsági problémák és kockázatok közé tartozik a kiberbiztonsági jogsértések széles skálája, amelyek különböző súlyosságúak a reagálási és kezelési idő, illetve a költségek alapján [204]. Ezeket a kockázatokat öt témakörbe sorolják: *biztonsági, függőségi, munkavállalói, stratégiai és jogi kockázatok* [64]. A kkv-k különösen sebezhetőek a kiberfenyegetésekkel szemben, mivel nem rendelkeznek a kiberbiztonság prioritásként való kezeléséhez szükséges erőforrásokkal és szakértelemmel [49]. A kkv-k számára ezek a kiberbiztonsági trendek és kockázatok jelentős következményekkel járnak. A kihívások közé tartoznak a költségvetési korlátok, a vezetői támogatás hiánya és a kiberbiztonsághoz való hozzáállás [205]. Emellett a kkv-k küzdenek a hatékony kiberbiztonsági intézkedések végrehajtásával, és gyakran hiányzik az elkötelezettségük a kiberbiztonsági irányítás és kultúra iránt [206].

A kiberbiztonság és az ahhoz kapcsolódó kiberstratégiák alapos megértése érdekében elengedhetetlen néhány alapfogalom áttekintése, amelyek jelentős szerepet játszanak mind a védekezési, mind a megelőzési szakaszokban. Ezek a fogalmak képezik a kiberbiztonsági tevékenységek keretrendszerének alapját. Noha az alábbi fogalmak fontosságában általános egyetértés tapasztalható, értelmezésük terén jelentős eltérések figyelhetők meg [207, 208].

A témához kapcsolódóan kulcsfontosságú fogalom a kibertér, amelynek meghatározása többféle megközelítésben jelenik meg a szakirodalomban. A kibertér magyarországi definícióját a 1139/2013. (III. 21.) Kormányhatározat rögzíti, amely szerint [209]: *„A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti.”* Ez a megközelítés hangsúlyozza a kibertér társadalmi és gazdasági dimenzióit, valamint az elektronikus információs rendszerek növekvő szerepét.

Az Amerikai Egyesült Államok Védelmi Minisztériuma (Department of Defense) ennél eltérő, technológia-központú definíciót alkalmaz. Meghatározásuk szerint a kibertér egy

információs környezet, amely magában foglalja az informatikai infrastruktúrákat, az azokban tárolt adatokat és ezek hálózatát, ideértve a számítógépes rendszereket és az internetet [210]. Ez a megközelítés elsősorban az információs rendszerek technológiai aspektusaira összpontosít, és kiemeli a hálózatok és az adatok közötti szoros összefüggést.

A kibertámadás jelensége szintén elengedhetetlen a kiberbiztonság és a kiberstratégia fogalmának tárgyalása előtt. Noha a digitális kompetencia fejlesztése kulcsfontosságú a biztonságos digitális térben való eligazodáshoz, érdemes megvizsgálni annak az oldalát is, ahol a magas szintű digitális kompetencia már nemcsak védekezési eszközként szolgál, hanem támadások alapjául is szolgálhat [191, 211, 212]. Ennek alátámasztására szolgál az a statisztika, amely szerint a kiberbiztonsági incidensek 95%-a emberi hibára vezethető vissza, ami arra utal, hogy az érintettek nem rendelkeznek megfelelő digitális kompetenciával és biztonságtudatossággal [213].

Fekete-Karydis és Lázár [214] szerint a kiberbiztonság olyan eszközök és intézkedések rendszere, amelyek állampolgári és katonai szinten egyaránt lehetővé teszik a kibertér védelmét a hálózatokat és információs infrastruktúrákat érő fenyegetésekkel szemben. Ezzel összhangban van Magyarország 2013-ban kiadott Nemzeti Kiberbiztonsági Stratégiája, amely szintén kiemeli a kiberbiztonság jelentőségét a nemzet biztonságának és stabilitásának megőrzésében. Az EU szintjén a kiberbiztonság először a 2010-ben elfogadott Európa 2020 stratégia keretében jelent meg, azon belül is az európai digitális menetrend részeként, amely a digitális piac fejlesztését célozta meg. Bár a kiberbiztonság ekkor még csak mellékesen került említésre, az egységes digitális piac létrehozásának és fejlesztésének szükségessége már ebben az időszakban hangsúlyozta annak fontosságát [215]. Három évvel később, 2013-ban az EU elfogadta első átfogó kiberbiztonsági stratégiáját, amely „Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér” címmel jelent meg. A stratégia két fő elemből állt: a kiberbiztonsági stratégiából és az úgynevezett NIS-irányelvre (network and information systems = hálózati és információs rendszerek biztonságára vonatkozó irányelv) tett javaslatból [215]. A stratégia második elemét képező NIS-irányelv kezdetben, 2013-ban még csak javaslatként létezett, azonban módosított formában, 2016-ban fogadták el, és az alábbi címen került bevezetésre: „Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről”.

Az EU kiberbiztonsági stratégiája és a NIS-irányelv bevezetése meghatározó lépés volt a tagállamok közötti együttműködés és a kiberbiztonsági fenyegetések elleni hatékony fellépés érdekében. Ezek az intézkedések azóta is az uniós kiberbiztonsági politika alapját képezik, amely folyamatosan igazodik a digitális környezet gyors változásaihoz. Azonban a NIS-irányelvhez fűzött változások elmaradtak, illetve több irányból sem minősültek teljeskörűnek. Ennek következtében az EU az eredeti NIS irányelv (2016/1148) tapasztalataira építve, kibővített hatókörrel és megerősített követelményekkel, létrehozta a NIS 2 irányelvet annak érdekében, hogy hatékonyabban kezelje a kibertérben megjelenő új fenyegetéseket [216]. Az új irányelvet 2022 decemberében tették közzé, és 2024. október 17-ig minden tagállam köteles volt átültetni azt saját nemzeti jogrendjébe. A végrehajtás kezdete 2024. október 18., amely egy új szakaszt nyit az EU kibervédelmi szabályozásában [217]. A NIS 1 és az azt követő NIS 2, kulcsfontosságú az Európai Unió kiberbiztonsági tájképe és gazdasága szempontjából. Ezen irányelvek célja az általános kiberbiztonsági helyzet javítása az egész EU-ban, elismerve a hálózati és információs rendszerek kritikus szerepét a mindennapi életben és a belső piac működésében [191, 218].

A kkv-kat gyakran a kiberbiztonsági kockázatokkal szemben legkevésbé érettnek és rendkívül sérülékenynek tekintik [64]. Ezt a sebezhetőséget súlyosbítja, hogy sok kkv alábecsüli a kiberbiztonsági fenyegetéseket, ami fokozott sebezhetőséghez és kockázatokhoz vezet, amelyek tényleges kihívásokká válhatnak számukra és más kapcsolódó felek számára [9]. A kkv-kat érintő kiberincidensek hatása súlyos lehet, beleértve a hírnévkárosodást, a pénzügyi veszteségeket és a működés megzavarását [67]. Továbbá az új technológiák, például a felhőszolgáltatások bevezetése, miközben üzleti lehetőségeket kínál, növeli a kiberfenyegetések lehetőségét is [9]. Ráadásul a kkv-k egyedi kihívásokkal szembesülnek a kiberbiztonsági intézkedések végrehajtása során, például a pénzügyi források és a technikai készségek hiányával [219]. E kihívások kezelése azonban kulcsfontosságú, mivel a szilárd kiberbiztonság versenyelőnyöket teremthet és új üzleti lehetőségeket nyithat. A NIS 2 elvárásai, bár potenciálisan megterhelőek lehetnek a kkv-k számára, egyben keretet is biztosítanak kiberbiztonsági helyzetük javításához, ami elengedhetetlen hosszú távú fenntarthatóságuk és növekedésük szempontjából az egyre inkább digitális gazdaságban.

Magyarország a közép-európai régióban élenjáróként fogalmazta meg nemzeti kiberbiztonsági stratégiáját, amelynek első változata már a 2010-es évek elején, 2013-ban

megjelent [220]. A stratégia korszerűsítésére hét évvel később került sor, amikor 2020-ban közzétették az új nemzeti kiberbiztonsági stratégiát *„Biztonságos Magyarország egy változékony világban”* címmel [221]. Ez a dokumentum a 1163/2020. (IV. 21.) Korm. határozat révén lépett hatályba [222].

A stratégia célkitűzései között kiemelt szerepet kapnak a következők [222]:

- A nemzeti intézkedések hatékonyságának és rugalmasságának erősítése, valamint a nemzeti szintű együttműködés szilárdítása a biztonság fokozása érdekében.
- A határon túli magyar közösségek alapvető jogainak védelme, különös tekintettel a digitális biztonságra.
- A versenyképes és exportorientált nemzeti védelmi ipar támogatása és fejlesztése.
- Hatékony többnemzeti együttműködések kialakítása, amelyek elősegítik a kiberbiztonsági és védelmi célok közös megvalósítását.
- A kétoldalú és regionális biztonsági együttműködések megerősítése, amelyek hosszú távú biztonságot nyújtanak.
- A fenntartható és globális fejlődés előmozdítása a kiberbiztonsági kezdeményezések által.

Ez a stratégiai dokumentum nemcsak a nemzeti szintű kiberbiztonsági kapacitások megerősítését célozza, hanem a regionális és nemzetközi együttműködésekben való hatékony részvételt is támogatja, összhangban Magyarország biztonsági prioritásaival és az európai uniós elvárásokkal. A bemutatott stratégiák rávilágítanak arra, hogy a vállalati és nemzeti szintű kiberbiztonsági megközelítések többféle védekezési módot kínálnak. Ezek gyakorlati megvalósításának értékelésére nemzetközi statisztikák és mutatók szolgálnak alapul, különös tekintettel Magyarország helyzetére.

A nemzetközi kapcsolatok kiépítése és a koordinált védelem erősítése kulcsfontosságú a hatékony kibervédelem szempontjából. A vizsgálatok, mint a „Digitális Mohács” és „Digitális Mohács 2.0” forgatókönyvek [223, 224], rávilágítanak a reális fenyegetésekre és a központi (állami) incidenskezelés növekvő jelentőségére.

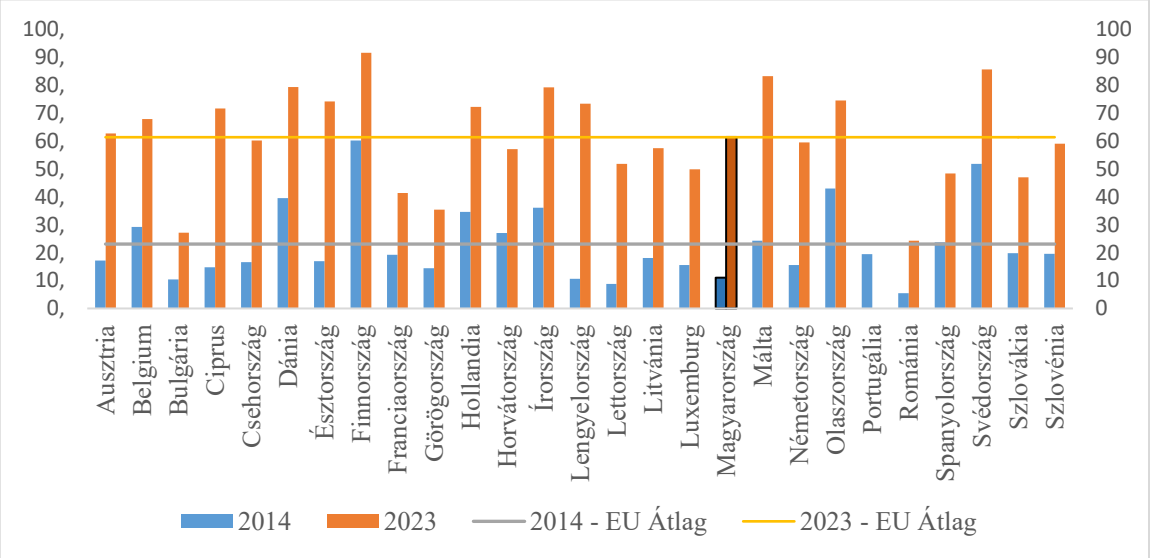
3. 4. Felhőszolgáltatások

Az IDG [225] felméréséből kiderül, hogy a vállalkozások 2015 óta, de főként az utóbbi években egyre nagyobb arányban alkalmaznak felhőszolgáltatásokat, és ez a tendencia a közeljövőben is folytatódni fog. A megkérdezett vállalatok kicsivel több mint a fele már

váltott is. A nagy mértékű átállások azonban még mindig a nagy vállalatokra jellemzőek, a kkv-k esetében ez még mindig várat magára. A felhőszolgáltatások sikerességét mi sem bizonyítja jobban, mint hogy 2021-ben közel 400 milliárd dollár értékű bevételt generált és további növekedés várható [226]. Az ENISA felmérése alapján pedig az is kiderül, hogy a szoftver (SaaS, Software as a Service) szinten veszik igénybe a felhő a vállalatok [227].

A felhőszolgáltatás (cloud computing – CC, felhő, felhőszolgáltatás) alkalmazása a kkv-k esetében is olyan előnyökkel jár, mint a rugalmasság, vagy épp a változó környezetre való gyors reagálás lehetősége [228]. Mindemellett kevesebb költséggel járnak, mint egy megfelelő digitális infrastruktúra kiépítése a vállalatnál. Annak ellenére, hogy ezek a szolgáltatások gyorsabbak és hatékonyabb belső folyamatokat tudnak eredményezni, mint a hagyományos verziójuk, azonban felmerül hátrányként, hogy az esetlegesen egy harmadik fél által kezelt és biztosított tárhelyet, szervert a megfelelő csatlakozás hiányában nem lehet elérni, ezáltal nagy a hálózatnak való kitettség, illetve a bizalmas adatok védelme mennyire biztosított [229]. Az előbb említett tényezők mellett azonban a rendszer adoptálását nagyban befolyásolja az adott vállalkozás mérete, digitális érettsége, valamint a vezetőség támogatói hajlandósága [230].

A 5. ábra az EU tagországaiban a felhőszolgáltatások használatának alakulását mutatja 2014 és 2023 közötti időszakban az EU-ban működő vállalkozások arányában, mérettől függetlenül.



5. ábra A felhőszolgáltatások használatának alakulása az Európai Unióban 2014 és 2023. években. Forrás: [231]. (saját szerkesztés)

Látható, hogy az EU átlaga 2014-ben közel 22%-os szintű felhőszolgáltatás használatot mutatott, ami 2023-ban már 59%-os szintet ért el. Az élen Finnország és Svédország található, ahol a vállalkozások több mint háromnegyede alkalmaz valamilyen felhőszolgáltatást. A legrosszabb helyzetben Románia és Bulgária van, ahol a vállalkozások alig több mint tíz százaléka (25-27%) alkalmazza ezeket a szolgáltatásokat. Magyarországot elnézve is az látható, hogy elmarad ezeknek a szolgáltatásoknak a kihasználtsága, mivel a vállalkozások 61%-ánál van alkalmazásban felhőtechnológia. Ez az érték az EU átlagnál 2%-kal magasabb. Összességében elmondható mindegyik tagállamról, hogy egyre több vállalkozás nyit a digitális újítások felé, azonban nem szabad elfelejteni, hogy valószínűleg az utóbbi 4-5 év növekedésében a pandémia is nagyban szerepet játszik. Bár azt látni, hogy növekedik a felhő igénybevétele, az eredményeket mélyebben megnézve azt látni, hogy többségében a levelezés és különböző fájlok, dokumentumok tárolására veszik igénybe a vállalatok, valamint a kereskedelem területén tapasztalható a szolgáltatás igazi térhódítása [232]. Portugália 2023-ban nem adott meg adatot.

A felhő átalakítja a szervezetek és iparágak működését. Az üzleti vonatkozású adatokhoz és elemzésekhez való hozzáférés nemcsak versenyelőnyhöz segíti a szervezeteket, hanem a felhőhasználat növekedésével a túlélésük szempontjából is kritikussá válik [233].

A felhő széles körben tanulmányozott téma az iparban és a tudományos életben egyaránt [234]. A megosztott erőforrások gazdaságos, skálázható és bármikor, bárhol használható jellemzői csak néhány azok közül, amelyek elősegítették és növelték a technológia iránti érdeklődést [235, 236]. A felhő három különböző formában és négy elérési módon áll a vállalkozások rendelkezésére. Megvalósulthat szoftver (Software as a Service, SaaS), platform (Platform as a Service, PaaS), illetve infrastruktúra (Infrastructure as a Service, IaaS) [237]. Az elérhetőséget tekintve pedig lehet nyilvános, magán, hibrid vagy közösségi [238]. A 3. táblázat A public, privát és hibrid felhőszolgáltatás típusok összehasonlítása (saját szerkesztés összefoglaló jelleggel és más aspektusokat is figyelembevéve mutatja a magán, privát és hibrid felhőszolgáltatások közötti különbségeket.

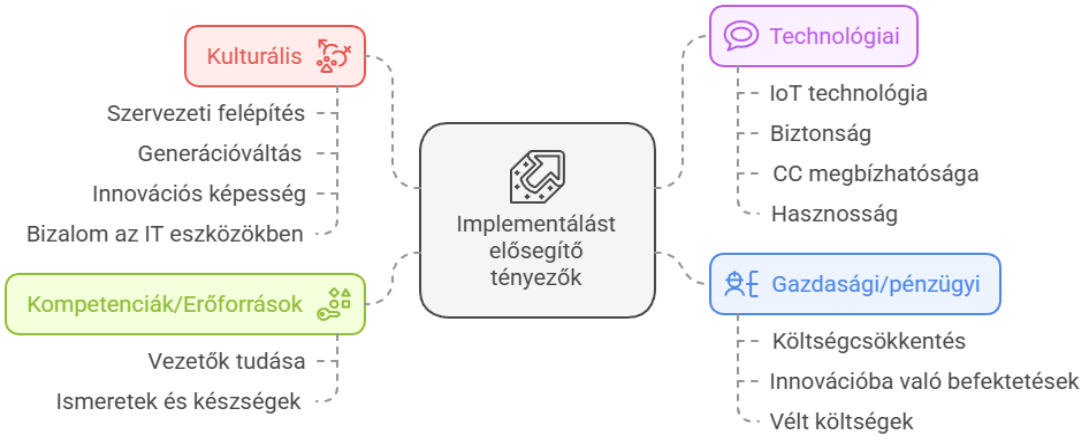
	Nyilvános felhő	**Privát felhő**	**Hibrid felhő**
Infrastruktúra	Több szervezet között oszlanak meg az erőforrások	Egyetlen szervezetnek dedikált	A nyilvános és a privát felhők kombinációja

Költség	Pay-as-you-go modell, költséghatékony	Magas kezdeti infrastrukturális beruházás, magasabb működési költségek	Az erőforrások felhasználásától függően változik
Vezérlés	A szervezet kisebb ellenőrzést gyakorol az infrastruktúra felett	A szervezet teljes mértékben ellenőrzi az infrastruktúrát	Változó, általában nagyobb a kontrol, mint a nyilvános felhők esetében
Skálázhatóság	Skálázható, igény szerint rendelkezésre álló források	Skálázható, de a skálázáshoz további beruházásokra lehet szükség.	Skálázható, megkönnyíti mind a köz-, mind a magánerőforrások bővítését
Biztonság	A biztonságot felhő-szolgáltató kezeli, a biztonsági intézkedések különböző szintjein	Magasabb szintű kontroll biztonsági intézkedések felett	A biztonsági aggályokat mind a nyilvános, mind a privát komponensek esetében kezelni kell
Rugalmasság	Rugalmasságot kínál az erőforrások elosztásában és felhasználásában	Rugalmas, de további beállítást és kompetenciát igényelhet	Rugalmasságot biztosít a nyilvános - és privát felhők legjobb kihasználása érdekében

3. táblázat A public, privát és hibrid felhőszolgáltatás típusok összehasonlítása (saját szerkesztés [239-241] alapján)

Ez a fejezet áttekintést nyújtott a felhőszolgáltatásokról, beleértve a kulcsfogalmakat, a telepítési modelleket és a szolgáltatási modelleket. Megvizsgáltam, hogy az EU-n belül a kkv-k körében mennyire használt eszköz. Mivel a felhő elfogadása továbbra is gyorsan növekszik, fontos, hogy gondosan mérlegeljük mind a lehetséges előnyöket, mind a kockázatokat. A következő fejezetben részletesen bemutatom a szervezetek számára a felhőszolgáltatások legfontosabb előnyeit és hátrányait. Ez a kiegyensúlyozott elemzés segít a felhő bevezetésével és a végrehajtási stratégiákkal kapcsolatos döntéshozatalban.

A 6. ábra bemutatja a felhő megvalósítását elősegítő tényezőket és csoportosítja azokat az akadályok és nehézségek elve szerint [3, 242-244].



6. ábra A felhő alkalmazását támogató tényezők (saját szerkesztés [3, 242-244] alapján)

A felhő segíthet a kkv-knak és a vállalkozásoknak a hatékonyság növelésében, a költségek csökkentésében és a saját piacaikon való versenyképességük javításában.

Azonban az előbb említett tényezők mellett akadnak hátrányok, negatívumok is, amiket érdemes a vállalatvezetésnek figyelembe venni, ha fontolóra veszik a technológia implementálását a vállalati működésbe [244].

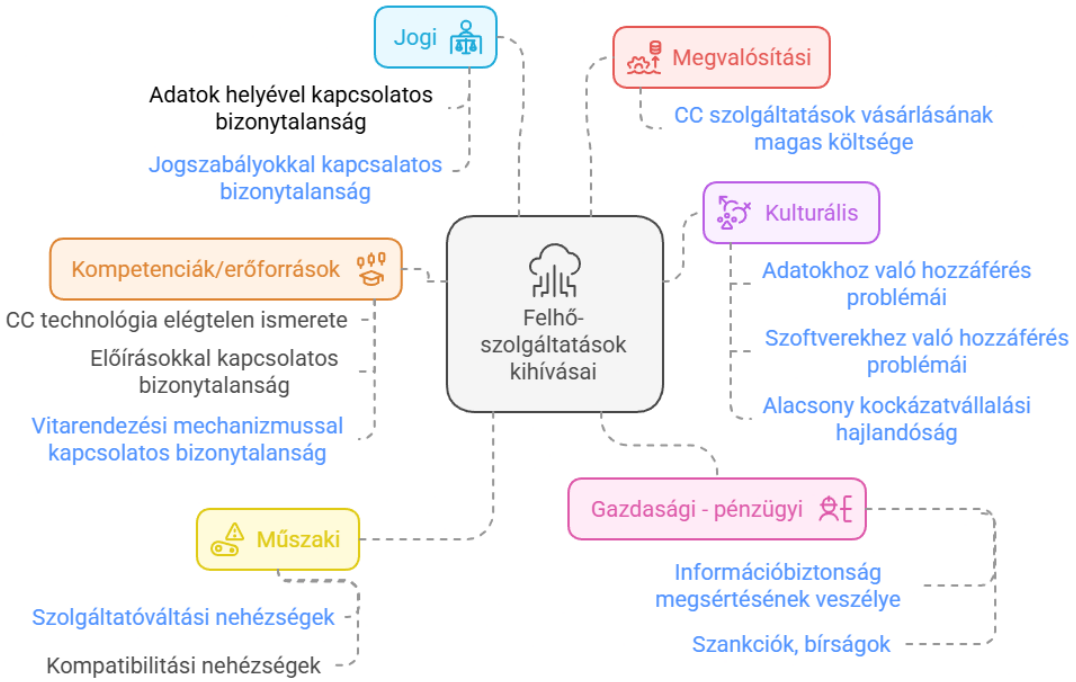
A felhőben rejlő sebezhetőségek és veszélyek a következők lehetnek [227]:

- Adatvédelmi incidensek: A felhőben tárolt érzékeny adatok sérülékenyek lehetnek a jogosulatlan hozzáférés vagy lopás szempontjából, akár hackerrel, akár emberi hiba miatt. A szolgáltatóknak robusztus biztonsági intézkedéseket kell bevezetniük, például titkosítást és többfaktoros hitelesítést, hogy minimalizálják ezeket a kockázatokat [1].
- Leállások: A felhő esetében előfordulhatnak leállások vagy egyéb zavarok, amelyek hatással lehetnek az üzleti működésre és a termelékenységre [2].
- Megfelelés: Egyes iparágakra szigorú előírások vonatkoznak, mint például az egészségügy (HIPAA) és a pénzügy (PCI), amelyek különleges adatvédelmi intézkedéseket írnak elő. A szolgáltatóknak biztosítaniuk kell, hogy szolgáltatásaik megfeleljenek ezeknek a szabályozásoknak, hogy elkerüljék az esetleges bírságokat és jogi szankciókat [245].
- Zártság: A felhasználók függővé válhatnak egy adott felhőszolgáltatótól, ami szükség esetén megnehezítheti a szolgáltatóváltást [246]. A szolgáltatóknak rugalmas és hordozható szolgáltatásokat kell nyújtaniuk, hogy minimalizálják a bezáródási kockázatokat [247].
- Költségek: A felhő költséghatékony lehet, de a költségek gyorsan emelkedhetnek, ha a felhasználási szokások megváltoznak, vagy ha további szolgáltatásokra van szükség. A szolgáltatóknak átlátható és rugalmas árképzési modelleket kell kínálniuk, hogy a felhasználók hatékonyan kezelhessék a költségeket [248].
- Interoperabilitás: Egyes felhőszolgáltatások nem feltétlenül kompatibilisek más szolgáltatásokkal, ami nehézségeket okozhat azoknak a felhasználóknak, akiknek több szolgáltatást kell integrálniuk egyetlen munkakörnyezetbe. A szolgáltatóknak biztosítaniuk kell, hogy szolgáltatásaik kompatibilisek legyenek más szolgáltatásokkal és technológiákkal az interoperabilitási kockázatok minimalizálása érdekében [247].

Már az első vizsgálat során szembetűnik, hogy a fenyegetések között olyan potenciális támadásokat jelennek meg, amelyek az információkkal vagy erőforrásokkal való

visszaéléshez vezethetnek, a sebezhetőségek között pedig a rendszer azon hibáira utalok, amelyek lehetővé teszik a támadás sikerét.

A 7. ábra összefoglalja azokat az irodalomban fellelhető akadályokat, nehézségeket és kockázatokat, amelyekkel a kkv-k szembesülnek a felhő használata során [1-3].



7. ábra A felhő alkalmazásának kihívásai/korlátjai és kockázatai (saját szerkesztés [1-3] alapján)

Az akadályok és nehézségek ilyen módon történő csoportosításának gondolata Orzes és munkatársai [249] kutatásából származik, valamint az Ipar 4.0 szakirodalmából, azonban az egyes csoportokba tartozó elemek ábrában szereplő kategorizálása szakirodalmi kutatásaim alapján történt [14, 83]. Az ábrán kékkel jelölt elemek a saját kutatásaim alapján kerültek az adott csoportba. A gazdasági-pénzügyi csoportba olyan tényezők tartoznak, mint a pénzügyi források és a jövedelmezőség, a költségek ésszerű szinten tartása - költségcsökkentés, egyértelműen meghatározott gazdasági előnyök és adókedvezmények hiánya, pénzügyi tervezés (kockázatkezelés és hatékonyság), valamint magas szakemberbeszerzési költség, hitelszerzési nehézségek. A felhőszolgáltatások kulturális nehézségei közé tartozik, hogy a vállalatok nem érzik szükségét ennek a technológiának a bevezetésének, a vezetés előnyeivel kapcsolatos nézeteltérések, a bizalom hiánya, a családi tulajdonban lévő kkv-k alacsony kockázati hozzáállása, nincs szükség új üzleti modellekre, nincs menedzsment. felkészültség, illetve a szervezet támogató funkcionális struktúrájának hiánya, a vezetők sem érzik szükségét az informatikai részleg állapotának megváltoztatására, a helyi támogató tényezők hiányát

sorolták fel. A jogi tényezők a joghatóság, az információbiztonsági aggályok, valamint a szabványok hiánya és a rendszerek megbízhatóságával kapcsolatos bizonytalanság. A kompetenciák/erőforrások csoportba olyan tényezők tartoznak, mint a hasznosság értékelésének hiánya, a képzett személyzet hiánya, az alkalmazottak ellenállása, az alkalmazottak képzésének hiánya, a személyzet folyamatos rotációja, a képességek nem ismerete és a felhőtechnológia lehetőségeivel kapcsolatos ismeretek hiánya. A technikai nehézségek közé tartozik a lassú internetkapcsolat, a nehéz átjárhatóság/kompatibilitás, a biztonság és az adatvédelem, a technikai kérdések (adatkezelés, adatkinyerés, hordozhatóság), az internetkapcsolat működésétől való függés és a gyenge informatikai infrastruktúra [250]. A megvalósítási problémák között szerepelt a magas koordinációs erőfeszítés, a megfelelő kutatópartner megtalálásának szükségessége, a változtatások kontrollálása, a tulajdonlás és a testre szabás, valamint a megvalósítás módszeres megközelítésének hiánya [251].

Az ENISA Cybersecurity Certification Statistics Reportja világosan rámutat, hogy az EU-ban a kiberbiztonsági tanúsítások száma habár növekszik, a szabályozási gyakorlatok erősen eltérőek és nem egységesek. Ez nemcsak a szolgáltatóknak jelent többletterheket (párhuzamos auditok, eltérő elvárások, magas megfelelési költségek), hanem a felhasználók bizalmát is gyengíti, mivel a tanúsítványok sokszor nem összehasonlíthatók. E kihívásokra válaszul az ENISA létrehozta az Information Assurance Framework-öt, aminek célja a biztonsági értékelések egységesítése és harmonizálása, különösen a felhőszolgáltatások területén [252].

Az SAP ECC, R/3, S/4 HANA és más ERP-megoldásokat kínáló magyar és nemzetközi szolgáltatók képessége, hogy kielégítsék a magyar kkv-k igényeit, több kritikus tényező hatására alakul, amelyek között szerepel az információbiztonság, a költségek és az erőforrások elosztása. A Software as a Service (SaaS) ERP-rendszerek bevezetése ígéretes a kkv-k számára, mert egyensúlyt teremt a képességek és az alacsonyabb irányítási és beruházási költségek között. Bár az adatbiztonság és a rendszer teljesítménye gyakran felmerülnek aggályként, a tanulmányok azt mutatják, hogy ezek a tényezők nem befolyásolják jelentősen a SaaS ERP bevezetésére vonatkozó döntést, mivel javulnak a biztonsági intézkedések és a gyártói támogatás [253, 254]. A magyar kkv-k számára, akárcsak a globális kkv-k számára, a bevezetés költségei döntő szerepet játszanak az ERP-rendszerek bevezetésének döntésében. A SaaS-modellek előnyt jelentenek azzal, hogy a beruházási költségeket működési költségekké alakítják át, ami jobban megfelel a

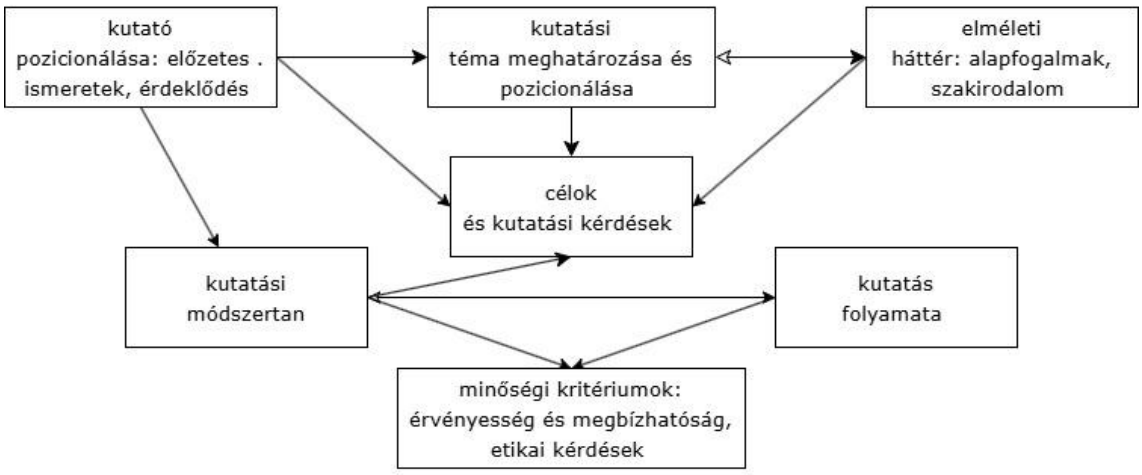
kkv-k pénzügyi korlátainak [253, 255]. Továbbá tanulmányok azt mutatják, hogy a költséghatékony megoldások, mint például az oroszországi 1C ERP rendszer, sikeresen kielégítik a kkv-k igényeit a funkcionalitás, az ár és a bevezetés sebessége közötti egyensúly megteremtésével [256]. Az ERP sikeres bevezetése a kkv-kban több kritikus sikertényező figyelembevételét igényli, mint például a rendszerkompatibilitás, a felhasználóbarát jelleg és az üzleti igények kielégítése. A szállítói támogatás, valamint a testreszabás és az értékteremtés iránti hajlandóság elengedhetetlen a kezdeti bevezetés és az azt követő kiigazítások során [254, 257]. A kkv-k korlátozott erőforrásaik miatt egyedi kihívásokkal szembesülnek, amelyek ellentétben állnak a nagyvállalatok igényeivel. Az olyan speciális stratégiák, mint a leggyengébb versenytényezőkre való összpontosítás, jelentős versenyelőnyöket eredményezhetnek az erőforrásokkal korlátozott kkv-k számára [258]. Az információs rendszerek, beleértve az ERP-t is, hatékonysága a versenykörnyezetben működő kkv-k stratégiai céljainak, az ügyfélszolgálat fejlesztésének, a költségek csökkentésének és a termelékenység növelésének függvénye [259]. Összességében a magyar és nemzetközi ERP-szolgáltatók által kínált szolgáltatások versenyképesek lehetnek és kielégítően megfelelhetnek a magyar kkv-k igényeinek, feltéve, hogy olyan megoldásokat vesznek figyelembe és valósítanak meg, amelyek hangsúlyt fektetnek a költségkezelésre, az információbiztonságra és a hatékony erőforrás-elosztásra az üzleti folyamatok támogatása érdekében. Míg ezeknek a szolgáltatóknak folyamatosan biztosítaniuk kell a kkv-kat a biztonság tekintetében és alkalmazkodniuk kell az egyedi üzleti igényekhez, a stratégiai bevezetés és a beszállítói együttműködés továbbra is kulcsfontosságú.

4. Az empirikus kutatás bemutatása

Tudományos megismerés során nem módszert választunk, hanem problémát kívánunk megoldani. A kvalitatív kutatások eredményei gyakran feltárnak olyan mintázatokat, jelenségeket és jellemzőket, amelyek kvantitatív módszerekkel esetleg nem lennének észlelhetők. Az alkalmazott szöveganalitikai megközelítés különösen jól használható a vélemények, attitűdök és imázsok formálódásának modellezésére [260]. A kvalitatív kutatásom szakértői interjúkon alapult, melynek elsődleges célja a felhőszolgáltatások és a kkv-k kapcsolatának vizsgálata, annak megértése.

Az elemzés során nem használtam előzetesen kidolgozott kódrendszert; a kódok maguk a szövegek iteratív elemzése során alakultak ki [261]. A kutatás egyik célja az volt, hogy feltárjam, mit tudnak a megkérdezettek a felhőről. Emellett az alkalmazott módszer lehetővé tette, hogy az elemzés során figyelembe vegyem a szövegek kontextuális elemeit is, amelyek jelentős hatással lehettek a vizsgált témakörökre [262].

A kutatás keretét és folyamatát, valamint az azok között fennálló kapcsolatot szemlélteti a 8. ábra. A kutatási folyamat több, egymással összefüggő elemet foglal magában, amelyek befolyásolják egymást és egymásra épülnek.



8. ábra A kutatás kerete és befolyásoló tényezői (saját szerkesztés)

A kutatási téma meghatározása és pozicionálása mint kezdeti lépés meghatározza a vizsgálat fókuszát és hatókörét, megalapozva ezzel a későbbi szakaszokat. Az alapfogalmak és a szakirodalom áttekintése segít a meglévő ismeretek hiányosságainak azonosításában és a kutatás irányának finomításában. Az elméleti háttér által vezérelve konkrét célok és kérdések fogalmazhatók meg az azonosított hiányosságok kezelésére.

Az érvényesség, a megbízhatóság és az etikai megfontolások a teljes kutatási folyamat során beépülnek a vizsgálat hitelességének és az etikai normák betartásának biztosítása érdekében. A választott módszereket a kutatási kérdések, az elméleti keret és a minőségi kritériumok befolyásolják, meghatározva az adatgyűjtés és -elemzés módját. A kutató előzetes ismeretei és érdeklődése alakítja a kutatási téma kiválasztását, az elméleti megközelítést és a módszertani választásokat, befolyásolva a teljes kutatási folyamatot. Ezek az elemek összekapcsolódnak és iteratívak, és minden egyes komponens befolyásolja és finomítja a többit a kutatási folyamat során. Az új felismerések megjelenésével a korábbi szakaszok felülvizsgálhatók és módosíthatók, biztosítva a tanulmány átfogó és dinamikus megközelítését.

A kutatáshoz a primer adatokat félig strukturált interjúk segítségével gyűjtöttem össze. Az ATLAS.ti szöveganalitikai szoftvert használtam a kvalitatív adatok strukturálására és tartalomelemzésére. A tartalomelemzés olyan kutatási technika, amely a szövegek vizsgálata révén nemcsak magára a szövegre, hanem annak tágabb kontextusára is igyekszik következtetéseket levonni. Az elemzés során nem a nyelvtani szerkezetre, hanem a szavak, mondatok és bekezdések tartalmára koncentráltam. Ezáltal a szövegen túlmutató, szélesebb jelenségekre vonatkozó érvényes megállapításokat is megfogalmazhattam [261].

4. 1. Félig strukturált interjúk általános elemzése

A kutatás során összesen 34 félig strukturált interjút bonyolítottunk le online platformon keresztül. 2024 januárja és októbere között összesen 34 interjút készítettem 16 szolgáltatóval/disztribútorral és 18 kkv-nál. A megkérdezettek információbiztonsági és-vagy felhőszolgáltatásban érintettek szolgáltatói és-vagy vállalati igénybe vevői oldalról. Az interjúalanyok részletesebb bemutatását a 3. sz melléklet tartalmazza. Az interjúalanyok kiválasztása részben személyes ismeretségek, szakmai ajánlások alapján zajlott, másrészt véletlenszerű módon történt a Nemzeti Cégtár online adatbázisának felhasználásával. Az interjúalanyok kiválasztásánál arra törekedtem, hogy lehetőség szerint a kkv-k vezető beosztásban dolgozó munkavállalót érjem el, mert úgy vélelmeztem, hogy ezek az emberek rendelkeznek a felhőszolgáltatás használata kapcsán információval és releváns információkat tudnak szolgáltatni. A szolgáltató oldal tekintetében a nyújtott szolgáltatás és a kkv szektor ismerete játszotta a fő kiválasztási szempontot.

Az interjúk során nyitott kérdéseket tettem fel. A témákról előzetesen tájékoztattam a kutatásba bevont válaszadókat, így fel tudtak készülni az interjúra. Az interjúk egyenként 1-1,5 órát vettek igénybe, lehetővé téve a témák alapos feltárását és a résztvevők véleményének részletes kifejtését. Az online formátum lehetővé tette a földrajzi korlátok áthidalását és a résztvevők számára kényelmes környezet biztosítását. Az interjúk során törekedtünk a nyitott, bizalmas légkör megteremtésére, amely elősegítette az őszinte és mélyreható válaszok megszületését. Az interjúvázlat rugalmas alkalmazásával biztosítottuk, hogy minden kulcsfontosságú témakört érintsünk, miközben teret hagytunk az egyéni tapasztalatok és meglátások kifejtésére is. Az interjúk célja az volt, hogy mélyreható betekintést nyerjek a kkv-k felhőszolgáltatásokkal kapcsolatos tapasztalataiba, attitűdjeibe és kihívásaiba, valamint a szolgáltatói oldal perspektívájába. A kkv-kkal folytatott interjúk során a vállalkozások saját tapasztalatairól, ismereteiről és véleményéről kérdeztünk. A felhőszolgáltatókkal készített interjúk során ugyanazokat a kérdésköröket érintettük, de a szolgáltatókat arra kértem, hogy az ügyfélkörükben előforduló kkv-k szemszögéből válaszoljanak.

Az interjúk során a következő főbb témaköröket érintettük:

1. Demográfiai adatok: A válaszadók nemét, korát, beosztását és munkatapasztalatát rögzítettem.
2. Vállalati jellemzők: A cég iparági besorolását, méretét és az interjúalany jelenlegi pozíciójában eltöltött idejét, valamint IT területen szerzett tapasztalatát vizsgáltam.
3. A kkv-k információbiztonsági helyzete: Az interjúalanyokat arra kértem, jellemezzék a kkv-k általános információbiztonsági helyzetét országos viszonylatban és más vállalkozásokhoz képest.
4. Felhőszolgáltatással kapcsolatos ismeretek: A kkv-k felhőszolgáltatásokkal kapcsolatos tudásszintjét és tájékozottságát mértem fel.
5. Trendek és motivációk: A felhőszolgáltatások igénybevételével kapcsolatos tendenciákat és a kkv-k motivációit vizsgáltam.
6. Akadályok és kihívások: Feltártuk azokat a tényezőket, amelyek visszatartják a kkv-kat a felhőszolgáltatások használatától, valamint az ezzel kapcsolatos kihívásokat. Az interjúk során nyert információk lehetővé teszik, hogy átfogó képet kapjak a kkv-k és a felhőszolgáltatások viszonyáról, mind a felhasználói, mind a szolgáltatói oldal szemszögéből.

Összesen 18 kkv oldali és 16 szolgáltatói oldali válaszadó állt a rendelkezésemre. A kkv oldal válaszadói a nemek arányát tekintve 12 férfi (70,6%) és 5 nő (29,4%), az átlagéletkor 43,6 év volt, ebből a legfiatalabb 28 éves, legidősebb pedig 58 éves volt. A beosztások változatosak, többek között ügyvezetők, IT vezetők, és szakmai pozíciókat sikerült megszólítanom. Iparági besorolás széles skálán mozog, például számítógépes programozás, építőipar, gyógyszeripar, élelmiszeripar.

A szolgáltatói oldal nemek arányában 15 férfi (93,75%) és 1 nő (6,25%). Az átlagéletkor 42,1 év volt, ebből a legfiatalabb: 27 éves, a legidősebb 55 éves. A beosztások főként IT-hoz kapcsolódnak, például IT manager, rendszergazda, biztonsági vezető. Iparági besorolás túlnyomórészt IT-hoz és informatikához kapcsolódik. Ahogy az látható, a szolgáltatói oldalon jelentősen magasabb a férfiak aránya. Az átlagéletkor hasonló mindkét oldalon - A kkv oldal változatosabb iparági besorolást mutat, míg a szolgáltatói oldal főként IT-fókuszú, érthető módon.

A félig strukturált interjúk során az elméleti telítettség [263] (theoretical saturation) a 13. interjúnál (6 + 7) következett be. Az elméleti telítettség az elemzés azon pontjaként határozható meg, amikor már nem található további adat, és így kialakíthatók a kutatott jelenség tulajdonságai. Mivel a kutató újra és újra hasonló eseteket lát, vagyis empirikusan bizonyossá válik, hogy egy kategória telítődött [31]. A félig strukturált interjúk vázlata az 1. sz és 2. sz. mellékletekben látható.

Az interjúk során elhangzottakat digitális hangrögzítő eszközzel rögzítettem, a résztvevők előzetes beleegyezésével. A hangfelvételek több részletben készültek el, összesen 50 óra időtartammal. A szó szerinti átiratokat megőrizve az eredeti megfogalmazásokat és nyelvi fordulatokat kb. 3 hét alatt készítettem el, 430.734 karakter (171 oldal) terjedelemben word formátumban. Az interjúk leíró statisztikai jellemzőit a 4. táblázat tartalmazza.

Interjúk száma	34 db
Résztvevők megoszlása	• 18 fő kkv szereplő • 16 fő szolgáltató
Interjúk időtartama és formája	1–1,5 óra – online
Teljes hangfelvétel időtartama	50 óra
Felvétel módja	Digitális hangrögzítő, videófelvétel
Átirat készítésének ideje	Kb. 3 hét
Átiratok terjedelme összesen	• 430.734 karakter • 171 oldal (A4 oldal – TNR 12)

Átirat jellemzői	Szó szerinti lejegyzés, eredeti megfogalmazások és nyelvi fordulatok megőrzésével
Elemzési módszerek (Atlas.ti sw)	• Kódolás (Grounded theory alapon) • Kódgyakoriságelemzés • Kontextuselemzés – kódhálózat • Szentimentelemzés

4. táblázat Az interjúkészítés és elemzés jellemzői (saját szerkesztés)

Az átiratok elkészítése során különös figyelmet fordítottam a non-verbális kommunikációs elemek (pl. hangsúly, szünetek) jelölésére is, amelyek értékes többletinformációt hordozhatnak az elemzés során. Az átiratok elkészítése után az adatok előkészítése következett. Ennek során eltávolítottam az azonosításra alkalmas személyes információkat, biztosítva a résztvevők anonimitását. Az átiratokat egységes formátumba rendeztem, megkönnyítve a későbbi kódolási és elemzési folyamatokat. Emellett minden interjúhoz egyedi azonosítót rendeltem, amely lehetővé tette a visszakereshetőséget, miközben megőrizte az anonimitást. Az elemzés során D1-D34 sorszámmal jelöltem, hogy melyik interjúalanytól származik a szövegrészlet. Az előkészített adatokat biztonságos, jelszóval védett digitális adatbázisban tároltam, biztosítva az adatvédelmi előírásoknak való megfelelést és a kutatás integritását. Ez a gondos előkészítési folyamat megalapozta a későbbi mélyreható elemzést és a GT módszertan sikeres alkalmazását.

Az interjúk elsődleges elemzése az interjúk általános átolvasásával indult. Először az felhőszolgáltatással kapcsolatos ismereteket vizsgáltam meg. A szövegrészletek (D6, D7, D8, D20) kiemelik, hogy a felhasználók képzése kulcsfontosságú az információbiztonsági problémák megelőzésében. Alapvető ismeretek, például a helyes jelszókezelés, jelentősen javíthatják a biztonságot. A megkérdezett vállalatok gyakran alkalmaznak szimulált phishing támadásokat és tudatosságnövelő kampányokat a munkavállalók felkészítésére. Ezen túlmenően pedig a biztonsági tudatosság folyamatos fejlesztése érdekében rendszeres képzéseket tartanak. Az interjúk arra utalnak, hogy a megkérdezett vállalatok egy részénél a biztonságtudatosság fejlesztése nem egyszeri esemény, hanem folyamatos, többrétű folyamat, amely magában foglalja az oktatást, gyakorlati teszteket és rendszeres frissítéseket.

„A felhasználók oktatása kulcsfontosságú, hogy ne okozzanak adatbiztonsági problémákat” (D6).

„A szimulált phishing támadások segítenek a biztonsági tudatosság fejlesztésében” (D7).

„A biztonsági tudatosság fejlesztése érdekében rendszeresen tartunk oktatásokat és teszteket, különösen az új belépők számára” (D8).

„A felhasználók többsége nem érti a biztonsági rendszerek működését. Egy egyszerű oktatás, például a jelszókezelésről, már sokat segítene” (D20).

A különböző résztvevőknek a felhőszolgáltatásokkal és az információbiztonsággal kapcsolatos tapasztalataikra és szempontjaikra vonatkozó válaszait elemezve több kulcsfontosságú különbség és hasonlóság rajzolódik ki.

Ezek közül először a hasonlóságokat mutatom be, melyek az alábbiak.

1. *A felhőszolgáltatások fokozott használata*: A legtöbb résztvevő a felhőszolgáltatások bevezetésének növekvő tendenciáját észlelte, ami a vállalatok IT-infrastruktúrájának üzemeltetési és kezelési módjában bekövetkezett változást jelzi.
2. *A biztonsággal kapcsolatos aggodalmak*: A felhőben tárolt adatok biztonságával kapcsolatban közös az aggodalom. A résztvevők kifejezték, hogy szükség van szilárd biztonsági intézkedésekre és képzésre annak biztosítása érdekében, hogy az alkalmazottak megértsék, hogyan kell kezelni az érzékeny információkat.
3. *Képzési és oktatási igények*: A résztvevők többsége kiemelte az alkalmazottak képzésének fontosságát a felhőszolgáltatások és a biztonság összetettségének eligazodásához, utalva arra, hogy a megértés hiánya jelentős kihívásokhoz vezethet.
4. *Rugalmasság és hozzáférhetőség*: A résztvevők általában egyetértettek abban, hogy a felhőszolgáltatások nagyobb rugalmasságot és elérhetőséget biztosítanak, lehetővé téve a munkavállalók számára, hogy különböző helyszínekről dolgozzanak, ami egyre fontosabb a hibrid munkakörnyezetben.

A hasonlóságok után pedig következzenek a különbségek.

1. *A felhőalapú és a helyhez kötött megoldások megítélése*: Egyes résztvevők a skálázhatóság és a könnyű kezelhetőség miatt a felhőalapú megoldásokat részesítették előnyben, míg mások óvatosabbak voltak, és bizonyos alkalmazások esetében a biztonsági kockázatok miatt a helyhez kötött megoldások fontosságát hangsúlyozták.

2. *Az információbiztonsággal kapcsolatos tapasztalatok*: A válaszok jelentősen eltértek a szervezeten belüli biztonságtudatosság és gyakorlat szintjét illetően. Egyes résztvevők magas szintű biztonsági képzésről és tudatosságról számoltak be, míg mások a strukturált képzés és a biztonsági protokollok megértésének hiányát jelezték.
3. *Végrehajtási kihívások:* A résztvevők eltérő tapasztalatokat szereztek a felhőalapú megoldások bevezetésével kapcsolatban. Egyesek zökkenőmentes átmenetről számoltak be, míg mások jelentős akadályokkal szembesültek, különösen a munkavállalók változással szembeni ellenállása és a meglévő rendszerek átállításának összetettsége tekintetében.
4. Forgalmazói/szolgáltatói kapcsolatok: A felhőszolgáltatókkal szembeni bizalom és megbízhatóság szintje a résztvevők között eltérő volt. Egyesek bizalmat mutattak a szolgáltatóik iránt, míg mások szkeptikusabbak voltak, az adatok tulajdonjogával és a szállítói bezáródás lehetőségével kapcsolatos aggodalmakra hivatkozva.

A felhőszolgáltatások és az információbiztonság előnyeivel és kihívásaival kapcsolatban a válaszok közös témákat tartalmaznak, az egyéni tapasztalatok és meglátások a szervezeti környezet, a korábbi tapasztalatok és a konkrét iparági követelmények alapján nagymértékben eltérnek. A válaszok sokfélesége rávilágít arra, hogy a felhő bevezetéséhez és a biztonsági képzéshez olyan testre szabott megközelítésekre van szükség, amelyek figyelembe veszik az egyes szervezetek egyedi körülményeit.

Az információbiztonság és felhőhasználat terén jelentős különbségek mutatkoznak a vállalatok között, méretüktől és erőforrásaiktól függően, illetve abban a tekintetben is, hogy a felhőszolgáltatás tekintetében csak felhasználói szemmel, vagy üzemeltetői oldalról is rendelkeznek-e rálátással. A nagyobb, valamint az üzemeltető cégek IT-vezetői általában fejlettebb biztonsági stratégiákat alkalmaznak, míg a kisebb cégek, akik gyakran kénytelenek kompromisszumokat kötni a költségvetési korlátok miatt. A felhőmegoldások használata is eltérő fázisokban van: egyes vállalatok már teljes infrastruktúrájukat a felhőbe költöztették, míg mások csak bizonyos funkciókat integráltak eddig.

„Nekünk minden a felhőben van, mi on-prem csináljuk a mentés róla napi szinten." (D18)

„Csak egy bizonyos szegmensét használjuk a felhőnek, lokális hálózatunk van itt lent saját házon belül, tehát ezek nem felhőben futnak, minden itt van lokálisan." (D6)

A felhőszolgáltatások használata és a megfelelő szakértelem között szoros összefüggés figyelhető meg. A hiányos tudás jelentős biztonsági kockázatokat rejthet magában, mivel az alkalmazottak gyakran nem értik teljesen a felhő működését, ami hibás konfigurációkhoz és potenciális adatvesztéshez vezethet. Ez különösen igaz a kkv-k esetében, ahol az adatok helyi tárolása gyakran nagyobb biztonságérzetet nyújt.

„Sok ember használja megfelelő tudás és megfontolás nélkül" (D5)

„A kkv-knál nem feltétlenül látom és érzem ezeket a megfelelő tréningeket, képzéseket, de én sajnos azt látom, hogy jellemzően a kkv-nál úgy általánosan az ott lévő szakembereknek, ott lévő munkavállalóknak a képzettsége is valamilyen szinten alacsonyabb, és emiatt még inkább hátrányban vannak a kkv-k így IT biztonság és bármilyen más szempontból." (D23)

A felhőszolgáltatások iránti bizalom szintje erősen függ a rendelkezésre álló ismeretektől, és az ismeretek hiánya gyakran eredményez bizonytalanságot és ellenállást a technológia adoptálásával szemben. A következő szekció ezt mutatja be.

„Sokan bizonytalanok, hogy mi történik, ha nem érik el az adatokat" (D6).

„Sok ügyféllel beszélgettem, és kicsit félnek a felhőtől, mert nem megfogható úgy, mint a szerverterem esetében, hogy bemegy, megfogja az eszközeit és „ez az enyém"… Birtoklási vágy. A felhőnél viszont nincs meg, az úgy valahol van, Dublinban itt-ott, nem is Magyarországon. Ez olyan ijesztően tud hangzani, egészen addig amíg meg nem ismerik."(D18)

A felhőrendszerek és az információbiztonsági mechanizmusok összetettsége miatt elengedhetetlen a felhasználók oktatása. Az átlagos felhasználók gyakran küszködnek a rendelkezésre álló lehetőséggel és szolgáltatással. A képzés nemcsak a könnyű használat, hanem a biztonság fokozása szempontjából is elengedhetetlen, mivel az emberi hiba továbbra is jelentős sebezhetőséget jelent.

„Az átlagos felhasználók könnyen elvesznek a sok lehetőség és szolgáltatás között" (D3).

„Hiába építünk erős védelmet, ha belülről kiszivárog az információ" (D6).

A felhőszolgáltatások integrációját befolyásoló kompetenciakülönbség gyakran tapasztalható az informatikai szakemberek és a döntéshozók között. A döntéshozók általában a pénzügyi szempontokra összpontosítanak, míg az informatikai szakemberek a technológiai alkalmasságot és a biztonságot helyezik előtérbe.

„A vezetés nem mindig érti, miért fontos a biztonság, amíg nem történik incidens" (D23).

Gyakori jelenség, hogy a vezetés csak egy biztonsági incidens bekövetkezése után ismeri fel teljes mértékben az információbiztonság jelentőségét. A kkv-k gyakran átfogó stratégia nélkül vezetik be a felhőszolgáltatásokat. Ez idővel megnövekedett költségekhez vagy technológiai hátrányokhoz vezethet. A kisvállalkozások hajlamosak az IT-biztonságot ad hoc módon kezelni, ahelyett, hogy előre gondolkodnának.

„A kis cégek nem gondolkodnak előre, gyakran ad hoc módon kezelik az IT-biztonságot" (D23).

A felhőszolgáltatások megfelelő alkalmazása egyszerűsítheti az informatikai műveleteket, ha az alkalmazottak kompetenciája megfelelő. A felhőszolgáltatások a rugalmasság és az adatbázisokhoz való távoli hozzáférés révén növelik a hatékonyságot. Az olyan nagy szolgáltatók, mint a Microsoft és a Google beépített biztonsági mechanizmusokat és a jogszabályi megfeleléseket kínálnak, ami növeli a megbízhatóságot.

„A felhő hozzáférhetővé teszi az adatokat bárhonnan" (D4).

„A nagyobb felhőszolgáltatók megfelelően biztosítják a biztonságot" (D1).

Ezek a pontok rávilágítanak a műszaki szakértelem, a stratégiai tervezés és a felhasználói oktatás egyensúlyának fontosságára a felhőszolgáltatások sikeres bevezetése és kezelése során a szervezetekben, különösen a kkv-kban.

Az érzékeny adatokat tároló vagy kezelő rendszereket célzó kibertámadások egyre kifinomultabbá válása miatt egyre nagyobb szükség van felhő- és információbiztonsági képzésekre. A folyamatos kapacitásépítés és a digitális készségekkel kapcsolatos kompetenciák elengedhetetlenek ahhoz, hogy szembe tudjunk nézni ezekkel a növekvő fenyegetésekkel, a kiberbiztonsági gyakorlati képzések pedig elengedhetetlenek a szakemberek továbbképzéséhez [264]. A felhőtechnológiák gyors fejlődése új

kiberbiztonsági kockázatokat hozott, így a biztonság komoly kihívást jelent a felhőalapú szolgáltatások számára [265].

4. 2. Adatelemző szoftver alkalmazása

Az ATLAS.ti szoftver a GT megközelítés során alkalmazott kvalitatív kutatást segíti. A szoftver hatékonyan támogatja az adatelemzés folyamatát, növeli a kutatás átláthatóságát és megbízhatóságát, továbbá a szoftver lehetővé teszi a különböző formátumú adatok (szöveg, kép, hang, videó) egységes kezelését és rendszerezését. Ez jelentősen megkönnyíti a nagy mennyiségű kvalitatív adat kezelését és áttekintését. A szoftver fejlett kódolási funkciókat kínál, amelyek lehetővé teszik a kutatók számára, hogy hatékonyan azonosítsák és jelöljék az adatokban megjelenő témákat, mintázatokat. Ezentúl a szoftver támogatja a nyílt, axiális és szelektív kódolást, ami különösen hasznos a GT alkalmazása során. A kódok hierarchikus rendszerbe szervezhetők, ami segíti a fogalmi struktúrák kialakítását és az elméletalkotást. Az ATLAS.ti szoftver különösen alkalmas a GT megközelítés támogatására a kvalitatív kutatásokban. A GT egy olyan módszertan, amely az adatokból kiindulva, induktív módon építi fel az elméletet. A GT módszertan egyik népszerű szoftveres támogatója az ATLAS.ti, amely segített a kvalitatív adatok elemzésében és az elméletalkotásban. Az ATLAS.ti vizuális, térbeli és összekapcsolt működési módjával különösen alkalmas a komplex, több mintát, longitudinális adatokat és többféle adattípust tartalmazó projektek kezelésére [266]. A szoftver lehetővé teszi a kódolás és modellalkotás iteratív folyamatát, ami a GT lényeges eleme [267].

Az interjúk elemzése során a következő módszereket alkalmaztam:

1. Kódolás
2. Kódgyakoriságelemzés
3. Kontextuselemzés – kódhálózat
4. Szentimentelemzés

A felvázolt sorrendet az indokolja, hogy a kódolás után a kódok gyakoriságának elemzése áttekintést nyújt a fő témákról. A kontextuselemzés ezekre a témákra épít, mélységet és árnyalatokat adva hozzá, illetve a mögöttes okokat és körülményeket tárja fel. A szentimentelemzés tovább gazdagítja a megértést az érzelmi szempontok feltárásával, például feltárva azokat az attitűdöket, amelyek nem feltétlenül vannak kimondva, de jelentősen befolyásolják a felhő használatára vonatkozó döntéseket. Ez az átfogó elemzés feltárhatja, hogy a különböző kontextusokban hogyan érzékelik eltérően a felhő

használatával kapcsolatos konkrét aggályokat vagy előnyöket, és hogy ezek az észlelések hogyan befolyásolják a kkv-k felhőtechnológiákkal kapcsolatos általános hozzáállását.

Az ATLAS.ti támogatja ezeket a kódolási szakaszokat, lehetővé téve a rugalmas adatgyűjtést, elemzést [267]. A szoftver nemlineáris felépítése támogatja a GT iteratív megközelítését, lehetővé téve a folyamatos finomításokat az adatok alapján [267, 268]. Ez a megközelítés különösen hasznos lehet az összetett jelenségek vizsgálatánál [269, 270]. A kódolás folyamata lehetővé teszi, hogy a nyers adatokból strukturált, értelmezhető és elméletileg megalapozott következtetéseket vonjunk le, amelyek választ adnak a kutatási kérdésekre és hozzájárulnak a vizsgált jelenség mélyebb megértéséhez. Az ATLAS.ti szoftver hatékony eszközt kínál a kvalitatív adatok hálózatelemzésére, lehetővé téve a komplex kapcsolatok vizualizációját. Az elemzés első lépése a szövegek, képek vagy egyéb adatok kódolása. A kódok reprezentálják a kulcsfogalmakat vagy témákat. A kódok között különböző típusú kapcsolatokat lehet definiálni, például „része", „oka", „ellentéte" stb. Az ATLAS.ti lehetővé teszi a kódok és kapcsolataik vizuális megjelenítését hálózati grafikonként. A hálózati nézet alapján azonosíthatók a központi fogalmak, klaszterek és mintázatok. A hálózatelemzés segít megérteni a fogalmak közötti bonyolult kapcsolatrendszert. A grafikus megjelenítés intuitív módon teszi érthetővé az adatok struktúráját. Meghatározhatók a hálózat kulcsfontosságú csomópontjai. A klaszterelemzés révén azonosíthatók az összetartozó fogalomcsoportok. A feltárt mintázatok új kutatási kérdések megfogalmazását ösztönözhetik. A hálózati struktúra alapján átfogó elméleti keretek alkothatók.

4. 2. 1. Kódolás

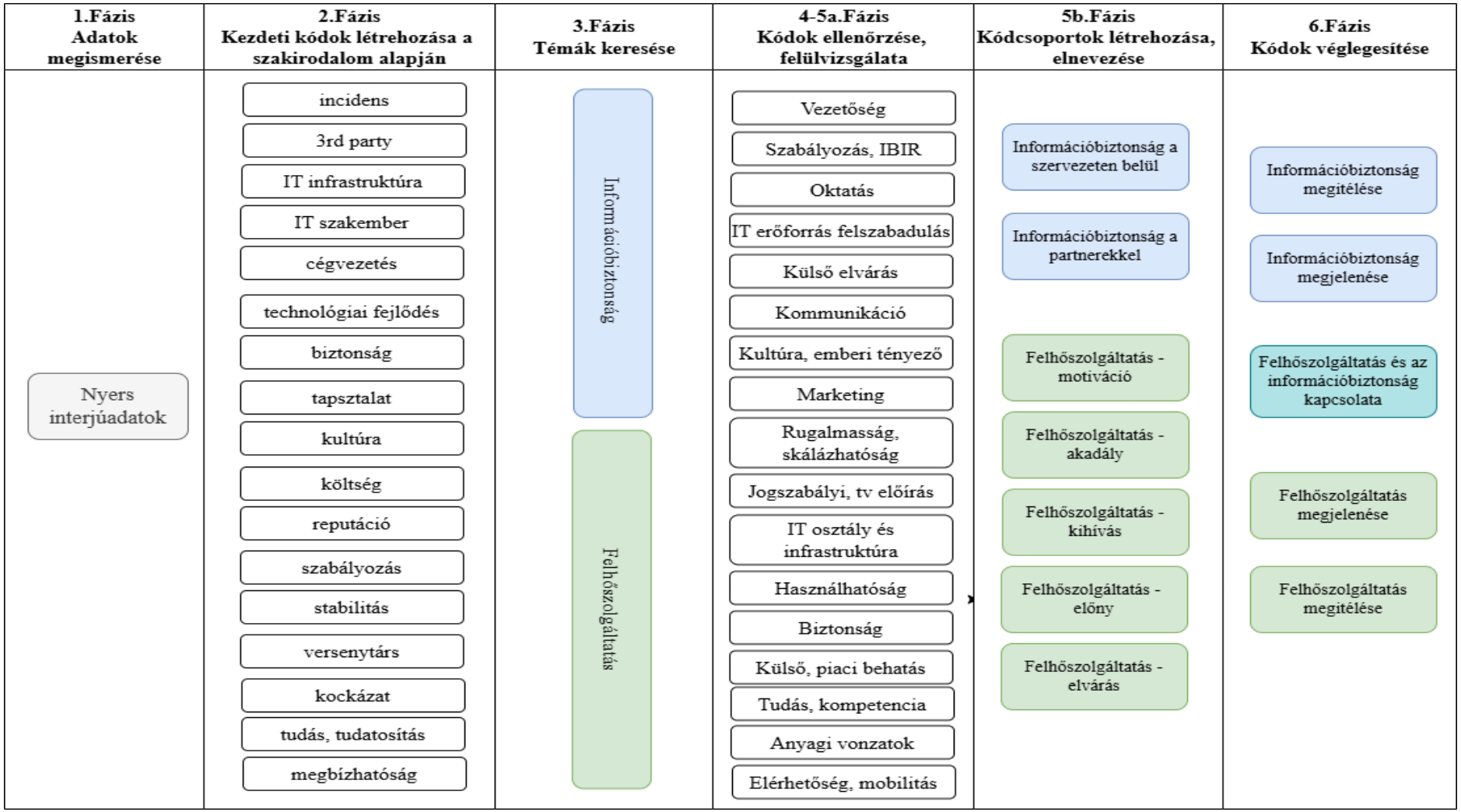
Az alábbiakban lépésről lépésre bemutatom, hogyan alkalmaztam a GT-t az interjúk során létrehozott megadott kódok és adatok alapján. A kvalitatív kutatási interjúk kódolása iteratív folyamat, amely szisztematikus elemzést és értelmezést igényel A kódolás előrehaladtával a kódokat tágabb témákba vagy fogalmakba kategorizáltam. Ez a lépés magában foglalja az adatokon belüli hasonlóságok és különbségek azonosítását [271, 272]. Az ATLAS.ti egy kvalitatív adatelemző szoftver, amely vizuális, térbeli és összekapcsolt működési módot kínál, így különösen alkalmas több minta, longitudinális adatok elemzéséhez és több fős kutatóicsoportok számára összetett kutatási projektekhez is [266]. Az ATLAS.ti lehetővé tette, hogy a nagy mennyiségű kvalitatív adattal dolgozzak, beleértve az interjú-átiratokat, és megkönnyíti a kódolási és értelmezési

folyamatokat [271, 273], továbbá lehetőség van a szövegszegmensek kategóriákhoz rendelésére, mind deduktív, mind induktív módon, és támogatja az adatokon belüli hasonlóságok, különbségek és minták felfedezését [271].

A kódolási folyamat három lépésből áll: nyílt, axiális és szelektív kódolás.

- A nyílt kódolás során azonosíthatók és megnevezhetők a rögzített szövegben lévő fogalmak. Ez magában foglalja a nagymennyiségű szöveg részletes vizsgálatát, összehasonlítását és kategorizálását, azaz kódok hozhatók létre minden egyes szövegrészletből. Itt nyitottnak kell lenni minden lehetséges értelmezésre a kulcsfogalmak és kategóriák azonosításához [267, 274].
- Az axiális kódolás során kapcsolatokat kerestem a nyílt kódolás során azonosított kategóriák között. Ez magában foglalja a kategóriák és alkategóriák közötti összefüggések feltárását, valamint a jelenség kontextusának és feltételeinek meghatározását [268, 275]. Az axiális kódolás a mélyebb megértést segíti.
- A szelektív kódolás a folyamat utolsó szakasza, amelyben kiválasztottamm a központi kategóriát, és szisztematikusan összekapcsoltam azt a többi kategóriával. Ez a lépés magában foglalja a kategóriák integrálását és finomítását egy koherens elmélet vagy magyarázó modell kialakítása érdekében [276, 277]. Egyes kutatók alternatív megközelítéseket javasolnak a hagyományos GT eljárásokhoz képest. Például, néhányan abduktív változatot alkalmaznak [268], mások meta-elméleti kereteket fejlesztenek ki a szimbolikus interakcionista perspektíva és a strukturációs elmélet szintézisével [275, 277].

A lefolytatott félig strukturált interjúk esetében, mint minden kvalitatív kutatási projekt esetében, a kódolást megelőzően jelentős mennyiségű munkát jelentett az összegyűjtött interjúadatok „megtisztítása”. Az összes interjúfelvételt átírtam, majd az átiratokat meghallgattam és alaposan elolvastam a pontatlanságok azonosítása érdekében. A kvalitatív elemzés során az alábbi fázisokat hoztam létre, melyek a kódok kialakulásának folyamatát szemléltetik (9. ábra)

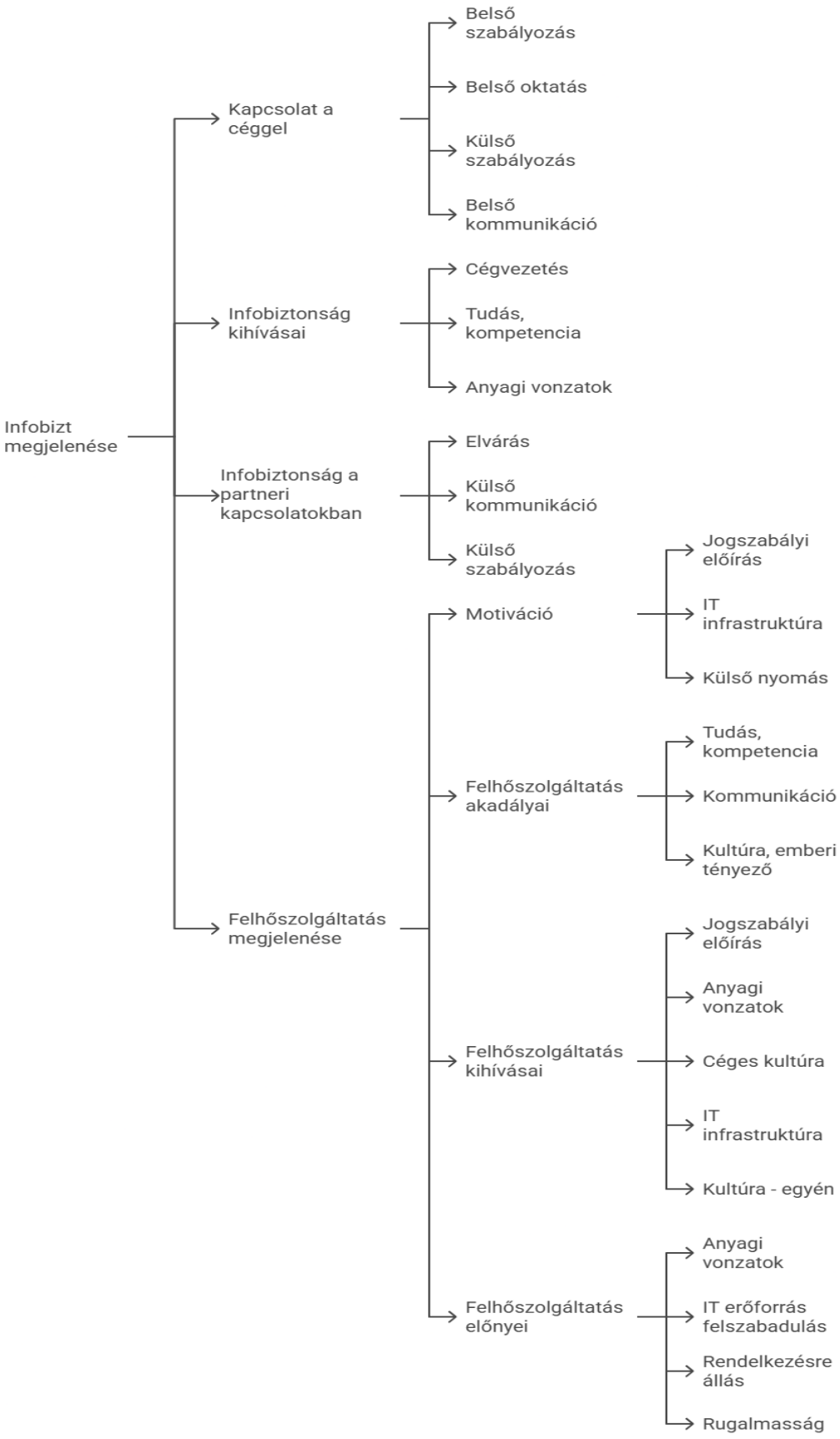


9. ábra A nyers interjúadatok kódolása (saját szerkesztés)

A felvázolt fázisok részletesen kifejtve az alábbi módon írható le.

1. Adatok megismerése - az interjúk átiratát elolvastam és újra olvastam, megjegyezve a kezdeti ötleteket. Az interjú-átiratokat ezután importáltam az ATLAS.ti adatkezelő szoftverbe.
2. Kezdeti kódok létrehozása a szakirodalom alapján- ez a szakasz, a leíró kódolás, az adatok dekonstrukcióját jelentette a kezdeti kronológiából. Az induktív folyamat eredményeként 94 hierarchikus kódot azonosítottam az interjúk adataiból, 654 szövegrészlettel.
3. Témák keresése - ez a fázis a nyílt kódolás felülvizsgálatát, a kezdeti kódok összevonását, átnevezését, szétválasztását és tágabb kódkategóriákba való összevonását foglalta magában. Ez lehetővé tette az adatok olyan módon történő felépítését, amely lehetővé tette a kutatás célkitűzéseinek teljesítését. A 3. fázis eredményeként 3 empirikus téma született az információbiztonsághoz kapcsolódóan és 6 a felhőszolgáltatáshoz kapcsolódóan.
4. A kódok ellenőrzése, felülvizsgálata - a „lefelé fúrás" folyamatát végeztem el, beleértve a szöveg újrakódolását a kezdeti kódok újra alkotásával, a kódolási keretbe való átszervezést, és a témák alkódokra bontását a bennük rejlő jelentések jobb megértése érdekében.
5. Kódcsoportok létrehozása, elnevezése - ez az adatok absztrakcióját jelentette egy szélesebb tematikus keretbe. Induktív eljárás alkalmazásával az adatokat az 1. kutatási célkitűzés négy összetevője, nevezetesen a felhőszolgáltatás motivációja, kihívása, előnye, elvárása és akadálya és az információbiztonsági kérdések vonatkozásában kódoltam.
6. A kódok véglegesítése - az utolsó fázisban az egyes témák tartalmának pontos összefoglalása és az empirikus megállapítások javaslása történt. A videófelvételek segítettek abban, hogy az eredményekről írásos értelmezést készítsek, kiegészítve saját megjegyzéseimmel és az interjúkból származó visszaemlékezésekkel.

Az összevetés eredményét szemléltető kódstruktúrát a 10. ábra mutatja be. A kódolási folyamat során 61 kódot véglegesítettem.



10. ábra A felhőszolgáltatást igénybevételét és használatát befolyásoló tényezők, a GT elemzés kódfája (saját szerkesztés)

A bemutatott kódfa átfogó keretrendszert mutat be az információbiztonság (Infobizt) és a felhőszolgáltatás szervezeti kontextusban való megjelenésének és következményeinek megértéséhez. Ez a hierarchikus struktúra feltárja az információkezelés különböző aspektusai, a vállalati kultúra és a technológiai átvétel közötti bonyolult kapcsolatokat. A legmagasabb szinten a fa két fő ágra ágazik szét: az információbiztonság megjelenése (Infobizt megjelenése) és a felhőszolgáltatás megjelenése. Ez a felosztás azt sugallja, hogy kettős hangsúlyt kell helyezni a belső biztonsági intézkedésekre és a külső szolgáltatások elfogadására, amelyek mindkettő kritikus fontosságú a modern üzleti környezetekben. Az információbiztonsági ág további három fő területre tagolódik: a vállalattal való kapcsolat (Kapcsolat a céggel), az információbiztonsági kihívások (Infobiztonság kihívásai) és az információbiztonság a partnerkapcsolatokban (Infobiztonság a partneri kapcsolatokban). Ez a hármas felosztás hangsúlyozza az információbiztonság sokrétű jellegét, amely magában foglalja a belső folyamatokat, a külső kihívásokat és a szervezetek közötti dinamikát. A vállalattal való kapcsolat alatt találjuk a belső szabályozást, a belső oktatást (Belső oktatás), a külső szabályozást és a belső kommunikációt. Ez az információbiztonság holisztikus megközelítését sugallja, amely egyensúlyt teremt a belső irányelvek és a képzés, a külső megfelelés és a hatékony kommunikációs stratégiák között. Az információbiztonsági kihívások ága a vezetés (Cégvezetés), a tudás és kompetencia (Tudás, kompetencia), valamint a pénzügyi ösztönzők (Anyagi vonzatok) fontosságát emeli ki. Ez a hármas alátámasztja, hogy a biztonsági problémák kezeléséhez felülről lefelé irányuló támogatásra, képzett személyzetre és megfelelő erőforrásokra van szükség. A partnerkapcsolatok ág az elvárásokat (Elvárás), a külső kommunikációt (Külső kommunikáció) és a külső szabályozást (Külső szabályozás) emeli ki, amely tovább bomlik jogi követelményekre (Jogszabályi előírás) és informatikai infrastruktúrára. Ez a struktúra rávilágít az egyértelmű elvárások, a hatékony kommunikáció és a jogi és technológiai előírások betartásának fontosságára a biztonságos partnerségek fenntartásában. A felhőszolgáltatások ága bővebb, részletezve a felhő bevezetésének motivációit (Motiváció), akadályait (Felhőszolgáltatás akadályai), kihívásait (Felhőszolgáltatás kihívásai) és előnyeit (Felhőszolgáltatás előnyei). Ez az átfogó megközelítés kiegyensúlyozott képet nyújt a felhőszolgáltatásokról, elismerve mind a potenciális előnyöket, mind pedig az akadályokat, amelyekkel a szervezetek a bevezetés során szembesülhetnek. A felhőhasználat motivációja a digitális infrastruktúrához és a külső nyomáshoz (Külső nyomás) kapcsolódik, ami arra utal, hogy a technológiai igények és a

piaci erők egyaránt a felhőhasználat mozgatórugói. A felhőszolgáltatások akadályai sokrétűek, beleértve a tudás- és kompetenciaproblémákat, a kommunikációs kihívásokat, valamint a kulturális és emberi tényezőket. A felhőszolgáltatások kihívásai magukban foglalják a jogi követelményeket, a pénzügyi megfontolásokat, a vállalati kultúrát, az IT-infrastruktúrát és egyéb kulturális tényezőket. A kihívások e sokrétű halmaza kiemeli a felhő bevezetésének összetettségét, és azt, hogy az akadályok leküzdéséhez multidiszciplináris megközelítésre van szükség. Végül a felhőszolgáltatások előnyei következnek, beleértve a pénzügyi előnyöket, az informatikai erőforrások felszabadítását, a rendelkezésre állást és a rugalmasságot. A fa szerkezetének pozitív lezárása azt sugallja, hogy a kihívások ellenére a felhőszolgáltatások jelentős előnyöket kínálnak, amelyek növelhetik a szervezeti hatékonyságot és versenyképességet.

4. 2. 2. Kódgyakoriság elemzés

A kódok gyakoriságának elemzése, előfordulásuk vizsgálata betekintést nyújt a kkv-k felhőszolgáltatásokkal kapcsolatos legelterjedtebb aggályaiba. Ez a módszer lehetővé teszi az interjúválaszokban közös minták és tendenciák azonosítását, kiemelve a felhőhasználatát befolyásoló kulcsfontosságú tényezőket. A kódgyakoriság-elemzés a kutatási kérdéseken alapuló kezdeti kódolási séma kidolgozásával kezdődik. Ez magában foglalja a kutatási kérdések és célkitűzések áttekintését, a tanulmány szempontjából releváns kulcsfogalmak és témák azonosítását, az ezeket a fogalmakat megragadó kódok előzetes listájának összeállítását, valamint az egyes kódok egyértelmű meghatározását a következetes alkalmazás biztosítása érdekében. A következő lépés az interjúk átiratainak kódolása az egyes átiratok gondos átolvasásával, a releváns kódok hozzárendelésével a szöveg egyes szegmenseihez, a kódok alkalmazásának következetességének fenntartásával az összes átiratban, valamint a kódolási séma felülvizsgálatával és finomításával, amennyiben a folyamat során szükséges. A kódolás után megszámoltam, hányszor fordulnak elő az egyes kódok az összes átiratban és kódgyakoriság táblázat készítettem a kódok eloszlásának szemléltetésére. A leggyakoribb témát és fogalmat ezután a kódok gyakorisága alapján történő rangsorolásával, a nagy gyakoriságú kódok közötti minták és kapcsolatok elemzésével, a kapcsolódó kódok tágabb témákba vagy kategóriákba való csoportosításával, valamint a legfontosabb megállapítások összegzésével azonosítottam a leggyakoribb témák alapján.

4. 2. 3. Kontextuselemzés - kódhálózat

A kontextuselemzés az interjúadatok árnyalatainak mélyebb megismerésére szolgál, megvizsgálva azokat a konkrét körülményeket és környezeteket, amelyekben a felhőt a kkv-kon belül alkalmazzák. A kontextuselemzés magában foglalja a kódolt szegmensek eredeti kontextusukban történő felülvizsgálatát az eredeti átiratokhoz való visszatéréssel, az egyes kódolt szegmenseket körülvevő teljes szöveg vizsgálatával, valamint az interjú és a résztvevő tágabb kontextusának figyelembevételével. A kódok és a környező szöveg közötti kapcsolatokat úgy azonosítottam, hogy kapcsolatot kerestem a különböző kódok között ugyanazon a kontextuson belül, elemeztem, hogy a kódolt szegmensek hogyan kapcsolódnak a szöveg kódolatlan részeihez, és azonosítottam a kontextuális információkban található mintákat vagy ellentmondásokat. Ez a megközelítés lehetővé teszi a felhőhasználati stratégiákat alakító kontextuális tényezők és az üzleti tevékenységekre gyakorolt hatásuk átfogóbb megértését. Az elemzés után arra összpontosítottam, hogy a kontextus hogyan befolyásolja a kódolt szegmensek jelentését annak értékelésével, hogy a környező szöveg hogyan befolyásolja a kódok értelmezését, figyelembe véve, hogy a résztvevők jellemzői vagy az interjú beállításai hogyan befolyásolják a jelentést, és azonosítva minden olyan árnyalatot vagy apróságot, amely nem volt nyilvánvaló a kezdeti kódolás során. Ez a témák árnyaltabb értelmezésének kialakításához vezet a témák kezdeti értelmezéseinek a kontextuális meglátásokon alapuló finomításával, a tágabb kategóriákon belüli altémák vagy variációk azonosításával, az egyes témák összetettségének átfogóbb megértésével, valamint a témák kontextuális gazdagságát szemléltető példák dokumentálásával. A kontextuselemzés alkalmazása során fontos a rugalmasság és az iteratív megközelítés. Az elemzés során felmerülő új információk és felismerések alapján szükség lehet a korábbi lépések felülvizsgálatára és finomítására. A módszertan következetes alkalmazása lehetővé teszi a vizsgált jelenség mélyebb megértését és a tágabb összefüggések feltárását.

A GT módszertanra alapozott félig strukturált interjúk ATLAS.ti szoftverrel történő kódhálózatlétrehozás hatékony módszer az összefüggések feltárására és elméletalkotásra[266]. A módszer lényege, hogy az interjúk szövegét kódoljuk, majd a kódok közötti kapcsolatokat vizuálisan ábrázoljuk és elemezzük. Az ATLAS.ti lehetővé teszi a kódok hálózatszerű megjelenítését, ami segíti az összefüggések feltárását és az elméletalkotást. A szoftver támogatja a folyamatos összehasonlítás módszerét, ami a GT

kulcseleme [278]. Az előnye, hogy vizuálisan megjeleníti a fogalmak közötti komplex kapcsolatokat, ami segíti az absztrakt elméleti sémák kialakítását [279]. Emellett lehetővé teszi a nagy mennyiségű kvalitatív adat szisztematikus elemzését, ami növeli az eredmények megbízhatóságát [263]. A főbb lépések: 1) interjúk kódolása, 2) kódok közötti kapcsolatok azonosítása, 3) hálózati ábra készítése, 4) a hálózat elemzése és értelmezése, 5) elméletalkotás. Ez a folyamat iteratív, az új adatok fényében folyamatosan finomítjuk a kódokat és a hálózatot, amíg el nem érjük az elméleti telítődést [263, 278].

4. 2. 4. Szentiment elemzés

A szentiment elemzés folyamata a következő lépésekből áll: 1. Előkészítés: Az interjúk átiratainak alapos áttekintése, a kontextus megértése. 2. Skála meghatározása: Egy háromfokozatú skála kialakítása (negatív, semleges, pozitív) az érzelmek kategorizálására. 3. Szegmentálás: Az interjúk releváns részeinek azonosítása és elkülönítése elemzésre. 4. Érzelmi töltet azonosítása: Minden szegmens érzelmi töltetének meghatározása a skála alapján, figyelembe véve a szóhasználatot, hangsúlyokat és kontextust. 5. Indoklás: Minden értékeléshez rövid indoklás készítése, kiemelve a döntést befolyásoló kulcselemeket. 6. Ellenőrzés: Az értékelések felülvizsgálata és szükség esetén finomítása a konzisztencia biztosítása érdekében. 7. Összesítés: Az eredmények összegzése, trendek és mintázatok azonosítása. 8. Értelmezés: Az eredmények összevetése a kutatás egyéb aspektusaival, következtetések levonása.

A szentiment elemzés vagy magyarul az érzelmi állapotok elemzése a kvalitatív kutatásban a vélemények, attitűdök szöveges adatokból történő kinyerésének és elemzésének módszere. A szentiment elemzés során dokumentumok, weboldalak, blogok vagy vitafórumok vizsgálata történik annak érdekében, hogy az egyének által kifejezett érzelmi mintákat azonosítani lehessen [280]. Az elemzés a szövegek három elsődleges érzelmi (hangnem) kategóriába sorolására összpontosít: pozitív, negatív és semleges [281]. Ez a technika különösen hasznos nagy mennyiségű strukturálatlan adat, például közösségi médiatartalmak, személyes blogok és online vélemények, interjúk elemzésére [282].

A szentiment elemzés különböző részletességű szinteken végezhető, amelyek mindegyike más-más betekintést nyújt a kifejezett véleményekbe. A különböző szintek az alábbiak lehetnek:

- Dokumentumszint: Ez a hangulatelemzés legszélesebb szintje, ahol egy teljes dokumentum általános hangulatát határozzuk meg [283]. Általában vélemények véleményének osztályozására használják, célja a teljes szöveg hangulatának pozitív, negatív vagy semleges kategóriába sorolása [284].
- Mondatszint: Ezen a szinten a dokumentumon belül az egyes mondatok hangulatát elemzik [283, 285]. Ez a megközelítés árnyaltabb képet ad a szöveg egészén belüli hangulatingadozásokról.
- Aspektusszint: Az entitásszintként is ismert elemzés ezen formája az entitás konkrét aspektusaihoz vagy jellemzőihez kapcsolódó hangnem azonosítására összpontosít [285, 286]. Finomabb szemcseméretű elemzést tesz lehetővé, megragadva a termék vagy szolgáltatás egyes jellemzőivel kapcsolatos véleményeket.
- Fogalmi szint: Ez az aspektusszintű elemzés fejlettebb formája, ahol az aspektusok többfogalmi fogalmak lehetnek [287]. Célja a szövegen belüli összetettebb vagy absztraktabb gondolatokhoz kapcsolódó érzések, a hangnem felderítése.

A megfelelő szint kiválasztása az adott feladat sajátos követelményeitől függ. Míg a dokumentumszintű elemzés széleskörű áttekintést nyújt, addig az olyan részletesebb megközelítések, mint az aspektus- vagy fogalomszintű elemzés mélyebb betekintést nyújtanak a szövegben kifejezett konkrét véleményekbe, a szövegrészletek hangnemébe. A szentiment elemzés többszintű megközelítése lehetővé tette, hogy különböző részletességű, értékes információkat nyerjek ki.

Jelen kutatásom során a mondatszintű szentiment elemzést használtam, melynek célja egy adott mondat általános hangnemének, érzelmi polaritásának meghatározása. Ez a megközelítés inkább az egyes mondatok elemzésére összpontosít, nem pedig teljes dokumentumok vagy a mondatokon belüli konkrét szempontok elemzésére.

A folyamat jellemzően az alábbi főbb lépésekből áll:

1. A mondatok osztályozása: A mondatokat először különböző típusokba soroljuk összetettségük vagy a bennük található érzelmi célpontok száma alapján [288]. A mondatok három típusba sorolhatók (semleges, negatív, pozitív).

2. Jellemzők kinyerése: Különböző technikákat alkalmazunk a releváns jellemzők kinyerésére a mondatból. Ezek lehetnek szóbeágyazások, szintaktikai struktúrák vagy pozícióinformációk [289].
3. Érzelmek osztályozása: A kinyert jellemzőket ezután egy osztályozási modellbe tápláljuk a szentiment polaritás meghatározásához. Erre a célra különböző modellek is használhatók.
4. Figyelemmechanizmusok: Számos megközelítés tartalmaz figyelemmechanizmusokat, hogy a mondat érzelemelemelemzés szempontjából legrelevánsabb részére összpontosítson [290].

Az alábbiakban bemutatásra kerül egy példa a mondatszintű szentimentelemzés működésére:

Tekintsük a mondatot: „A felhőszolgáltatás olcsó, de a működtetése költséges is lehet”. A mondatszintű szentiment elemzés folyamatát a 11. ábra mutatja be.

11. ábra Mondat szintű szentiment elemzés folyamata (saját szerkesztés)

Az ábrán bemutatott folyamat lépései a mintamondaton szemléltetve a következő módon alakul:

1. Érzelmi aspektusok azonosítása. A mondat többféle érzelmi célpontot (felhőszolgáltatás és működtetés) tartalmazónak minősül.
2. Kivonásra kerülnek a jellemzők, beleértve a szóbeágyazásokat és a „felhőszolgáltatás” és a „működtetés” helyzeti információit.
3. A figyelemmechanizmus során a „felhőszolgáltatás” esetében az „olcsó”, a „működtetés” esetében pedig a „költséges” kifejezés összpontosítunk.
4. Az osztályozási modell ezután meghatározza az általános hangulatot, valószínűleg vegyes vagy semleges hangulatot állapítható meg az felhőszolgáltatás pozitív aspektusa és a működtetés negatív aspektusa miatt.

5. Eredmények bemutatása

Az interjúk rávilágítottak arra, hogy az információbiztonság és a felhőhasználat közötti kapcsolat összetett és dinamikus. A belső folyamatok, a vezetési tényezők és a szervezeti kultúra jelentősen befolyásolják az információbiztonságot. A felhőhasználat fő vonzereje a rugalmasság, azonban ennek kihasználását gyakran akadályozzák olyan tényezők, mint a szükséges tudás és szakértelem hiánya, valamint a kapcsolódó költségek. A vezetőség döntései kulcsfontosságúak mind az információbiztonság, mind a felhőhasználat terén, mivel ezek határozzák meg a belső szabályozást és kommunikációt, amelyek az információbiztonság alapjait képezik.

C1: A kutatás célja feltárni, hogy a kis- és középvállalkozások (kkv-k) milyen gazdasági, technológiai, szervezeti, kulturális és bizalmi tényezőket vesznek figyelembe a felhőszolgáltatások igénybevétele során, és ezek hogyan hatnak a döntéshozatali folyamatokra.

C2: A cél annak vizsgálata, hogy milyen értelmezési keretek és prioritások mentén jelenik meg az információbiztonság a kkv-k és a felhőszolgáltatók körében, különös tekintettel a kihívásokra, érintettekre és szervezeti megközelítésekre.

C2a: A kutatás célja annak feltérképezése, hogy a felhőszolgáltatók és a kkv-k miként értelmezik a felhőtechnológiát, milyen akadályokat és előnyöket látnak benne, milyen kihívásokkal szembesülnek, és milyen belső vagy külső motivációk befolyásolják a bevezetését és használatát.

C2b: A cél az, hogy azonosítsam és feltérképezzem azokat a strukturális és tematikus kapcsolatokat, amelyek az információbiztonság különböző aspektusai (pl. szervezeti működés, tudás, attitűd, szabályozás) között fennállnak a kkv-kon belül, kvalitatív kódhálózat alapján.

C3: A kutatás célja feltárni, hogy milyen viszonyrendszerek és kapcsolati hálók rajzolódnak ki a felhőtechnológia bevezetését és használatát befolyásoló különböző tényezők között, a kvalitatív adatelemzés során létrejött kódok hálózati összefüggései alapján.

C4: A cél az interjúalanyok felhőszolgáltatásokkal kapcsolatos érzelmi viszonyulásainak feltérképezése, különös figyelemmel az ambivalens attitűdökre, félelmek és motivációk együttes jelenlétére, valamint ezek kapcsolatára a döntési és bevezetési folyamatokkal.

5. 1. Döntési tényezők

C1: A kutatásom célja az volt, hogy feltárjam, hogy a kis- és középvállalkozások (kkv-k) milyen gazdasági, technológiai, szervezeti, kulturális és bizalmi tényezőket vesznek figyelembe a felhőszolgáltatások igénybevétele során, és ezek hogyan hatnak a döntéshozatali folyamatokra.

5. 1. 1. A kódolási folyamat eredményei

A 5. táblázat a kódolási folyamat strukturált bontását mutatja be, illusztrálva a nyílt kódolástól, ahol a kezdeti fogalmakat azonosítottam és címkéztem, az axiális kódolásig, amely a kategóriák közötti kapcsolatokat állapítja meg, és végül a szelektív kódolásig, ahol a központi témák integrálódnak, hogy összefüggő elméleti keretet alkossanak.

Iniciális nyitott kód – szövegrészlet (forrás)	**Nyílt kód**	**Axiális kód**	**Szelektív kód**
„nincs saját IT”, „külsős rendszergazda”, „beugrós ember”	Nincs dedikált IT	IT működés kiszervezése	IT üzemeltetés
„nincs fixen saját IT emberük… külsősként van megbízva erre”	Beugrós rendszergazda	IT működés kiszervezése, igénybe vett szolgáltatás	
Jelszóhasználat és kulcskezelés problémái	Véletlen megosztás, jogosultságok elfelejtése,	belső szabályozás	Információbiztonság kihívásai
„áh, úgysem lesz baj”, "tudatosságra kell nevelni..."	szakértelem hiánya, rossz döntések a kockázatok mérlegelésében	belső oktatás, tudás, kompetencia	
„nincs mentés”, „nem látták a kockázatokat”, "nincs tervezett IT-büdzsé"	csak működjön	cégvezetés, elvárás	

„nem voltak tisztában, mekkora költsége lenne, ha elvesztik” *"bizalmatlanok vagyunk a felhővel..."*	Vezetői IT-ismeret hiánya	cégvezetés	
„nehéz volt átverni, hogy álljunk át felhőre”	IT és felhő iránti ellenállás	céges kultúra, kommunikáció	Felhő kihívásai
„legolcsóbb router”, *„kalóz szoftver”,* *„felhő drágább x%-kal”*	Kalóz szoftverhasználat	céges kultúra, anyagi vonzatok	

5. táblázat Kódolás folyamata - részlet (saját szerkesztés interjúk alapján)

Az interjúk rávilágítanak arra, hogy a felhő technológiák értékelésénél nem elegendő kizárólag a gazdasági mutatókat figyelembe venni, hanem olyan kevésbé kézzelfogható, puha tényezőket is mérlegelni szükséges. A kkv-k ragaszkodnak a fizikai tulajdonhoz és a helyben telepített megoldásokhoz, mivel ezek biztosítják számukra a kézzelfogható kontroll érzetét. Ez a megközelítés azonban gátolhatja a technológiai fejlődést és a felhőmegoldások elfogadását. Szemléletváltásra van szükség annak érdekében, hogy a kkv-k felismerjék: a szolgáltatók által kínált infrastruktúra nem csupán biztonságosabb, de a skálázhatóság és költséghatékonyság révén hosszú távú versenyelőnyt is biztosíthat. A technológiai átállás során a tanácsadók kulcsfontosságú szerepet töltenek be, elősegítve az akadályok lebontását, az új technológiák megfelelő értelmezését és a vállalat-specifikus megoldások kialakítását.

5. 1. 2. A felhő bevezetését befolyásoló tényezők

A felhőszolgáltatások havi díjas modellje lehetővé teszi a kkv-k számára, hogy elkerüljék a jelentős kezdeti beruházásokat. Ahelyett, hogy drága szervereket kellene vásárolniuk, a vállalkozások előfizethetnek felhőalapú megoldásokra, amelyek havi díjfizetéssel működnek. Ez különösen előnyös lehet a levelezőrendszerek esetében, ahogy azt a D6 jelű interjúalany is megjegyezte:

„A felhőben lévő levelezés előnyös, mert nem igényel nagy kezdeti befektetést, és havi díjban tervezhető.” (D6).

A felhő egyik kulcsfontosságú előnye a rugalmas skálázhatóság. Ez azt jelenti, hogy a vállalatok könnyen növelhetik vagy csökkenthetik az igénybe vett erőforrásokat a pillanatnyi szükségleteiknek megfelelően. Ez a rugalmasság költséghatékony megoldást

kínál, különösen a növekvő vállalkozások számára, amelyeknek változó igényeik lehetnek.

„A felhőszolgáltatások gyorsan alkalmazhatók az üzleti környezetben, a skálázhatóság előnyös…" (D3).

Ezek az előnyök összhangban vannak a felhőszolgáltatások általános értékajánlatával, amely a rugalmasságot, a költséghatékonyságot és a skálázhatóságot helyezi előtérbe, különösen a kkv-k számára, akiknek korlátozott erőforrásaik lehetnek a digitális infrastruktúra kiépítésére és fenntartására.

A felhőszolgáltatások gyakran havi díjas modellt alkalmaznak. Ennek előnye a kiszámíthatóság, mivel a vállalkozások rendszeres, előre tervezhető költségekkel számolhatnak. Azonban hosszú távon ez a modell összességében drágább lehet, mint az egyszeri nagy beruházások. Az interjúalanyok tapasztalata szerint sokan nehezen fogadják el ezt a folyamatos költséget, szemben az egyszeri licencvásárlással, amely véglegesnek tűnhet (D6).

„Sokan nehezen fogadják el, hogy a havi díjas szolgáltatás folyamatos költség, míg az egyszeri licenc vásárlás véglegesnek tűnik." (D6).

A felhőbe való átállás során gyakran felmerülnek további költségek. Az interjúkban szereplő cégek tapasztalatai szerint a meglévő helyi rendszerek és a felhőszolgáltatások közötti átmenet időigényes és költséges lehet. Ez magában foglalja a meglévő rendszerek átalakítását, hogy kompatibilisek legyenek a felhőalapú megoldásokkal (D22).

„A meglévő rendszerek átalakítása, hogy a felhőbe költözhessünk, további ráfordítást igényel." (D22).

A kkv-k gyakran szembesülnek szűkös költségvetéssel. Ez korlátozhatja a felhőalapú megoldásokhoz való hozzáférésüket, mivel nem mindig engedhetik meg maguknak ezeket a szolgáltatásokat. Az egyes interjúkban elhangzottak, többek között a kiemelt részlet arra utal, hogy a magyar kkv-k különösen érintettek ebben a kérdésben.

„A magyar KKV-k nem engedhetik meg maguknak a teljes biztonságot, mert túl drága…" (D7).

Ezek a pontok rávilágítanak arra, hogy bár a felhőszolgáltatások előnnyel járhatnak, a vállalkozásoknak, különösen a kkv-knak, gondosan mérlegelniük kell a költségeket és a potenciális kihívásokat a felhő bevezetése előtt.

- ***Reaktív döntéshozatal*:** A döntéseket a múltbeli tapasztalatok, veszteségek vagy külső nyomás (például auditok vagy incidensek) befolyásolják a proaktív stratégiai tervezés helyett. Ez a reaktív megközelítés olyan döntésekhez vezethet, amelyek nem igazodnak a hosszú távú szervezeti célokhoz. Ez rámutat egy olyan átfogó stratégia kidolgozásának fontosságára, amely ellenáll a jövőbeli változásoknak.

- ***Szaktudásbeli hiányosságok***: A felhőtechnológiák gyors fejlődése gyakran meghaladja a házon belüli szakértelem fejlődését. A szervezeteknek szembe kell nézniük azzal a kihívással, hogy vagy a meglévő személyzetet képezzék tovább, vagy a munkaerőpiacon versenyezzenek a szűkös felhőszakértőkért, ami mindkettő hatással lehet a felhőtechnológiák alkalmazásának kezdeményezésére és sikerére.

- ***Biztonsági költségmegfontolások*:** A döntéshozók gyakran az azonnali költségmegtakarítást helyezik előtérbe a hosszú távú biztonsági beruházásokkal szemben. Ez a rövid távú fókuszálás kiszolgáltatottá teheti a szervezeteket a kiberfenyegetéseknek és az adatok megsértésének. A robosztus biztonsági intézkedések és a költségvetési korlátok közötti egyensúlyozás jelentős kihívást jelent a felhőtechnológiák alkalmazását támogató stratégiákban.

- ***A fokozatosság paradoxona*:** Míg a fokozatos megközelítés a végrehajtásban óvatosabbnak tűnhet, potenciálisan párhuzamos, szervezetlen rendszereket hoz létre. A szervezetek dilemmával szembesülnek az óvatos, lépésről lépésre történő bevezetés és a széttagolt, nem hatékony infrastruktúrák létrehozásának kockázata között. Ez a paradoxon rávilágít a gondos tervezés és koordináció szükségességére a zökkenőmentes átmenet biztosítása érdekében, anélkül, hogy az általános rendszer integritása sérülne.

- ***Bizalomhiány*:** A technikai aggályok gyakran elhomályosítják a mögöttes pszichológiai és szervezeti kérdéseket, ami az elfogadás elsődleges akadálya. A technológiai szempontokon túl a felhő bevezetése gyakran a mélyen gyökerező szervezeti kultúra, a változástól való félelem és a munkahelyi biztonsággal

kapcsolatos aggodalmak miatt ütközik ellenállásba. Ezeknek a pszichológiai akadályoknak a kezelése kulcsfontosságú a sikeres felhőtechnológiák használatához.

Tézis 1: ***A kkv vezetőivel folytatott interjúk szövegelemzése során azonosítottam a felhőszolgáltatás bevezetésének releváns akadályait, melyek felismerése hozzájárul a felhőszolgáltatás bevezetés hatékony leküzdéséhez*** [14, 83, 291-293].

5. 2. Felhőhasználati attitűdök feltérképezése

C2: A cél annak vizsgálata, hogy milyen értelmezési keretek és prioritások mentén jelenik meg az információbiztonság a kkv-k és a felhőszolgáltatók körében, különös tekintettel a kihívásokra, érintettekre és szervezeti megközelítésekre.

C2a: A kutatás célja annak feltérképezése, hogy a felhőszolgáltatók és a kkv-k miként értelmezik a felhőtechnológiát, milyen akadályokat és előnyöket látnak benne, milyen kihívásokkal szembesülnek, és milyen belső vagy külső motivációk befolyásolják a bevezetését és használatát.

C2b: A cél az, hogy azonosítsam és feltérképezzem azokat a strukturális és tematikus kapcsolatokat, amelyek az információbiztonság különböző aspektusai (pl. szervezeti működés, tudás, attitűd, szabályozás) között fennállnak a kkv-kon belül, kvalitatív kódhálózat alapján.

5. 2. 1. A kódgyakoriság elemzés eredményei

A kódgyakoriság elemzéssel azonosíthatók a szövegrészletekben fellelhető minták. A konkrét kifejezések vagy témák előfordulásának számszerűsítésével olyan betekintést nyerhetünk, amely a kvalitatív módszerekkel önmagában nem feltétlenül nyilvánvaló. A kódgyakoriság elemzés legfontosabb előnye a kvalitatív kutatásban, hogy lehetővé teszi a visszatérő témák, kifejezések azonosítását, és ezáltal a kulcsfontosságú elemeik felismerését [294], továbbá a gyakoriság elemzés alkalmazása javíthatja az adatok megértését [295]. A kódgyakoriság elemzés feltárhatja olyan témák gyakoriságát, amelyeket aztán kvalitatív módon mélyebben fel lehet tárni, mindemellett objektív mérőszámot biztosít, amely alátámaszthatja a kvalitatív megállapításokat, kvantitatív dimenziót kínálva a kvalitatív kutatásnak, amely érvényesítheti vagy megkérdőjelezheti a kezdeti értelmezéseket [294, 296].

A kódgyakoriság elemzéssel az információbiztonság és a felhő használat kódokhoz kapcsolódó szövegrészleteket vizsgáltam. Az interjúkhoz kapcsolódó kódgyakoriságokat és a kódokat a 12. ábra tartalmazza.

Name	Grounded	Density	Groups
ib szervezet:belso szabalyozas	71	6	[IB COMPANY]
ib kihivas:cégvezetés	61	5	[IB KIHIVAS]
felho akadaly:tudás, kompetencia	61	4	[FELHO AKADALY]
felho kihivas:szakértelem, kompetencia	59	5	[FELHO KIHIVAS]
felho kihivas:ráfordítás	51	6	[FELHO KIHIVAS]
ib velemeny:pozitív	46	3	[IB VELEMENY]
ib kihivas:tapasztalat, tudás	42	6	[IB KIHIVAS]
ib szervezet:belso kommunikacio	41	2	[IB COMPANY]
felho elony:rugalmasság - skálázhatóság	40	3	[FELHO ELONY]
felho elvaras:biztonsági elvárások	39	1	[FELHO ELVARAS]
ib kihivas:ráfordítás	38	1	[IB KIHIVAS]
felho elony:anyagi vonzatok	37	4	[FELHO ELONY]
felho - ib:van kapcsolat	35	0	[FELHO - IB]
felho kihivas:IT infrastruktúra - IT osztály	34	3	[FELHO KIHIVAS]
felho elony:IT erőforrás felszabadulás	33	3	[FELHO ELONY]
felhős sw	30	0	[FELHO MEGJELENES]
ib incidens	29	1	[FELHO - IB] [IB MEGJELENES]
ib szervezet:belso oktatas	29	1	[IB COMPANY]
felho velemeny:pozitív	28	1	[FELHO VELEMENY]
ib kihivas:IT	28	3	[IB KIHIVAS]

12. ábra Az interjúk kódolásából származó top 20 kód (saját szerkesztés)

Az ábra a kkv-k információbiztonságával és felhőszolgáltatások használatával kapcsolatos interjúk során azonosított leggyakoribb témát mutatja be a 20 leggyakoribb kód formájában. A táblázat első oszlopában a kódok elnevezése szerepel, a másodikban pedig az adott kód gyakorisága. Az alábbiakban ezeket magyarázom:

1. Információbiztonság és belső szabályozás (71 említés): Ez a leggyakrabban említett téma, ami arra utal, hogy a megkérdezettek nagy hangsúlyt fektetnek a belső biztonsági protokollokra. Maga a kód együttesen tartalmazza a vonatkozó szabályzatok pozitív és negatív megemlítését is. A kutatások azt mutatják, hogy a hatékony belső szabályozás kulcsfontosságú az információbiztonság fenntartásában.

2. Felhőszolgáltatások és kompetencia hiánya (61 említés): A második leggyakoribb kihívás a felhőszolgáltatásokhoz szükséges tudás és kompetencia hiánya. Ez

összhangban van azzal a globális trenddel, hogy a vállalatok küzdenek a felhő gyors fejlődésével való lépéstartással.

3. Vezetőségi kihívások az információbiztonságban (61 említés): A vezetőség szerepe kritikus az információbiztonsági stratégiák megvalósításában. A gyakori említés arra utal, hogy sok vállalatnál ez kihívást jelent.

4. Felhőszolgáltatások előnyei: A rugalmasság és skálázhatóság (40 említés), valamint az anyagi előnyök (37 említés) a felhőszolgáltatások leggyakrabban említett pozitív aspektusai. Ez összhangban van a szakirodalommal, amely kiemeli ezeket mint a felhőtechnológia fő előnyeit.

5. Információbiztonsági incidensek (29 említés): Az incidensek viszonylag gyakori említése rámutat arra, hogy a vállalatok aktívan foglalkoznak a biztonsági eseményekkel és azok kezelésével. Azonban itt érdemes megjegyezni azt is, hogy az incidensek említése túlnyomó részben a szolgáltatói interjúkban fordult elő és negatív vonatkozásban, mely szerint az incidensek szolgálnak elrettentőerővel, de főként abban az esetben, amikor személyes, céges érintettségű. A médiában olvasható lokális vagy globális incidensek nem váltanak ki semmilyen lépéseket a vállalatokból.

6. Pozitív vélemények: Mind az információbiztonságról (46 említés), mind a felhőszolgáltatásokról (28 említés) elhangzottak pozitív vélemények, és ezek arra utalnak, hogy a vállalatok általában elismerik ezek fontosságát és előnyeit.

7. Belső kommunikáció és tréning: A belső kommunikáció (41 említés) és a tréningek (29 említés) gyakori említése azt jelzi, hogy a kkv-k felismerik az alkalmazottak oktatásának és tájékoztatásának fontosságát és szükségességét az információbiztonság terén. Azonban tényleges képzések ezen a téren elmaradásban vannak.

A 6. táblázat alapján látható, hogy az IT (részleg, infrastruktúra) a felhőszolgáltatók véleménye szerint hatalmas (23) kihívást jelent a cégeknél, komoly akadálya tud lenni a fejlődésnek és akár a (megfelelő) információbiztonság vagy felhőszolgáltatás kialakításának, azonban korántsem akkora gát a fejlődésben, mint a cégvezetés (és a cégeskultúra) (39), akik sokszor nem látják jelentőségét az információbiztonság kialakításának, valamint a példamutatásban sem járnak élen. Ez arra utalhat, hogy a

szolgáltatók jobban érzékelik a vezetői támogatás hiányának hatását a felhőszolgáltatások elterjedésére. A kkv oldal esetében is magas gyakorisággal (22) fordul elő a cégvezetés, mint kardinális tényező. A ráfordítás, mint kihívás tekintetében mind a két oldal hasonlóan vélekedett, azaz a szolgáltatói oldal 22, míg a kkv oldal 16 alkalommal nevesítették a tényezőt, ami azt jelzi, hogy a felhasználók számára a költségek jelentősebb akadályt képeznek. A „tapasztalat, tudás" kategória mindkét oszlopban magas (17 és 25), ami azt mutatja, hogy mind a felhőszolgáltatók, mind a felhasználók szerint kulcsfontosságú tényezőként és hatalmas akadályként látják az IT-fejlesztések és a felhőmegoldások alkalmazásában a hiányos tudást. Ezt támasztja alá az is, hogy a megkérdezett kkv-k nagy hangsúlyt (20) fektetnek a munkavállalók képzésére, belső tréningek tartására.

Különbségként jelenik meg a partnerek vagy más külső érintett felek részéről érkező megkeresések, elvárások megjelenése, illetve a felhőszolgáltatás bevezetését indukáló tényező. A szolgáltatók esetében 13 alkalommal vélekedtek úgy, hogy a kkv-k általában valamelyik külsős partner, piaci szereplő hatására kezdenek el a felhőszolgáltatáson gondolkozni. Ezzel szemben a megkérdezett kkv-k elmondása alapján ez kevésbé van így (6).

Az adatok alapján a felhőhasználók és a szolgáltatók prioritásai és kihívásai bizonyos pontokon átfednek, például a belső szabályozás, tapasztalat és tudás fontosságában. Ugyanakkor a szolgáltatók inkább a vezetői támogatás és partnerek elvárásai felé orientálódnak, míg a felhasználók számára a költségek, belső oktatás és külső kommunikáció kiemelkedőbb kérdések. Ezek a különbségek rávilágítanak arra, hogy a két oldal eltérő fókuszokkal közelíti meg a felhőszolgáltatások alkalmazását és bevezetését.

	Felho_hasznalo_ mind Gr=310; GS=18		**Felho_szolgaltato_ mind Gr=344; GS=16**		**Totals**	
ib kihivas:cégvezetés Gr=61	**22**	36,07%	**39**	63,93%	61	100,00%
	12,16%	5,80%	19,70%	10,29%	16,10%	16,10%
ib kihivas:IT Gr=28	**5**	17,86%	**23**	82,14%	28	100,00%
	2,76%	1,32%	11,62%	6,07%	7,39%	7,39%
ib kihivas:ráfordítás Gr=38	**16**	42,11%	**22**	57,89%	38	100,00%
	8,84%	4,22%	11,11%	5,80%	10,03%	10,03%
ib kihivas:tapasztalat, tudás Gr=42	**17**	40,48%	**25**	59,52%	42	100,00%
	9,39%	4,48%	12,63%	6,60%	11,08%	11,08%

ib stakeholderek:kulso kommunikacio Gr=22	**11**	50,00%	**11**	50,00%	22	100,00%
	6,08%	2,90%	5,56%	2,90%	5,80%	5,80%
ib stakeholderek:kulso szabalyozas Gr=9	**1**	11,11%	**8**	88,89%	9	100,00%
	0,55%	0,26%	4,04%	2,11%	2,37%	2,37%
ib stakeholderek:partneri elvárás Gr=19	**6**	31,58%	**13**	68,42%	19	100,00%
	3,31%	1,58%	6,57%	3,43%	5,01%	5,01%
ib szervezet:belso kommunikacio Gr=41	**26**	63,42%	**15**	36,59%	41	100,00%
	14,36%	6,86%	7,58%	3,96%	10,82%	10,82%
ib szervezet:belso oktatas Gr=29	**20**	68,97%	**9**	31,03%	29	100,00%
	11,05%	5,28%	4,54%	2,37%	7,65%	7,65%
ib szervezet:belso szabalyozas Gr=71	**46**	64,79%	**25**	35,21%	71	100,00%
	25,41%	12,14%	12,63%	6,60%	18,73%	18,73%
ib szervezet:kulso szabalyozas-nyomas Gr=19	**11**	57,89%	**8**	42,11%	19	100,00%
	6,08%	2,90%	4,04%	2,11%	5,01%	5,01%
Totals	**181**	47,76%	**198**	52,24%	379	100,00%
	100,00%	47,76%	100,00%	52,24%	100,00%	100,00%

6. táblázat Az információbiztonsággal kapcsolatos kódok alakulása (saját szerkesztés)

Az interjúk elemzése alapján a következő főbb különbségek és hasonlóságok rajzolódnak ki a kkv-k és a felhőszolgáltatók nézőpontja között:

A cégvezetéshez kapcsolódó információbiztonsági kihívások terén a szolgáltatók (39) nagyobb arányban említettek problémákat, mint a felhőhasználók (22). Ez arra utal, hogy a szolgáltatók jobban érzékelik, hogy a vezetői döntések és attitűdök jelentős hatással vannak a biztonság szintjére. Az IB kihívásoknál a másik jelentős tényező az IT: a szolgáltatók körében 23, míg a kkv-k esetében csak 5 db. Ez azt jelenti, hogy a szolgáltatók élesen érzékelik az IT infrastruktúrával kapcsolatos biztonsági kihívásokat, míg a felhasználói oldal ezeket vagy nem látja, vagy nem tekinti elsődleges problémának. A kihívások tekintetében a ráfordításokat mindkét oldal (16 vs. 22) hasonlóan látja. A kkv-k visszafogottabb említése mögött az állhat, hogy sok esetben rejtett költségek nem tudatosulnak náluk. Mindkét oldal érzékeli, hogy az információbiztonsági tudás és tapasztalat hiánya korlátozó tényező, de a szolgáltatók valamivel nagyobb arányban (17 vs. 25) hangsúlyozzák ezt, ami megfelel annak, hogy ők gyakran oktatói vagy támogatói szerepben vannak.

Stakeholderekhez kapcsolódó tényezők, külső kommunikáció esetében teljes szimmetria figyelhető meg: a felhasználók és szolgáltatók egyaránt 11 vs 11 alkalommal említik ezt a tényezőt. Ez a kód azt jelzi, hogy az információbiztonság külső kommunikációja (pl. ügyfelek, partnerek felé) egyaránt kihívás a két csoport számára. A külső szabályozásnál nagyobb különbség mutatkozik: a kkv-k csak 1, a szolgáltatók 8 alkalommal említik a

külső szabályozás szerepét. Ez alátámasztja, hogy a szolgáltatók sokkal érzékenyebbek a szabályozási környezet változásaira, míg a felhasználók vagy nem érzik közvetlen hatását, vagy nem tudják pontosan értelmezni azt. A Partneri elvárások tekintetében a szolgáltatók itt is hangsúlyosabb mértékben (13) említik ezt a faktort, szemben a felhasználók 6 említésével. A szolgáltatók számára tehát a partneri oldalon megjelenő biztonsági elvárások egyértelműbb és erősebb nyomást jelentenek, míg a kkv-k gyakran passzívabb szerepben vannak. Szervezeti tényezőkön belül a belső kommunikációs kihívásokat a kkv-k 26, a szolgáltatók 15 alkalommal említették. Ez azt sugallja, hogy a belső információáramlás akadozása erősebben jellemzi a kkv-k működését, és talán kevésbé formalizált náluk a kommunikációs struktúra.

A szolgáltatók esetében ez kevésbé kiemelt probléma, ami utalhat stabilabb szervezeti struktúrákra. A belső oktatásnál a kkv-k szintén dominálnak (20), szemben a szolgáltatókkal (9). Ez azt mutatja, hogy a biztonságtudatosság oktatása a felhasználói oldalon egy kritikus probléma, míg a szolgáltatók esetében valószínűleg formalizáltabb és rendszeresebb a képzési gyakorlat. A Belső szabályozás kategóriában szintén a kkv-k (46) dominálnak, ami arra utal, hogy a belső szabályozási mechanizmusok hiánya vagy nem megfelelő volta az ő oldalukon jelent nagyobb problémát. A szolgáltatók esetében a magasabb belső szabályozottság feltehetően megfelel az iparági elvárásoknak és compliance követelményeknek. A Külső szabályozási nyomás kiegyensúlyozottabb a megoszlás mutat: a kkv-k 11, míg a szolgáltatók 8 alkalommal említik. Ez arra utal, hogy a szabályozói környezet nemcsak az iparági szereplőkre, hanem már a kkv-kra is egyre nagyobb nyomást gyakorol, és ez valószínűleg GDPR-hoz vagy egyéb szabályozásokhoz köthető.

Összességében látható, hogy bár vannak átfedések a két oldal nézőpontja között, a szolgáltatók jobban látják a szervezeti és vezetői kihívásokat, míg a kkv-k inkább a gyakorlati előnyökre és költségekre fókuszálnak. Ez arra utal, hogy szükség van a két fél közötti jobb kommunikációra és megértésre a sikeres felhőalkalmazás érdekében. Az összehasonlítás alapján látható, hogy a felhőszolgáltatók és -felhasználók véleménye több ponton is eltér egymástól, illetve látni némi egyezést is. A következő fejezetben a felhő használatát elősegítő megoldások, javaslatok következnek az interjúk eredményei alapján.

A kutatás során nemcsak a felhőszolgáltatást igénybe vevő kkv-k nézőpontját vizsgáltam, hanem a szolgáltatók perspektíváját is feltártam, hogy átfogó képet kapjak a két oldal elvárásairól, tapasztalatairól és kihívásairól. A két szereplő nézőpontjának összevetése **r**ávilágít azokra az egyező pontokra és különbségekre, amelyek meghatározhatják a felhőszolgáltatások hatékony bevezetését és működtetését.

A 13. ábra A felhővel kapcsolatos kódok megjelenése az interjúkban (saját szerkesztés)13. ábra a felhőszolgáltatással kapcsolatos kódok előfordulását és megoszlását mutatja be az egyes interjúcsoportoknál a GT módszertan alapján létrehozott kódfa struktúráját követve, azaz azt mutatja meg, hogy Felhőszolgáltatás megjelenéséhez tartozó négy kód (akadály, előny, kihívás és motiváció) hogyan jelennek meg az egyes interjúcsoportokban. Az egyes interjúkat csoportosítottam aszerint, hogy kik voltak a válaszadók (szolgáltató, használó kkv).

		Felho_hasznalo_mind 18 310		Felho_szolgaltato_mind 16 344		Totals	
felho akadaly:cégkommunikáció	16			16 4,53%	100,00% 2,68%	16 2,68%	100,00% 2,68%
felho akadaly:kultúra, emberi tényező	20	3 1,23%	15,00% 0,50%	17 4,82%	85,00% 2,85%	20 3,35%	100,00% 3,35%
felho akadaly:tudás, kompetencia	61	14 5,74%	22,95% 2,35%	47 13,31%	77,05% 7,87%	61 10,22%	100,00% 10,22%
felho elony:anyagi vonzatok	37	8 3,28%	21,62% 1,34%	29 8,22%	78,38% 4,86%	37 6,20%	100,00% 6,20%
felho elony:biztonság	27	17 6,97%	62,96% 2,85%	10 2,83%	37,04% 1,68%	27 4,52%	100,00% 4,52%
felho elony:hasznalhatoság	27	12 4,92%	44,44% 2,01%	15 4,25%	55,56% 2,51%	27 4,52%	100,00% 4,52%
felho elony:IT erőforrás felszabadulás	33	18 7,38%	54,55% 3,02%	15 4,25%	45,45% 2,51%	33 5,53%	100,00% 5,53%
felho elony:rendelkezesre-allas	27	19 7,79%	70,37% 3,18%	8 2,27%	29,63% 1,34%	27 4,52%	100,00% 4,52%
felho elony:rugalmasság - skálázhatóság	40	16 6,56%	40,00% 2,68%	24 6,80%	60,00% 4,02%	40 6,70%	100,00% 6,70%
felho elvaras:biztonsági elvárások	39	17 6,97%	43,59% 2,85%	22 6,23%	56,41% 3,69%	39 6,53%	100,00% 6,53%
felho elvaras:elérhetőség - mobilitás	27	14 5,74%	51,85% 2,35%	13 3,68%	48,15% 2,18%	27 4,52%	100,00% 4,52%
felho elvaras:használhatóság	20	6 2,46%	30,00% 1,01%	14 3,97%	70,00% 2,35%	20 3,35%	100,00% 3,35%
felho kihivas:céges kultúra	23	10 4,10%	43,48% 1,68%	13 3,68%	56,52% 2,18%	23 3,85%	100,00% 3,85%
felho kihivas:IT infrastruktúra - IT osztály	34	23 9,43%	67,65% 3,85%	11 3,12%	32,35% 1,84%	34 5,70%	100,00% 5,70%
felho kihivas:jogszabályi, tv előírás	15	1 0,41%	6,67% 0,17%	14 3,97%	93,33% 2,35%	15 2,51%	100,00% 2,51%
felho kihivas:kultúra - egyén	8	7 2,87%	87,50% 1,17%	1 0,28%	12,50% 0,17%	8 1,34%	100,00% 1,34%
felho kihivas:ráfordítás	51	23 9,43%	45,10% 3,85%	28 7,93%	54,90% 4,69%	51 8,54%	100,00% 8,54%
felho kihivas:rugalmasság, elérés	3	3 1,23%	100,00% 0,50%			3 0,50%	100,00% 0,50%
felho kihivas:szakértelem, kompetencia	59	28 11,48%	47,46% 4,69%	31 8,78%	52,54% 5,19%	59 9,88%	100,00% 9,88%
felho motivacio:IT infrastruktúra és IT osztály	5	1 0,41%	20,00% 0,17%	4 1,13%	80,00% 0,67%	5 0,84%	100,00% 0,84%
felho motivacio:jogszabályi, törvényi előírás	4			4 1,13%	100,00% 0,67%	4 0,67%	100,00% 0,67%
felho motivacio:külső, piaci benyomás - partner	21	4 1,64%	19,05% 0,67%	17 4,82%	80,95% 2,85%	21 3,52%	100,00% 3,52%
Totals		244 100,00%	40,87% 40,87%	353 100,00%	59,13% 59,13%	597 100,00%	100,00% 100,00%

13. ábra A felhővel kapcsolatos kódok megjelenése az interjúkban (saját szerkesztés)

Az interjúk csoportosításának köszönhetően láthatjuk, hogy az egyes kódok milyen gyakorisággal jelennek meg a szolgáltatói és-vagy a használói oldalon.

A szolgáltatói oldal markánsabban érzékeli a felhőalapú technológiák bevezetését akadályozó tényezőket, mint a felhasználói oldal. Különösen szembetűnő ez a tudás és kompetenciahiány kategóriában: míg a szolgáltatók több mint háromszor annyi esetben említik ezt akadályként (47), a felhasználók mindösszesen 14 alkalommal nevesítették. Hasonló tendencia figyelhető meg a kulturális és emberi tényezők (3 vs. 17) és az cégkommunikáció (0 vs. 16) esetében is. Ez arra utal, hogy a szolgáltatók élesebben látják azokat a strukturális és szervezeti gátakat, amelyek gátolhatják az adaptációt – míg a felhasználók hajlamosabbak ezeket kevésbé reflektáltan kezelni, vagy éppen internalizálták, hogy ezekkel „együtt kell élni”. Az előnyök tekintetében világos elválás

figyelhető meg a két oldal észlelési horizontja között. A felhasználói oldal sokkal inkább a gyakorlati, üzletileg kézzelfogható hasznot emeli ki. Ilyen például a biztonság (17 vs. 10), a rendelkezésre állás (19 vs. 8) és az IT-erőforrások felszabadulása (18 vs. 15). Ezek az előnyök közvetlenül visszacsatolódnak a napi működésre, és gyakran a költséghatékonyság, gyorsaság, illetve kiszámíthatóság mentén értelmeződnek. Ezzel szemben a szolgáltatói oldal kiemeltebb hangsúlyt helyez olyan technológiai előnyökre, mint a rugalmasság és skálázhatóság (16 vs. 24) vagy a használhatóság (12 vs. 15). Ez a különbség arra utal, hogy a szolgáltatók kommunikációja és ajánlatai sokszor olyan előnyöket hangsúlyoznak, amelyeket a végfelhasználók nem feltétlenül érzékelnek elsődlegesnek. Ez az eltérés potenciálisan félreértésekhez vezethet a szolgáltatás értékajánlatának kommunikációjában: míg a szolgáltatók technológiai érvekkel dolgoznak, a kkv-k gyakorlati, működéshez kapcsolódó előnyöket várnak. A szolgáltatói oldal dominanciája figyelhető meg az elvárások tekintetében, különösen a biztonsági elvárások (17 vs. 22) és használhatóság (6 vs. 14) területén, míg a felhasználók esetében az elérhetőség-mobilitás (14 vs 13) játszik döntő szerepet, hiszen a szolgáltatók a szabályozásorientált stabilitást és megfelelést tartják szem előtt. A felhasználói elvárás alátámasztja azt az értelmezést, hogy a kkv-k számára a kényelem a szolgáltatásokkal szemben támasztott elsődleges elvárás, hiszen a felhasználók az azonnali használati értéket keresik. A kihívásokat tekintve a felhasználók leggyakrabban az IT infrastruktúrával (23) és az egyéni tényezőkkel (7) kapcsolatos nehézségeket emelik ki, vagyis olyan belső adottságokat, amelyek gátolják az új technológia beillesztését a meglévő működésbe. A szolgáltatói oldal ezzel szemben jóval hangsúlyosabban jelzi a kulturális kihívásokat (10 vs. 13), a szakértelem hiányát (28 vs. 31), valamint a ráfordítás kérdését (23 vs. 28). Ez ismét megerősíti, hogy a szolgáltatók a szervezeti átalakulás és tudásmegosztás oldaláról érzékelik leginkább a nehézségeket, míg a felhasználók inkább technikai és működési szinten szembesülnek problémákkal. A jogszabályi és törvényi előírásokkal kapcsolatos kihívások mindkét oldalon hasonló súllyal jelennek meg, ami közös szabályozási környezetre és annak általános komplexitására utal. A motivációk esetében a felhasználók számára a külső elvárások, mint például a piaci partnerek nyomása (4) és a IT infrastruktúra és IT osztály (1) jelentik a fontosabb hajtóerőt jelentenek. Ezzel szemben a szolgáltatók e tényezőket gyakorlatilag máshogy látják. A szolgáltatók szerint a piaci nyomás – partneri elvárások (17) jelentenek leginkább motivációs tényező a kkv-k számára a felhő bevezetése, alkalmazása kapcsán, míg az IT infrastruktúrát és a jogszabályi törvényi előírásokat nem, vagy alig említik, ami arra

utalhat, hogy számukra ezek a szempontok már strukturális adottságként vannak jelen, nem mint motivációk.

Tézis 2 Az interjúk alapján a kis- és középvállalkozások, valamint a szolgáltatók vonatkozásában tartalmi hasonlóságok és eltérések azonosíthatók az információbiztonság és a felhőszolgáltatások megjelenéséhez kapcsolódó kódok értelmezési dimenzióiban. [14, 292]

5. 3. Adaptációs viszonyrendszerek

C3: A kutatás célja feltárni, hogy milyen viszonyrendszerek és kapcsolati hálók rajzolódnak ki a felhőtechnológia bevezetését és használatát befolyásoló különböző tényezők között, a kvalitatív adatelemzés során létrejött kódok hálózati összefüggései alapján.

5. 3. 1. A kontextuselemzés – kódhálózat eredményei

A következő fejezetben a kódfában szereplő kódok alapján a felhőhasználat akadályai és előnyei közötti dinamika, valamint az információbiztonság és a felhőszolgáltatások kapcsolatát elemzem. A megkérdezettek válaszaiban említett szövegrészleteken kontextuselemzést végeztem, melynek eredményeit ebben a fejezetben mutatom be.

5. 3. 2. Információbiztonság és a szervezeti tényezők

A belső tréningek, kommunikáció és szabályozások együttesen határozzák meg a vállalatok információbiztonságát. Ez összhangban van Bulgurcu és munkatársainak. [133] megállapításaival, akik kimutatták, hogy az alkalmazottak információbiztonsági tudatossága és attitűdje jelentősen befolyásolja a vállalati információbiztonság szintjét. A belső kommunikáció és képzés fontosságát Siponen és munkatársai [138] is megerősítették, hangsúlyozva, hogy ezek kulcsfontosságúak az információbiztonsági politikák hatékony végrehajtásában. Az általam létrehozott kódfában szereplő idevonatkozó kódok és kapcsolataik:

„Információbiztonság cég: belső szabályozás” ↔ „Információbiztonság cég: belső kommunikáció” ↔ „Információbiztonság cég: belső tréning”

A kontextuselemzés szempontjából fontos megjegyezni, hogy ezek a témák nem izoláltan léteznek, hanem komplex kölcsönhatásban állnak egymással. Például, a

felhőszolgáltatások bevezetéséhez szükséges szakértelem hiánya nemcsak költségvonzattal jár, de közvetlenül befolyásolja a biztonsági kockázatokat is. Hasonlóképpen, a hatékony belső kommunikáció és képzés nemcsak az információbiztonságot javítja, de hozzájárulhat a felhőtechnológiák hatékonyabb és biztonságosabb használatához is.

A kutatás eredményei rávilágítanak arra, hogy a vállalatok számára kritikus fontosságú az információbiztonság és a felhő közötti egyensúly megteremtése. Ez magában foglalja a megfelelő szakértelem kiépítését, a biztonsági szabályozások folyamatos fejlesztését, valamint az alkalmazottak rendszeres képzését és tájékoztatását. A jövőbeli kutatások szempontjából érdekes lehet annak vizsgálata, hogy a vállalatok hogyan tudják optimalizálni erőforrásaikat e kihívások kezelésére, valamint hogyan változnak ezek a dinamikák különböző iparágakban és vállalati méretekben.

Az interjúalanyoknak a kkv-nál tetten érhető információbiztonsági helyzetre vonatkozóan is válaszolniuk kellett. Az információbiztonság kapcsán többek között olyan szempontból végeztem vizsgálatot, hogy miként vélekednek az információbiztonságról általánosságban, illetve a cégen belül, ez hogyan jelenik még a kkv-nál, valamint milyen kihívásokkal szembesülnek a kkv-k, amikor információbiztonságról beszélünk.

A 7. táblázat Az információbiztonsághoz kapcsolódó kódok (saját szerkesztés)

az információbiztonsághoz kapcsolódó megjelenési formák, kihívások és cégen kívüli hatások megjelenését mutatja az egyes interjúkban, aszerint, ahogy miként ítélik meg az információbiztonságot, mi a véleményük róla, illetve az információbiztonsági incidensek. A táblázatban szereplő számok mögött zárójelben található a c-koefficiens érték, ami a két kód közötti kapcsolat erősségét jelzi. A c-koefficiens értéke 0 és 1 között mozog: 0 azt jelenti, hogy a kódok nem fordulnak elő együtt; az 1 azt jelenti, hogy ezek a kódok mindenhol együtt fordulnak elő, ahol használják őket. A c-koefficiens kiszámítása a következőképpen történik: $c = n_{12} / (n_1 + n_2 - n_{12})$. A n_{12} = a kódok n_1 és n_2 együttes előfordulásainak száma. A kódok után szereplő Gr érték pedig az adott kóddal ellátott szövegrészletek számát jelöli.

	ib incidens Gr=29	**ib velemeny: negatív Gr=8**	**ib velemeny: pozitív Gr=46**	**ib velemeny: semleges Gr=17**
ib kihivas: cégvezetés Gr=61	4 (0,05)	0 (0)	2 (0,02)	1 (0,01)

ib kihivas: IT Gr=28	3 (0,06)	0 (0)	0 (0)	0 (0)
ib kihivas: ráfordítás Gr=38	7 (0,12)	1 (0,02)	3 (0,04)	3 (0,06)
ib kihivas: tapasztalat, tudás Gr=42	4 (0,06)	0 (0)	1 (0,01)	0 (0)
ib stakeholderek: kulso kommunikacio Gr=22	1 (0,02)	0 (0)	6 (0,1)	0 (0)
ib stakeholderek: kulso szabalyozas Gr=9	0 (0)	0 (0)	2 (0,04)	0 (0)
ib stakeholderek: partneri elvárás Gr=19	0 (0)	0 (0)	5 (0,08)	1 (0,03)
ib szervezet: belso kommunikacio Gr=41	2 (0,03)	2 (0,04)	5 (0,06)	0 (0)
ib szervezet: belso oktatas Gr=29	4 (0,07)	0 (0)	2 (0,03)	0 (0)
ib szervezet: belso szabalyozas Gr=71	6 (0,06)	1 (0,01)	4 (0,04)	1 (0,01)
ib szervezet: kulso szabalyozas-nyomas Gr=19	2 (0,04)	1 (0,04)	0 (0)	2 (0,05)

7. táblázat Az információbiztonsághoz kapcsolódó kódok (saját szerkesztés)

A megkérdezettek pozitívan értékelik az információbiztonság jelenségét és csak elenyésző számban gondolják negatívnak *(„szükséges nyűg”*). Maga az információbiztonság főként szabályzatok és szabályozási vonalon került megemlítésre a megkérdezetteknél és többségüknél valamilyen mértékben vannak is szabályzatok erre vonatkozólag. Viszont az egyik legnagyobb kihívás, akárcsak a felhőszolgáltatás kapcsán a ráfordítás *(„általában a minimumra törekednek, ameddig meg nem történik a baj, utána átesnek a ló túloldalára”, „budget alapon, ha marad pénz rá, akkor szívesen veszik …”*), hiszen nem fordítanak rá eleget.

Az interjúkból általános véleményként leszűrhető, hogy az információbiztonságot a legtöbb résztvevő kritikus fontosságúnak tartotta, mind az üzleti működés, mind a partneri kapcsolatok szempontjából. Továbbá említésre kerültek olyan kulcsfontosságú szempontok is, mint az ISO 27001 tanúsítás, a többfaktoros hitelesítés (MFA), a jelszókezelési szabályok bevezetése és használata, illetve informatikai biztonsági képzések léte, szükségessége.

„Az IT-biztonság ma már alapvető üzleti követelmény, különösen B2B kapcsolatokban” (D3).

A D3 résztvevőtől származó figyelemre méltó szövegrészlet hangsúlyozza, hogy az IT-biztonság ma már alapvető üzleti követelmény, különösen az üzleti vállalkozások közötti (B2B) kapcsolatokban.

Ez az összefoglaló arra utal, hogy a szervezetek egyre inkább felismerik az információbiztonság kritikus szerepét az üzleti működés fenntartásában és a partnerekkel és ügyfelekkel szembeni bizalom ápolásában. A konkrét biztonsági intézkedések említése azt jelzi, hogy az érzékeny információk védelme és az iparági szabványoknak való megfelelés érdekében konkrét stratégiák végrehajtására összpontosítanak.

5. 3. 3. Információbiztonság és a felhőhasználat

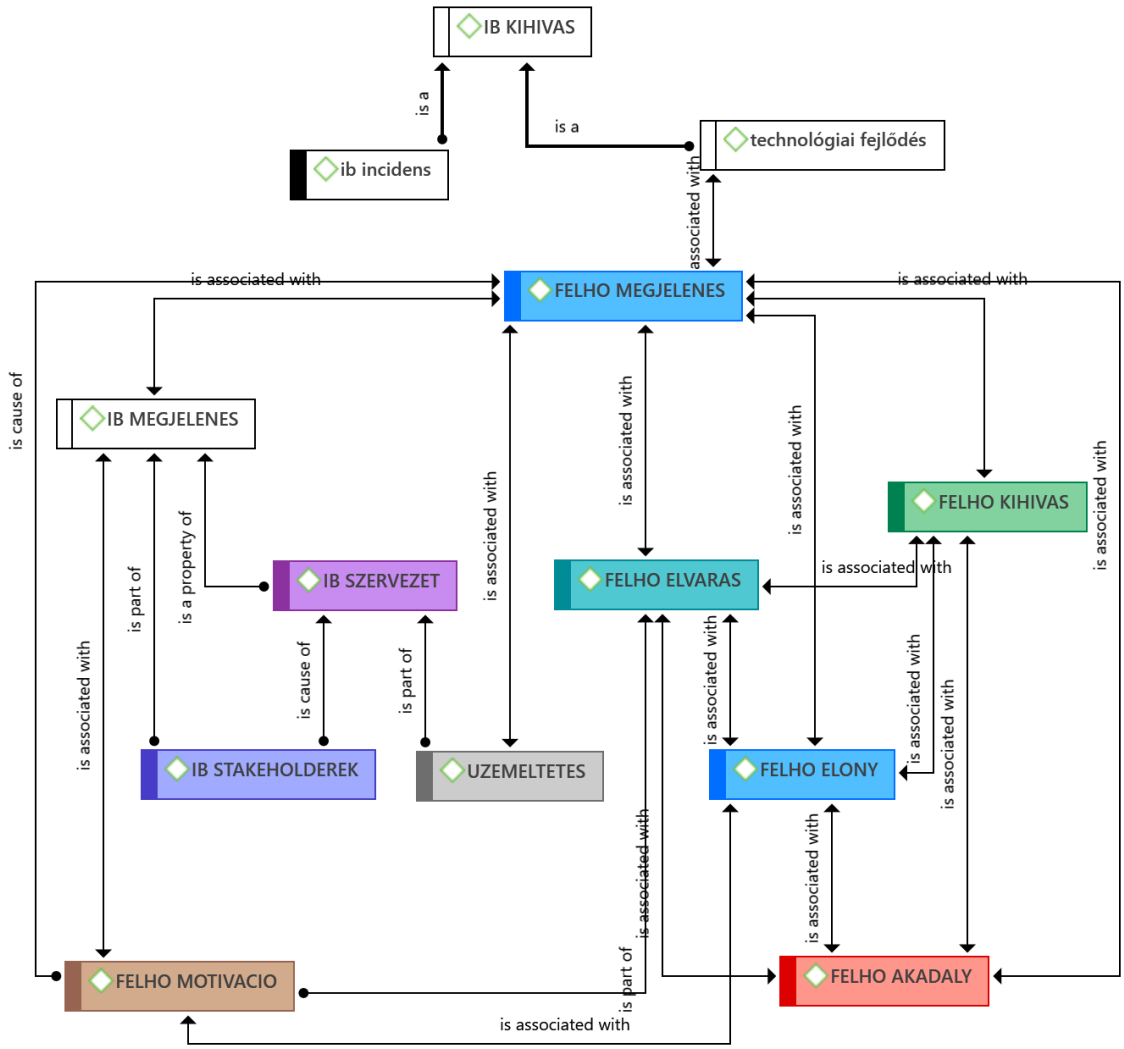
A felhő bevezetésének egyik fő akadálya a szükséges szakértelem hiánya és az ehhez kapcsolódó költségek. Ez összhangban van El-Gazzar és munkatársainak [297] megállapításaival, akik kimutatták, hogy a technológiai bizonytalanság és a szakértelem hiánya jelentős gátló tényezők a felhőhasználatban. Ugyanakkor a felhő előnyei, mint a rugalmasság és a potenciális költségmegtakarítások, vonzóak a kkv-k számára. Uddin és munkatársainak [298] kutatása rámutatott, hogy a felhőszolgáltatások rugalmassága és skálázhatósága különösen értékes a gyorsan változó üzleti környezetben. Az általam létrehozott kódfában szereplő idevonatkozó kódok és kapcsolataik:

„Felhő akadály: tudás, kompetencia” ↔ „Felhő kihívás: szakértelem, kompetencia” ↔ „Felhő kihívás: ráfordítás”

A biztonsági elvárások kulcsszerepet játszanak a felhő bevezetésében. Ez összhangban van Subashini és Kavitha [299] megállapításaival, akik hangsúlyozták, hogy az információbiztonság és az adatvédelmi kérdések a felhő legkritikusabb aspektusa. A felhő és az információbiztonság közötti szoros kapcsolat kiemeli az információbiztonsági szabályozás fontosságát. Chang és munkatársainak [300] kutatása rámutatott, hogy a hatékony biztonsági szabályozások és gyakorlatok kulcsfontosságúak a felhőalapú rendszerek biztonságos működtetésében. Az általam létrehozott kódfában szereplő idevonatkozó kódok és kapcsolataik:

„Információbiztonság kihívás: IT” ↔ „Felhő - információbiztonság: van kapcsolat” ↔ „Felhő elvárás: biztonsági elvárások”

A felvett interjúkat a már korábban ismertetett GT kódfa fogalmai mentén elemeztem. Első körben a felhő megjelenéséhez kapcsolódó kódok hálózatát választottam. A 14. ábra hierarchikus struktúrát alkalmaz, az elemek közötti különböző kapcsolatokkal, amelyeket különböző típusú kapcsolatok képviselnek. Az ábra központi fogalmai a FELHO MEGJELENES (Felhő megjelenése): ez az egyik központi csomópont, amely több más koncepcióhoz is kapcsolódik. IB MEGJELENES (Információbiztonság megjelenése): A felhő megjelenéséhez szorosan kapcsolódó másodlagos kulcsfogalom. Az ábra az információbiztonsági kihívások, a felhőalapú megoldások és a szervezeti tényezők közötti összetett kölcsönhatásra utal. Rávilágít arra, hogy a felhő megjelenése hogyan befolyásolja és befolyásolja az információbiztonság különböző aspektusait, beleértve a kihívásokat, elvárásokat, előnyöket és akadályokat. Az ezen elemek közötti kapcsolatok kétirányúak, ami kölcsönös befolyásra és kölcsönös függőségre utal.



14. ábra Az interjúk kódhálózata és kapcsolódásai (saját szerkesztés)

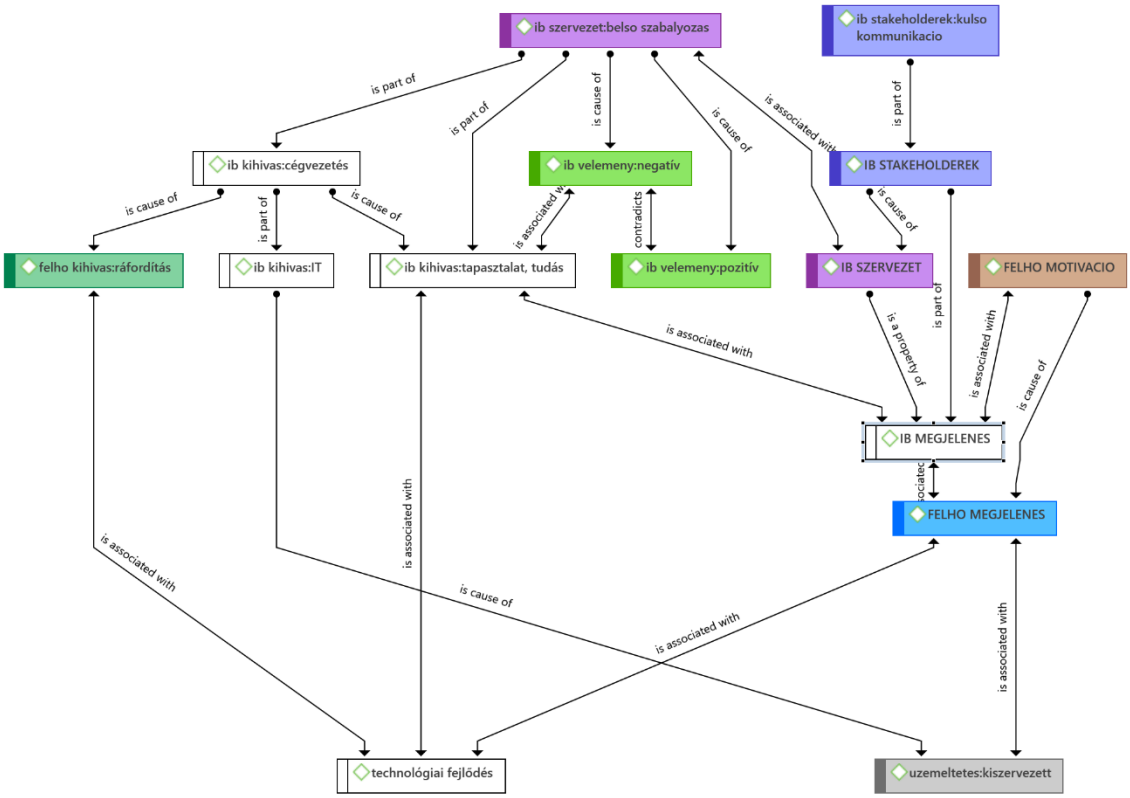
A kódokat összekötő kapcsolatokat az interjúk szövegrészletei alapján, illetve az ATLAS.ti szoftverben előzetsen meghatározott kapcsolati típusok szerint kötöttem össze. Az előredefiniált kapcsolati típusokat az alábbi 8. táblázat szemlélteti.

Kapcsolat típusa	***Példamondat***	***Példabeli fogalompár***	***Logikai tulajdonság***
is-associated-with (összefügg/társul)	A stressz szintje társulhat az alvásminőség romlásával.	stressz – alvásminőség	Szimmetrikus
is-part-of (része)	A billentyűzet része a számítógépnek.	billentyűzet – számítógép	Tranzitív
is-cause-of (oka)	A biztonsági frissítések elmaradása okozza a rendszer sebezhetőségét.	frissítések elmaradása – sebezhetőség	Tranzitív
contradicts (ellentéte)	A nyílt hozzáférés ellentmond az adatvédelem elvének.	nyílt hozzáférés – adatvédelem	Szimmetrikus
is-a (az)	A tűzfal egy hálózati biztonsági megoldás.	tűzfal – biztonsági megoldás	Tranzitív
is-property-of (tulajdonsága)	A modularitás a szoftverfejlesztési architektúrák egyik jellemzője.	modularitás – architektúra	Aszimmetrikus

8. táblázat Az ATLAS.ti szoftver előre definiált logikai kapcsolattípusai (saját szerkesztés)

A kódokat összekötő nyilak a kódok közötti kapcsolatokat, összefüggéseket jelölik. Ennek megfelelően a „*is a*” kapcsolatok: Osztályozást vagy kategorizálást jeleznek (pl. az IB incidens az IB KIHIVAS egy típusa). Az. „*is associated with* (társul)” kapcsolatok a fogalmak közötti kölcsönös hatásokat vagy korrelációkat reprezentálják. Az „*is part of* (része)” kapcsolatok hierarchikus struktúrákat vagy nagyobb fogalmak összetevőit jelölik. A „*is reason of* (oka)” kapcsolatok: Az elemek közötti ok-okozati kapcsolatokra utalnak.

A 16. ábra az információbiztonsághoz kapcsolt fogalmak és kapcsolatok összetett vizuális megjelenítését szemlélteti. A hálózati ábra egy komplex, többtényezős értelmezési keretet kínál az információbiztonság (IB) szervezeti szintű léterhozásához, alkalmazásához kapcsolódó tényezők feltérképezésére. A vizualizáció fogalmi kapcsolatokon (pl. „is cause of”, „is associated with”, „is part of”) keresztül jeleníti meg a kulcskategóriák közötti viszonyrendszert, hangsúlyozva a technológiai fejlődés, a tudás- és tapasztalathiány, valamint a szervezeti és kommunikációs tényezők kulcsszerepét.



15. ábra Az interjúk információbiztonsággal kapcsolatos kódhálózata és kapcsolódásai (saját szerkesztés)

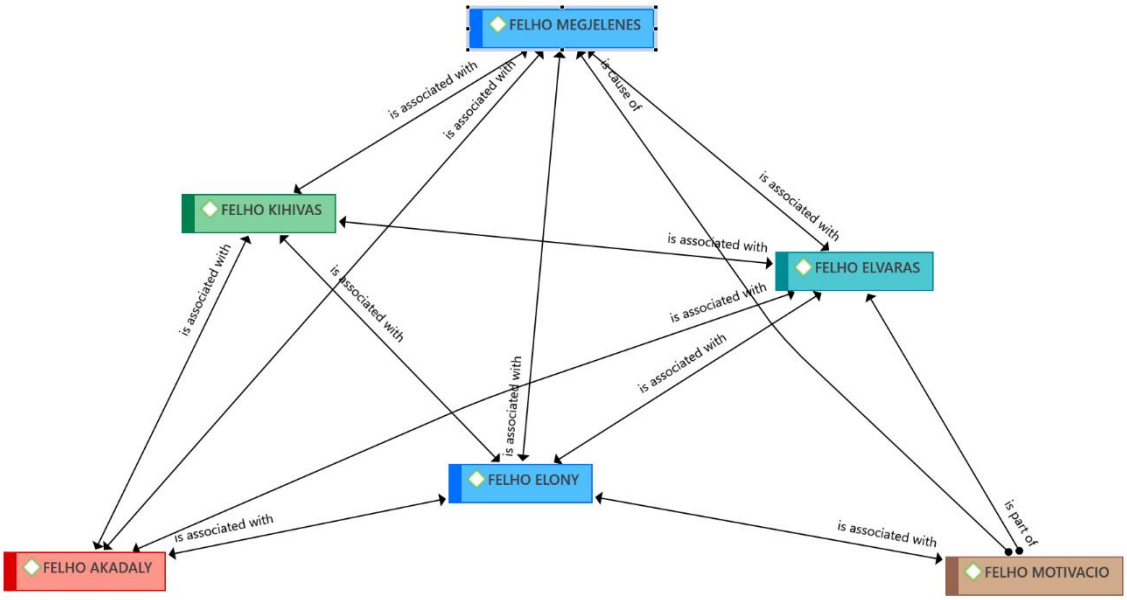
Az ábra alapján világosan látható, hogy az információbiztonság (IB megjelenés) **bevezetése és alkalmazása** nem csupán technikai, hanem **szervezeti, tudásbeli és kommunikációs tényezők által strukturált folyamat**. A tudáshiány és a vezetési kihívások kulcsszerepet játszanak a ráfordítási nehézségek és a negatív vélekedések kialakulásában, míg a belső szabályozás és a külső kommunikációs tér befolyásolja, hogy miként jelenik meg a technológia, a biztonság, és milyen motivációk kapcsolódnak hozzá.

A hálózati elemzés lehetőséget teremt arra, hogy a **puha (soft) tényezők** – például vélemények, megjelenés, kommunikáció – éppoly meghatározóként jelenjenek meg, mint a hard (technikai, strukturális) elemek, így holisztikus képet adva a kkv-k és szolgáltatók adaptációs stratégiáiról.

Ez a vizuális ábrázolás segít megérteni az információbiztonság sokrétűségét a felhő kontextusában, hangsúlyozva a technológiai, szervezeti és működési tényezőket figyelembe vevő átfogó megközelítés szükségességét. Az elemzés keretet biztosít a felhőbevezetést és -használatot befolyásoló különböző tényezők és a szervezetek információbiztonság közötti összetett összefüggések vizsgálatához. Útmutatóul szolgálhat a felhőtechnológia bevezetésével kapcsolatos kihívások, motivációk és

akadályok, valamint az ebben az összefüggésben kialakuló információbiztonsági viselkedésminták kutatásához.

A 16. ábra a felhőhöz kapcsolt fogalmak és kapcsolatok összetett vizuális megjelenítését szemlélteti.



16. ábra Az interjúk felhővel kapcsolatos kódhálózata és kapcsolódásai (saját szerkesztés)

A „felhő megjelenés" főkategória esetében öt, egymással összefüggő kategóriát azonosíthatunk: felhő kihívások, felhőhasználati motiváció, felhő akadályok, felhő előnyök és felhő elvárások. Az ábra több csomópontból áll, amelyeket különböző színű téglalapok ábrázolnak, és amelyeket irányjelző nyilak kötnek össze. Minden egyes csomópont egy adott fogalmat vagy változót képvisel, míg a nyilak a fogalmak közötti kapcsolatokat vagy összefüggéseket jelzik. A csomópontokat összekötő nyilak olyan kifejezésekkel vannak jelölve, mint „része", „társul" és „típusa", amelyek a fogalmak közötti kapcsolatok jellegét jelzik. A nyilak a kapcsolatok irányát jelzik, ami a fogalmak közötti oksági vagy hierarchikus kapcsolatokra utal. A hálózat magas fokú komplexitást mutat, több egymást keresztező kapcsolattal és több szintű kapcsolattal. Egyes csomópontok sűrűbben kapcsolódnak egymáshoz, klasztereket alkotva, amelyek a nagyobb kereten belül szorosan összefüggő fogalmakat vagy részterületeket képviselhetnek.

Ezek a kategóriák összefüggenek egymással, és két különböző csoportba sorolhatók:

1. csoport: A felhő bevezetését befolyásoló tényezők

- Felhővel kapcsolatos kihívások
- Felhőhasználat akadályai
- Felhőhasználati motiváció

2. csoport: A felhő bevezetésének észlelt eredményei

- A felhő előnyei
- Felhővel kapcsolatos elvárások

Az első csoport azokra a tényezőkre összpontosít, amelyek befolyásolják egy szervezet felhőtechnológia bevezetésére vonatkozó döntését. A felhővel kapcsolatos kihívások és akadályok a bevezetési folyamat során felmerülő akadályokat és nehézségeket jelentik, míg a felhőhasználat motivációja a felhőmegoldások bevezetésére vonatkozó döntés mögött álló hajtóerőket foglalja magában.

A második csoport a felhő bevezetésének várható és megvalósult előnyeivel foglalkozik. A felhőelőnyök a felhőtechnológiát bevezető szervezetek által tapasztalt pozitív eredményeket emelik ki, míg a felhőelvárások a várt előnyöket és fejlesztéseket képviselik, amelyek az alkalmazást motiválják.

Ahhoz, hogy ezek a kategóriák fogalmakká fejleszthetők legyenek, szükséges az adatok további elemzése annak érdekében, hogy az egyes kategóriákon belül konkrét témákat, mintákat és kapcsolatokat lehessen azonosítani. Erre egy lehetséges példát az alábbi 9. táblázat tartalmaz.

Felhő kihívások	**Felhőhasználati motiváció**	**Felhőhasználat akadályai**	**A felhő előnyei**	**Felhőelvárások**
Információ-biztonsági aggályok	Költség-csökkentés	Szabályozási megfelelési kérdések	Fokozott rugalmasság és agilitás	Fokozott működési hatékonyság
Integráció a meglévő rendszerekkel	Skálázhatósági követelmények	Hagyományos rendszerfüggőségek	Jobb katasztrófa utáni helyreállítás	Jobb erőforrás-elosztás
A személyzet képzése és a készségek hiányosságai	Javított együttműködési képességek	Ellenállás a változással szemben	Hozzáférés a fejlett technológiákhoz	Versenyelőny a piacon

9. táblázat Az interjúkból azonosított kódkategóriák részlete (saját szerkesztés)

Az e fogalmak és kategóriák közötti kapcsolatok vizsgálatával átfogó kép alkotható a felhő megjelenésének jelenségéről és a szervezetekre gyakorolt hatásáról. Ez a GT alapú megközelítés lehetővé teszi az új meglátások és elméletek kialakulását az összegyűjtött adatok alapján, ahelyett, hogy előre kialakított elképzelésekre vagy meglévő keretekre támaszkodnának.

A részletesebb kódhálózati ábrát a 4. és 5. sz. melléklet tartalmazza.

A kkv-knál meghatározhatók a kódok hálózatával az információbiztonságot és a felhőt befolyásoló tényezők.

a) A kkv-knál meghatározhatók a kódok hálózatával az információbiztonságot befolyásoló tényezők. Az információbiztonságot befolyásoló tényezők a kkv-k esetében az alábbiak: az információbiztonsági kihívások, a szervezet, a stakeholderek, az információbiztonságról alkotott vélemény és a technológiai fejlődés, továbbá a felhő megjelenése is.
b) A kkv-knál meghatározhatók a kódok hálózatával a felhőt befolyásoló tényezők. A kkv-nál a felhő megjelenését befolyásolja a felhővel kapcsolatos kihívások, akadályok, elvárások, előnyök és motivációk.

Tézis 3 A kutatásban kódhálózati elemzéssel meghatároztam és bizonyítottam, hogy a kkv-k információbiztonságát a biztonsági kihívások, szervezeti és technológiai tényezők, míg a felhőhasználatot a motivációk, előnyök, akadályok és elvárások együttesen befolyásolják.[14, 292]

5. 4. Érzelmi mintázatok

Az interjúkérdésekre adott válaszok alapján megállapítottam, hogy az egyes megkérdezettek hogyan vélekednek a felhőszolgáltatással és annak használatával kapcsolatban. Bár 654 szövegrészlet került bekódolásra az interjúkból, a szentiment elemzésbe kevesebb került be. A kódolás és a szentiment elemzés közötti eltérés az alábbi tényezőkkel indokolt:

- Nem minden kódolt szövegrészlet tartalmaz érzelmi töltetet vagy véleményt, ami a szentiment elemzés szempontjából releváns lenne.
- Egyes szövegrészletek önmagukban nem hordoznak egyértelmű érzelmi töltetet, csak a tágabb kontextusban értelmezhetők.

- A hasonló tartalmú vagy ismétlődő szövegrészletek kiszűrése a pontosabb elemzés érdekében erősen indokolt.
- Csak a leginkább informatív és egyértelmű érzelmi töltetet hordozó részletek kerültek be a szentiment elemzésbe.

A kisebb minta alkalmazását továbbá a manuális elemzés is indokol a kutatás során használt szoftver nyelvi korlátai miatt, ami szükségessé teszi a manuális feldolgozást.

Az elemzés során 91 mondatot három (pozitív, semleges, negatív) érzelmi kategóriába soroltam. Mindezek mellett a bekategorizált mondatokat aszerint is osztályoztam, hogy milyen formában jelenik meg az adott mondat tartalma, valamint a tartalmuk mire vonatkoznak. A mondat tartalmának formája lehetett gyenge pont, motiváció, hozzáállás és vágy; míg vonatkozása pedig az alábbiak lehettek: bevezetés, teljesítmény, elégedettség, tapasztalat, elkötelezettség, megtartás. A mondatoknál megvizsgáltam hogy a mondat összességében negatív, semleges vagy pozitív polaritású-e. Ezeket összegezve megkaptam, hogy a 91 azonosított és kategorizált mondat érzelemszerinti megoszlása 32 negatív, 54 semleges és 5 pozitív, azaz a válaszok közel 60%-a semleges kicsengésű, kicsivel több mint harmada (35,2%) negatív és alig 6%-a pozitív. A 34 interjúból a feltételezések mentén szentiment elemzést is végeztem a korábban említett mondatszinten. Ennek eredményeit a 10. táblázat - 13. táblázatok mutatják be, ami a beazonosított mondatok mintegy felét (42 db) tartalmazza.

A 10. táblázat azt mutatja, hogy a munkavállalók képzésének és tájékoztatásának hiánya hogyan akadályozza a felhőszolgáltatások használatát.

Megjelenés - Cél	Pozitív	Semleges	Negatív
Munkavállalók képzésének és tájékoztatásának hiánya hátráltatja a felhőszolgáltatás használatát (n = 11)			
Gyenge pont - Bevezetés	-	9,1% (1)	-
Gyenge pont - Teljesítmény	-	9,1% (1)	-
Gyenge pont - Elégedettség	-	-	27,3% (3)
Gyenge pont - Tapasztalat	-	-	9,1% (1)
Motiváció - Elégedettség	-	9,1% (1)	9,1% (1)
Motiváció - Teljesítmény	-	9,1% (1)	-
Motiváció - Elkötelezettség	-	9,1% (1)	-
Motiváció - Megtartás	-	9,1% (1)	-

10. táblázat Az interjúk szentiment elemzése a munkavállalók képzésének és tájékoztatásának hatásai alapján (saját szerkesztés)

Ez a kutatási téma a szervezeti menedzsment és az informatikai bevezetés összefüggésében releváns. Az eredmények összesen 11 releváns szövegrészlet mutatnak,

amelyek 4 negatív és 7 semleges érzelmű szövegrészletet tartalmaznak. Ez az eloszlás arra utal, hogy a szervezeten belül vegyesen érzékelik a felhőszolgáltatások bevezetésével kapcsolatos kihívásokat.

Az elemzés feltárta a gyengepontok és a szervezeti célok közötti összetett kölcsönhatást. Az első felismerés egy kritikus gyengepontot emelt ki: az alkalmazottak képzésének és tájékoztatásának hiányát. Ezt a gyenge pont azonban szembeállítható a felhő bevezetésének átfogó szervezeti céljával. Ez a kettősség kiemeli az azonnali kihívások és a hosszú távú stratégiai célok közötti feszültséget. Ez a bontás betekintést nyújt a felhőszolgáltatások elfogadásának azon konkrét aspektusaiba, amelyeket a munkavállalók képzésének és tájékoztatásának hiánya befolyásol. A negatív vélemények koncentrációja a „Gyenge pont - elégedettség" kategóriában arra utal, hogy a dolgozók elégedettségét különösen befolyásolja az elégtelen képzés és tájékoztatás. A gyenge pontok és a motivációs tényezők jelenléte egyaránt árnyalt nézőpontot jelez a kérdéssel kapcsolatban. Miközben vannak egyértelmű kihívások, vannak potenciális területek is a javulás és a motiváció szempontjából. Ezek az eredmények arra utalnak, hogy a felhő bevezetésével és az információbiztonsági megfeleléssel kapcsolatos különböző kihívások kezeléséhez sokoldalú megközelítésre van szükség. Az eredmények hozzájárulnak a szervezeteken belüli technológiai bevezetés emberi tényezőinek megértéséhez, és kiemeli a munkavállalók oktatásának fontosságát a sikeres digitális átalakítási kezdeményezésekben.

A 11. táblázat a felhőszolgáltatás elfogadását befolyásoló kommunikációt mutatja be az interjúkon végzett szentiment elemzés alapján.

Megjelenés - Cél	Pozitív	Semleges	Negatív
Kommunikáció hiánya hatással van a felhő elfogadására (n = 6)			
Gyenge pont - Elkötelezettség	-	-	16,7% (1)
Gyenge pont - Megtartás	-	-	33,3% (2)
Gyenge pont - Elégedettség	-	33,3% (2)	-
Gyenge pont - Tapasztalat	-	-	16,7% (1)

11. táblázat Az interjúk szentiment elemzése a kommunikáció felhőre gyakorolt hatása alapján (saját szerkesztés)

A vizsgálat hat releváns szövegrészletet azonosított szentiment elemzéssel. Az elemzés kimutatta, hogy négy szövegrészlet negatív hangnemű, míg kettő semleges volt. Ez az eloszlás túlnyomórészt negatív megítélésre utal a kommunikációs hiányosságok felhőátvételre gyakorolt hatását illetően.

A gyenge pont - elkötelezettség megjelenés – cél párosnál megjelenő 1 szövegrészlet negatív érzelmeket fejezett ki. Ez azt jelzi, hogy a nem megfelelő kommunikáció negatívan befolyásolhatja a felhőátvétel céljai iránti szervezeti elkötelezettséget. A gyenge pont – Megtartás párosnál a 2 negatív szövegrészlet magasabb aránya ebben a kategóriában arra utal, hogy a kommunikációs problémák jelentősen befolyásolják a felhőtechnológiák vagy a kapcsolódó készségek megtartását a szervezeten belül. Azonban a gyenge pont – Elégedettség pároshoz tartozó 2 semleges érzelmeket tartalmazó szövegrészletek ebben a kategóriában arra utalnak, hogy a kommunikáció hiánya nem befolyásolja közvetlenül a felhasználók felhőtechnológiákkal való elégedettségét, vagy annak hatása nem egyértelműen meghatározható.

Az eredmények azt mutatják, hogy a kommunikáció hiánya elsősorban a megtartás és az elkötelezettség szempontjait befolyásolja a felhő bevezetése során. A szervezeteknek a kommunikációs stratégiák javítására kell összpontosítaniuk, hogy ezeket a területeket erősítsék. Az elégedettséggel kapcsolatos semleges vélemények arra utalnak, hogy más tényezők jelentősebb szerepet játszhatnak a felhőtechnológiákkal való felhasználói elégedettség meghatározásában.

A 12. táblázat a felhőszolgáltatás elfogadásával kapcsolatos interjúk hangulatelemzése a döntéshozók és az IT szakemberek felhőszolgáltatás igénybevételére gyakorolt összetett kölcsönhatását tárja fel.

Megjelenés - Cél	Pozitív	Semleges	Negatív
Döntéshozókon és az IT-n múlik a felhőszolgáltatás igénybevétele (n = 6)			
Hozzáállás - Megtartás	-	16,7% (1)	-
Motiváció - Megtartás	-	16,7% (1)	-
Motiváció - Elkötelezettség	-	16,7% (1)	16,7% (1)
Motiváció - Teljesítmény	-	16,7% (1)	16,7% (1)

12. táblázat Az interjúk szentiment elemzése a döntéshozók és IT szakemberek jelentősége alapján (saját szerkesztés)

Szentiment elemzéssel 6 releváns szövegrészletet azonosítottam, 2 negatív és 4 semleges hangneműeket. Ez az eloszlás azt sugallja, hogy a megkérdezettek kiegyensúlyozott szemléletet képviselnek a felhőszolgáltatás elfogadásával kapcsolatban, a semleges nézetek felé való enyhe hajlammal.

Az elemzés a hangnemüket tekintve az alábbiakat sugallja. Mérsékelt hozzáállást jelez a jelenlegi felhőszolgáltatási megállapodások fenntartásával kapcsolatban, illetve kiegyensúlyozott véleményt sugall a felhőszolgáltatások további használatát ösztönző

tényezőkkel kapcsolatban. A felhőszolgáltatások szervezeti elkötelezettségét befolyásoló tényezők vegyes megítélését tükrözi. A negatív érzelmek jelenléte a motiváció-elkötelezettség területen a teljes elkötelezettség lehetséges akadályaira utalhat. Az elkötelezettséghez hasonlóan a motiváció-teljesítmény kategória is megosztott véleményeket mutat arról, hogy a felhőszolgáltatások hogyan hatnak a szervezeti teljesítményre.

A semleges hangnemű szövegrészletek túlsúlya az összes kategóriában arra utal, hogy a döntéshozók és az informatikai szakemberek óvatos vagy ambivalens álláspontot képviselnek a felhőszolgáltatásokkal kapcsolatban. Ez a felhő szolgáltatások bevezetésének összetett jellegével magyarázható, amely különböző tényezők, például a költségek, a biztonság, a skálázhatóság és a meglévő rendszerekkel való integráció mérlegelését jelenti.

Különösen figyelemre méltóak a negatív vélemények a Motiváció - elkötelezettség és a Motiváció - teljesítmény kategóriákban. Ezek a felhőszolgáltatások hatékony bevezetésének kihívásaival kapcsolatos aggodalmakat vagy a felhőszolgáltatások állítólagos előnyeivel kapcsolatos szkepticizmust tükrözhetik. Ezek az érzések korábbi tapasztalatokból, vélt kockázatokból vagy a felhő bevezetésének hosszú távú következményeivel kapcsolatos bizonytalanságokból eredhetnek.

A szövegrészletek különböző hangnemei azt jelzik, hogy a felhőszolgáltatások bevezetéséhez árnyalt megközelítésre van szükség. A szervezeteknek foglalkozniuk kell a negatív véleményekben tükröződő aggodalmakkal, miközben a semleges nézőpontokat az oktatás és a stratégiai tervezés lehetőségeként kell kihasználniuk. A további kutatások feltárhatják a fenti vélemények mögött meghúzódó konkrét okokat, és így esetleg iparágspecifikus kihívásokat vagy lehetőségeket tárhatnak fel a felhőszolgáltatások bevezetése terén.

Ez az érzelmek különböző kategóriák közötti megoszlása értékes betekintést nyújt a szervezeti dinamikába. A negatív érzelmek koncentrációja a teljesítmény kategóriában arra utal, hogy a pénzügyi prioritások felállítását az általános teljesítményeredményekre nézve károsnak tekinthetik. A motivációval kapcsolatos kategóriák semleges érzelmei arra utalnak, hogy a pénzügyi ösztönzőknek a munkavállalói magatartás és a szervezeti siker irányításában betöltött szerepét árnyaltabban értelmezik. A negatív és semleges vélemények keveredése a kategóriák között rávilágít a szervezeti döntéshozatal

sokrétűségére, ahol a pénzügyi megfontolások keresztezik egymást a stratégiai célokkal és a hasznossági értékelésekkel. A semleges vélemények jelenléte az olyan területeken, mint a megtartás és a motiváció bevezetése, olyan hatékonyabb stratégiák kidolgozásának lehetőségeit sugallja, amelyek kiegyensúlyozzák a pénzügyi és nem pénzügyi tényezőket.

Összefoglalva, ez az érzelemelemelemzés rámutat arra, hogy a szervezeteknek kritikusan át kell értékelniük a pénzügyi megfontolások, a stratégiai célkitűzések és a hasznossági értékelések közötti egyensúly megteremtésére irányuló megközelítésüket. Az eredmények azt sugallják, hogy bár a pénzügyi szempontok jelentősek, nem szabad, hogy háttérbe szorítsák a szervezeti sikerhez és a munkavállalók elégedettségéhez hozzájáruló egyéb kulcsfontosságú tényezőket.

A technológiai fejlődéssel és az információbiztonsági kultúrával kapcsolatos interjúk hangulatelemzése a válaszadók összetett felfogását és hozzáállását mutatja a 13. táblázat.

Megjelenés - Cél	Pozitív	Semleges	Negatív
Technológiai fejlődés miatt új fajta kihívások, fenyegetések magasabb szintű információbiztonsági kultúra kialakítását igénylik (n = 12)			
Hozzáállás - Bevezetés	-	33,3% (4)	8,3% (1)
Motiváció - Teljesítmény	-	8,3% (1)	-
Vágy - Bevezetés	-	16,7% (2)	-
Vágy - Elégedettség	-	16,7% (2)	-
Vágy - Megtartás	-	8,3% (1)	8,3% (1)

13. táblázat Az interjúk szentiment elemzése a megnövekedett információbiztonásgi kultúra iránti igény alapján (saját szerkesztés)

Az elemzés 12 releváns szövegrészlet azonosított az érzelemelemelemzés segítségével, amelyek között 3 negatív, 4 semleges és 5 pozitív érzelmekből állt. Ez a megoszlás arra utal, hogy az információbiztonsággal kapcsolatos kihívások vegyes fogadtatásban részesülnek.

A Hozzáállás - Bevezetés kategória 4 semleges és 1 negatív érzelmet eredményezett, ami az új biztonsági intézkedések óvatos megközelítését jelzi. A semleges vélemények túlsúlya határozott vélemények hiányára vagy az új biztonsági protokollokkal szembeni kivárásra utalhat. A Motiváció – teljesítmény esetén egy semleges vélemény azt jelezheti, hogy a válaszadók nem látnak szoros kapcsolatot az információbiztonsági intézkedések és a munkahelyi teljesítményük között, vagy bizonytalanok a hatásukat illetően. A Vágy – Bevezetés kategóriában a két semleges érzés itt arra utalhat, hogy bár a válaszadók elismerik a fokozott biztonsági intézkedések szükségességét, nem éreznek erős személyes késztetést a bevezetésükre. A Vágy – Elégedettség kategóriában található két semleges

vélemény ezen a területen azt jelezheti, hogy a válaszadók nem különösebben elégedettek vagy elégedetlenek a jelenlegi vagy javasolt biztonsági intézkedésekkel. Egy semleges és egy negatív vélemény a Vágy - Megtartás kategóriában azt jelentheti, hogy kihívást jelenthet az információbiztonsági gyakorlatok iránti hosszú távú elkötelezettség fenntartása. A negatív érzelmek a biztonsági követelmények folyamatos jellegével kapcsolatos frusztrációt tükrözhetik.

Ezek az eredmények hangsúlyozzák, hogy a technológiai fejlődésre reagálva árnyalt megközelítésre van szükség a magasabb szintű információbiztonsági kultúrák bevezetéséhez. A semleges és negatív vélemények keveredése, különösen a vágyakozással és a hozzáállással kapcsolatos területeken, arra utal, hogy a szervezeteknek kihívásokkal kell szembenézniük az új biztonsági protokollok iránti lelkesedés és elkötelezettség előmozdításában. E kihívások kezelése érdekében a szervezeteknek fontolóra kell venniük a kommunikációs stratégiák javítását az új biztonsági intézkedések céljának és előnyeinek tisztázása érdekében. Az átfogó képzés biztosítása is szükséges a tudásbeli hiányosságok áthidalása és a biztonsági gyakorlatok bevezetése iránti bizalom növelése érdekében. Ezek mellett olyan ösztönző struktúrák kialakítására is szükség van, amelyek az információbiztonsági megfelelés és a személyes és szakmai célok összehangolását szolgálják. Mindazon által az aggodalmak rendszeres értékelésére és kezelésére is gondolni kell a negatív megítélés mérséklése és a folyamatos biztonsági intézkedések fontosságának megerősítése érdekében. A folyamatos tanulás és alkalmazkodás kultúrájának előmozdítása pedig kulcsfontosságú a fejlődő technológiai fenyegetésekkel való lépéstartás érdekében.

Ez az elemzés értékes meglátásokkal szolgál azon szervezetek számára, amelyek a gyors technológiai változások közepette szilárd információbiztonsági kultúrát kívánnak kialakítani. A tanulmányban feltárt mögöttes érzelmek és motivációk kezelésével a szervezetek hatékonyabb stratégiákat dolgozhatnak ki a magas szintű információbiztonsági gyakorlatok bevezetésére és fenntartására.

5. 4. 1. A felhő bevezetésének észlelt eredményei

Az automatikus frissítések és karbantartás a felhőszolgáltatások egyik kulcsfontosságú előnye, amely jelentősen hozzájárul a rendszerek biztonságához és hatékonyságához. A szolgáltatók által rendszeresen végrehajtott frissítések nemcsak csökkentik a biztonsági

rések kialakulásának esélyét, de egyúttal tehermentesítik az IT-részlegeket is. Ez lehetővé teszi, hogy a vállalatok erőforrásaikat más, stratégiailag fontosabb feladatokra összpontosíthassák. A naprakész rendszerek biztosítása révén a felhőszolgáltatások hozzájárulnak a vállalatok versenyképességének fenntartásához és növeléséhez a gyorsan változó technológiai környezetben. Ezek az interjúkban is visszaköszönő tényezők, előnyök.

„A felhőszolgáltatók gondoskodnak a rendszeres frissítésekről, ami nagy terhet vesz le az IT-részleg válláról" (D6).

„A felhőszolgáltatások egyik nagy előnye, hogy a rendszerek mindig naprakészek, mivel a szolgáltatók rendszeresen gondoskodnak a frissítésekről" (D34).

A többfaktoros hitelesítés (MFA) bevezetése és kötelezővé tétele a felhőszolgáltatásokban jelentős mértékben fokozza a felhasználói fiókok és ezáltal az egész rendszer biztonságát. Az MFA alkalmazása egy további védelmi réteget biztosít a hagyományos jelszavas azonosítás mellett, megnehezítve a jogosulatlan hozzáférést még abban az esetben is, ha a felhasználó jelszava kompromittálódna. Ez a biztonsági intézkedés különösen fontos a felhőalapú szolgáltatások esetében, ahol gyakran érzékeny vállalati adatok és alkalmazások találhatók. Az MFA széles körű alkalmazása nemcsak a felhasználók biztonságérzetét növeli, de a vállalatok számára is biztonságosabb működési környezetet teremt a digitális térben. Az MFA vonatkozásában az alábbi interjúrészletek említendők meg:

„A kétfaktoros hitelesítés használata kötelezővé vált, ami megerősíti a rendszer védelmét" (D6).

„Az MFA kötelezővé tétele a felhőalapú szolgáltatásokban alapvető lépés volt a biztonság növelésében" (D18).

A felhőalapú biztonsági megoldások, különösen az ISO 27001 és NIS 2 szabványoknak való megfelelés, jelentős hatással vannak a vállalatok működésére és piaci pozíciójára. Ezek a szabványok nemcsak a belső folyamatok optimalizálását és a biztonsági szint emelését szolgálják, hanem gyakran üzleti előnyt is jelentenek a partnerkapcsolatokban. Ahogy az egyik interjúalany megjegyezte:

„Az ISO 27001 és NIS 2 megfelelőség üzleti előnyként jelenik meg, sőt, gyakran alapfeltétel a partnerek részéről" (D3).

Ez arra utal, hogy a megfelelőség már nem csupán opció, hanem sok esetben elengedhetetlen követelmény az üzleti kapcsolatok kialakításához és fenntartásához.

„A nagyobb ügyfelek rendszeresen kérnek be információt arról, hogy milyen biztonsági szabványoknak felelünk meg, és ez befolyásolja a döntéseiket" (D8).

A felhő további előnye a rugalmasság és a hozzáférhetőség, ami különösen fontos a modern munkakörnyezetben. A távoli munkavégzés lehetősége és az adatok bárhonnan történő elérése jelentősen növeli a vállalatok hatékonyságát. Ahogy egy másik szakértő kiemelte:

„A felhő rugalmassága elengedhetetlen a modern munkavégzéshez" (D16).

„A felhőbiztonság megfelelő alkalmazása lehetővé teszi, hogy a kritikus rendszerekhez mindig hozzáférjünk, még akkor is, ha a helyi infrastruktúra nem elérhető" (D6).

Ez a rugalmasság nem csak a mindennapi működésben jelent előnyt, hanem kritikus helyzetekben is kulcsfontosságú lehet. A megfelelően alkalmazott felhőbiztonsági megoldások biztosítják, hogy a vállalatok kritikus rendszereikhez mindig hozzáférjenek.

Tézis 4 Az interjúkban nem azonosíthatóak érzelmi mintázatok a felhőszolgáltatásokkal kapcsolatban. A szentiment elemzés nem mutatott egyértelműen kimutatható hatást a kkv-k esetében a felhő igénybevételének vizsgálatára. [301]

A következő táblázatban (14. táblázat) összegzésként bemutatom a kutatásom előfeltevéseit és eredményként definiált téziseket.

N	Kutatási kérdés	Előfeltevés	Módszertan	Tézis
1	Milyen tényezők befolyásolják a felhőszolgáltatás használatát a kkv-k esetében?	Nem csak gazdasági tényezők befolyásolják a felhőszolgáltatás használatát.	kódolás	A kkv vezetőivel folytatott interjúk szövegelemzése során azonosítottam a felhőszolgáltatás bevezetésének releváns akadályait, melyek felismerése hozzájárul a felhőszolgáltatás bevezetés hatékony leküzdéséhez.
2	Hogyan látják a felhőszolgáltatók és a kkv-k az információbiztonságot és a felhőt?	Az interjúk alapján a kis- és középvállalkozások, valamint a szolgáltatók vonatkozásában tartalmi hasonlóságok és eltérések azonosíthatók az információbiztonság és a felhőszolgáltatások megjelenéséhez kapcsolódó kódok értelmezési dimenzióiban.	kódgyakoriság	Az interjúk alapján a kis- és középvállalkozások, valamint a szolgáltatók vonatkozásában tartalmi hasonlóságok és eltérések azonosíthatók az információbiztonság és a felhőszolgáltatások megjelenéséhez kapcsolódó kódok értelmezési dimenzióiban.
3	Milyen összefüggések fedezhetők fel a kkv-knál az információbiztonságot és a felhőt befolyásoló tényezők között?	A kkv-knál meghatározhatók a kódok hálózatával az információbiztonságot és a felhő megjelenését, használatát befolyásoló tényezők**.**	kontextus-elemzés - kódhálózat	A kutatásban kódhálózati elemzéssel meghatároztam és bizonyítottam, hogy a kkv-k információbiztonságát a biztonsági kihívások, szervezeti és technológiai tényezők, míg a felhőhasználatot a motivációk, előnyök, akadályok és elvárások együttesen befolyásolják
4	Milyen érzelmi mintázatok jelennek meg a felhőszolgáltatásokkal kapcsolatos interjúkban?	Az interjúalanyok gyakran kettős érzelmi viszonyulással élnek (egyszerre vonzó és félelmetes a technológia).	szentiment	Az interjúkban nem azonosíthatóak érzelmi mintázatok a felhőszolgáltatásokkal kapcsolatban. A szentiment elemzés nem mutatott egyértelműen kimutatható hatást a kkv-k esetében a felhő igénybevételének vizsgálatára

14. táblázat A kutatási kérdések, előfeltevések, alkalmazott módszertan és tézisek összefoglalója (saját szerkesztés)

6. Új tudományos eredmények

A kkv vezetőivel folytatott interjúk szövegelemzése során azonosítottam a felhőszolgáltatás bevezetésének releváns akadályait, melyek felismerése hozzájárul a felhőszolgáltatás bevezetés hatékony leküzdéséhez. [14, 83, 291-293]

A felhőtechnológiák bevezetését számos szervezeti kihívás befolyásolja, köztük a reaktív döntéshozatal, amely gyakran múltbeli eseményeken vagy külső nyomáson alapul, és eltérhet a hosszú távú céloktól. A gyors technológiai fejlődés szaktudásbeli hiányosságokat tár fel, így a szervezetek kénytelenek fejleszteni a belső kapacitásaikat vagy versenyezni a piacon a szűkös szakértői erőforrásokért. A döntéshozók gyakran az azonnali költségmegtakarítást részesítik előnyben, miközben alábecsülik a hosszú távú biztonsági beruházások szükségességét. A fokozatos bevezetés ugyan óvatosnak tűnhet, de szervezetlen rendszerekhez vezethet, ha hiányzik a megfelelő koordináció. Végül a technikai kérdések mögött meghúzódó pszichológiai és kulturális bizalomhiány is akadályozza az elfogadást, ezért ezek kezelése kulcsfontosságú a siker érdekében.

Tézis 2 Az interjúk alapján a kis- és középvállalkozások, valamint a szolgáltatók vonatkozásában tartalmi hasonlóságok és eltérések azonosíthatók az információbiztonság és a felhőszolgáltatások megjelenéséhez kapcsolódó kódok értelmezési dimenzióiban. [14, 292]

A felhőszolgáltatók és a kkv-k nézőpontjai között jelentős különbségek rajzolódnak ki: míg a szolgáltatók inkább a szervezeti, kulturális és tudásbeli akadályokra fókuszálnak, a felhasználók a gyakorlati előnyöket és működési szempontokat emelik ki. A szolgáltatók sokkal élesebben érzékelik a tudáshiányt, a kulturális kihívásokat és a strukturális gátakat, míg a kkv-k ezeket kevésbé tematizálják. Az előnyöket is eltérően értelmezik: a felhasználók azonnali működési haszonként (biztonság, elérhetőség, költséghatékonyság), míg a szolgáltatók technológiai szempontból (skálázhatóság, rugalmasság) közelítik meg. Az elvárások terén a kkv-k az egyszerű használatot és mobilitást tartják fontosnak, míg a szolgáltatók inkább megfelelőségi és biztonsági szempontokra építenek. A motivációk kapcsán is eltérés mutatkozik: a kkv-k az IT-infrastruktúrához és partnerek elvárásaihoz kötődő hajtóerőket említik, míg a szolgáltatók ezeket másként értelmezik, ami kommunikációs és értelmezési eltérésekre utal.

Tézis 3 A kutatásban kódhálózati elemzéssel meghatároztam és bizonyítottam, hogy a kkv-k információbiztonságát a biztonsági kihívások, szervezeti és technológiai tényezők, míg a felhőhasználatot a motivációk, előnyök, akadályok és elvárások együttesen befolyásolják.[14, 292]

Az információbiztonság bevezetése a kkv-knál nem csupán technikai kérdés, hanem összetett, szervezeti, tudásbeli és kommunikációs tényezők által befolyásolt folyamat. A tudáshiány és vezetési problémák gyakran negatív attitűdökhöz és korlátozott ráfordításhoz vezetnek, miközben a belső szabályozás és a külső kommunikáció meghatározza a technológia és biztonság észlelt szerepét. A kvalitatív kódelemzés hálózatai alapján egyértelműen azonosíthatók azok a tényezők, amelyek az információbiztonság alakulását befolyásolják a kkv-k esetében, például a kihívások, a szervezeti működés, a stakeholderek szerepe, valamint az infobiztonságról alkotott vélemény. Hasonlóan, a felhőtechnológia megítélését és alkalmazását is több tényező – kihívások, előnyök, elvárások, akadályok és motivációk – együttesen határozza meg. Ezek a tényezők rendszerszinten észlelhetők, és feltárásuk segíti a biztonsági és technológiai megoldások hatékonyabb bevezetését a kkv-k körében.

Tézis 4 Az interjúkban nem azonosíthatóak érzelmi mintázatok a felhőszolgáltatásokkal kapcsolatban. A szentiment elemzés nem mutatott egyértelműen kimutatható hatást a kkv-k esetében a felhő igénybevételének vizsgálatára. [301]

Az elemzés rámutatott, hogy a felhőszolgáltatások és az információbiztonság szervezeti bevezetését jelentősen befolyásolja a munkavállalók képzésének és tájékoztatásának hiánya, ami negatívan hat az elkötelezettségre, megtartásra és elégedettségre. Az érzelemelemzés során azonosított szövegrészletek túlnyomórészt negatív vagy semleges hangvételűek, ami azt jelzi, hogy a felhasználók óvatos, ambivalens hozzáállással viszonyulnak a technológiai újításokhoz. A motiváció és teljesítmény témakörében megjelenő negatív vélemények a bizalmatlanságot és a pénzügyi prioritásokkal szembeni szkepticizmust tükrözik, míg a semleges nézőpontok lehetőséget kínálnak a tudásfejlesztésre és stratégiai finomhangolásra. Az információbiztonsági intézkedések elfogadottságát különösen befolyásolja a belső kommunikáció hatékonysága, az átlátható célmeghatározás és a megfelelő ösztönzők megléte. Összességében az eredmények azt sugallják, hogy a sikeres digitális és biztonsági átállás érdekében a szervezeteknek

integrált, emberközpontú megközelítést kell alkalmazniuk, amely figyelembe veszi a munkavállalói attitűdöket, érzelmeket és tanulási szükségleteket.

6. 1. Összegzett következtetések

Az információbiztonság és a folyamatos elérhetőség kulcsfontosságú szempontokká váltak a modern vállalatok működésében. A digitális transzformáció és a mesterséges intelligencia térnyerésével a cégek egyre inkább támaszkodnak az informatikai megoldásokra, ami fokozott kockázatokat is jelent. A felhőszolgáltatások rugalmasságot és költséghatékonyságot kínálnak, különösen a kkv-k számára, lehetővé téve számukra a versenyképesség megőrzését. Ugyanakkor a vállalatok gyakran nem rendelkeznek megfelelő információbiztonsági tudatossággal, ami sebezhetővé teheti őket a kibertámadásokkal szemben. A kihívások kezelésére több konkrét lépés is ajánlott. Elsődleges fontosságú az információbiztonsági képzések kiterjesztése a munkavállalók körében, hogy mindenki tisztában legyen a potenciális veszélyekkel és a helyes gyakorlatokkal. A biztonsági intézkedések, mint például a többfaktoros hitelesítés (MFA) és a rendszeres biztonsági mentések bevezetése elengedhetetlen a kockázatok csökkentéséhez. A felhő alkalmazása mellett érdemes részletes kockázatelemzést végezni a digitális átállás előtt, hogy a cégek felmérhessék a szükséges erőforrásokat és felkészülhessenek a változásokra. Végül, a rendszeres biztonsági auditok segíthetnek az intézkedések hatékonyságának ellenőrzésében és a folyamatos fejlesztésben, biztosítva ezzel a vállalat hosszú távú biztonságát és versenyképességét a digitális korban.

A kutatás, valamint az interjúk tartalmi összefoglalását a 15. táblázat mutatja be három gondolalt mentén, mely a TOE modellel mutat átfedést. Az interjúkbókból kirajzolódó koncepciók megfeleltetését a TOE modellel, a táblázat első oszlopa tartalmazza. Az első szempont a kutatásban megtalálható főbb gondolatok, következő az interjúkból visszaköszönő elképzelések, vélemények, harmadik pedig az ezekhez kapcsolódó és mögöttük megbújó magyarázatok.

TOE dimenzió	Főbb gondolatok	Interjúkból kirajzolódó koncepciók	Interjúkból kirajzolódó magyarázatok
Technológia	**Növekvő megfelelési igény:** A vállalatokra nyomást gyakorolnak, hogy a versenyelőny érdekében megfelelő tanúsítványokkal rendelkezzenek.	**Digitális átalakulás:** A digitális megoldások és a felhőszolgáltatások felé való elmozdulás a szervezeti viselkedés és a technológiai integráció szélesebb körű összefonódását jelzi.	**Biztonsági aggályok:** A tapasztalatok azt mutatják, hogy az információbiztonság sérülésétől és a zsarolóvírus-támadásoktól való félelem erős, ami fokozott biztonsági intézkedésekhez vezet.
Technológia	**Hibrid munka és felhőszolgáltatások:** Megnövekedett a felhőszolgáltatások használata és ezáltal javult az adatok hozzáférhetősége, de biztonsági kihívásokat is felvet.		
Szervezet	**Képzési kihívások:** Az alkalmazottak gyakran küzdenek az összetett rendszerekkel, és nincsenek tisztában azzal, hogy a rendszerek hol működnek (felhő vs. on-prem).	**Munkavállalók képzése és alkalmazkodása:** Kiemelésre kerül a hatékony képzési programok szükségessége, amelyek segítik az alkalmazottak alkalmazkodását az új technológiákhoz és rendszerekhez.	**Oktatásra van szükség:** Egyértelműen szükség van az alkalmazottak és a vezetés körében az informatikai- , információbiztonsággal és a felhőszolgáltatásokkal kapcsolatos jobb oktatásra és tudatosságra.
Technológia & Szervezet metszete	**Az adatok hozzáférhetősége:** Az adatokhoz való könnyű hozzáférés a különböző platformokon keresztül jelentős előny, de biztonsági intézkedéseknek is meg kell lenniük.	**A felhő elfogadása és a biztonság:** Egyre több elméleti koncepció jelenik meg a felhő adoptálása és a kapcsolódó biztonsági kockázatok közötti egyensúly kialakítása kapcsán.	**Szkepticizmus a felhőszolgáltatások iránt:** Néhány alany szkeptikusan nyilatkozik a felhőszolgáltatásokkal kapcsolatban, mivel félnek az adatok feletti ellenőrzés elvesztésétől.
Technológia (biztonsági aspektus)	**IT-biztonsági fókusz:** Fokozott hangsúlyt kap az IT-biztonság, a vállalatok a korábbi tapasztalatok miatt többet fektetnek a biztonsági intézkedésekbe.		
Környezet	**Megfelelési nyomás:** tanúsítványok és szabványok megszerzésének igénye a versenyelőny érdekében	-	-

15. táblázat A kutatás főbb tartalmi elemei, interjúkban megtalálható koncepciók (saját szerkesztés)

Az **elméleti tényezők**, amelyek következetesen megjelennek az interjúkban, a következők:

1. **Technológiai Innováció**: A technológiai fejlődés és innováció kulcsszerepet játszik a vállalkozások sikerében. A startupok esetében sokan küzdenek a piaci versenyben, és nem mindenki képes a technológiai újításokat sikeresen alkalmazni.

2. **Információbiztonság**: A felhőalapú megoldások elterjedésével a vállalatok egyre inkább aggódnak az adataik védelme miatt. A biztonsági intézkedések, mint például a többfaktoros azonosítás és a jelszókezelés, kiemelt fontosságúak.

3. **Költséghatékonyság**: A felhőszolgáltatások használata lehetővé teszi a vállalatok számára, hogy csökkentsék a tőkeberuházásokat, és rugalmasabb költségmodelleket alkalmazzanak, amelyek lehetővé teszik a költségek tervezését.

4. **Digitális Átalakulás**: A vállalatoknak alkalmazkodniuk kell a digitális tér követelményeihez, és a digitális eszközök használata elengedhetetlen a versenyképesség megőrzéséhez.

5. **Felhőalapú Szolgáltatások**: A felhőszolgáltatások előnyei, mint a skálázhatóság és a rugalmasság, egyre inkább vonzóvá válnak a kis- és középvállalkozások számára.

6. **Képzés és Tudatosság**: Az IT biztonsági tudatosság és a megfelelő képzés elengedhetetlen a felhasználók számára, hogy megértsék a technológiai megoldások használatát és a biztonsági kockázatokat.

7. **Versenyelőny**: A vállalatoknak folyamatosan figyelniük kell a piaci trendeket és a versenytársakat, hogy fenntartsák a versenyelőnyüket.

8. **Hibrid Megoldások**: A nagyvállalatok gyakran hibrid megoldásokat alkalmaznak, amelyek kombinálják a felhő- és on-premise rendszereket, hogy maximalizálják a biztonságot és a hatékonyságot.

Ezek a koncepciók összefonódnak, és a kkv-knak figyelembe kell venniük őket a stratégiai döntéshozatal során, hogy sikeresen navigáljanak a technológiai és piaci kihívások között.

A fogalmak közötti kapcsolatok az alábbi tényezők miatt jelentősen eltérhetnek a különböző kontextusokban:

1. **Kontextuális relevancia:** A fogalom fontossága és jelentése változhat a környező kontextus alapján. Például egy műszaki környezetben az olyan kifejezések, mint a felhőszolgáltatás, felhőtechnológia vagy az információbiztonság olyan sajátos jelentéstartalommal bírhatnak, amely eltérhet az üzleti vagy alkalmi beszélgetésekben használt jelentésüktől.

2. **Felhasználói tapasztalat és ismeret:** A felhasználók gyakran másként találkoznak a fogalmakkal az ismereteik és tapasztalatuk alapján. Egy tipikus felhasználónak például nem feltétlenül kell megértenie az adattárolás technikai részleteit, de tudnia kell, hogyan férhet hozzá az adatokhoz és hogyan használhatja azokat hatékonyan. Ez rávilágít arra, hogy a felhasználó megértési szintjének megfelelő, személyre szabott kommunikációra van szükség.

3. **Kommunikáció és oktatás:** A hatékony kommunikáció kulcsfontosságú a különböző kontextusok közötti átmenet során. Például egy rendszerátállás során az érdekelt feleket úgy kell tájékoztatni a változásokról, hogy az a mindennapi feladataikhoz kapcsolódjon. Ehhez világos magyarázatra van szükség, amely kerüli a szakzsargont, és a gyakorlati következményekre összpontosít.

4. **A szakértelem változatossága:** A különböző érdekeltek eltérő szintű szakértelemmel rendelkezhetnek, ami befolyásolja a fogalmak megítélését. Az informatikai szakemberek például a végfelhasználókhoz képest mélyebben ismerhetik a biztonsági protokollokat, ami eltérő oktatási és kommunikációs megközelítéseket tesz szükségessé.

5. **Kulturális és szervezeti tényezők:** Egy szervezet kultúrája befolyásolhatja a fogalmak és technológiák megértését és alkalmazását. Egyes szervezetekben nagy hangsúlyt fektethetnek az innovációra és a technológia átvételére, míg más szervezetekben ellenállás tapasztalható a változásokkal szemben, ami befolyásolja, hogy az új fogalmak, technológiák hogyan épülnek be a meglévő keretekbe.

6. **Szabályozási és megfelelési megfontolások:** Bizonyos kontextusokban, mint például az egészségügy vagy a pénzügy, a fogalmak közötti kapcsolatokat

nagymértékben befolyásolják a szabályozási követelmények. Ez meghatározhatja az adatok kezelésének, megosztásának és védelmének módját, ami az olyan fogalmak összetettebb megértéséhez vezet, mint az adatvédelem és az információbiztonság.

7. **Technológiai fejlődés:** A technológia fejlődésével a fogalmak közötti kapcsolatok is fejlődnek. A felhőszolgáltatások térhódítása például átalakította a szervezetek adattárolásra és biztonságra vonatkozó nézeteit, ami új keretrendszerekhez és gyakorlatokhoz vezetett, amelyek újra fogalmazzák ezeket a folyamatokat, fogalmakat.

8. **Interdiszciplináris kapcsolatok:** A fogalmak gyakran keresztezik a különböző területeket, ami változatos értelmezésekhez vezet. Például az „adat” fogalmát az informatika, a marketing és a megfelelés szemüvegén keresztül lehet vizsgálni, és mindegyik egyedi meglátásokat és következményeket kínál.

Összefoglalva, a fogalmak közötti kapcsolatok nem statikusak, hanem dinamikusak, és a kontextus, a felhasználói tapasztalatok, a kommunikációs stratégiák, a szakértelem szintjei, a szervezeti kultúra, a szabályozási keretek, a technológiai fejlődés és az interdiszciplináris kapcsolatok befolyásolják őket. Ezeknek a változatoknak a megértése kulcsfontosságú a fogalmak hatékony kommunikációjához és különböző környezetekben történő megvalósításához.

7. Az eredmények gyakorlati hasznosíthatósága

A felhő stratégiai szintű bevezetésének megkönnyítése a kkv-k számára gyakorlati jelentőségét az adja, hogy a felhő javíthatja a működési hatékonyságot, a skálázhatóságot és az adatok hozzáférhetőségét, miközben olyan kihívásokat is kezel, mint az információbiztonság és a meglévő rendszerekkel való integráció. A kkv-k vezetőinek és döntéshozóinak több kulcsfontosságú kérdést kell mérlegelniük, melyek a felhő bevezetésének szükségességére is ki kell térnie, illetve az előnyök és a teljesítménynövekedés mérhetőségére is.

A felhő bevezetését olyan érzékelt előnyök mozgatják, mint a tranzakciós költségek csökkenése, a szolgáltatás minőségének javítása és az adatok jobb hozzáférhetősége [302]. Ezek az előnyök jobb gazdasági teljesítményhez és versenypozícióhoz vezethetnek [303, 304].

A felhő bevezetésének szükségessége olyan tényezőktől függ, mint a szervezeti felkészültség, a felsővezetés támogatása és az észlelt hasznosság [303, 305]. A kkv-knak fel kell mérniük sajátos igényeiket és a felhőtechnológiák bevezetésére való felkészültségüket, figyelembe véve mind az előnyöket, mind a lehetséges kihívásokat, például az információbiztonságot és az erőforráskorlátozásokat [302, 306].

A kkv-k számára a felhő stratégiai szintű bevezetésének elősegítése kulcsfontosságú ahhoz, hogy kihasználhassák a jobb működési hatékonyság és gazdasági teljesítmény előnyeit. A döntéshozóknak gondosan fel kell mérniük a potenciális előnyöket, konkrét mérőszámokon keresztül mérniük kell a javulást, és fel kell mérniük a szervezeti felkészültséget, hogy meghatározzák a felhő bevezetésének szükségességét. E megfontolások figyelembevétele segíthet a kkv-knak abban, hogy megalapozott döntéseket hozzanak a felhő üzleti tevékenységükbe történő integrálásáról.

8. További kutatási irányok

A kutatásom folytatásaként egy kezdeti kérdéscsomagot tervezek összeállítani, ami a kkv-k számára segíthet a technológiai fejlődés megkezdésében és a felhőmegoldások megfelelő bevezetésében. A javaslat az interjúkból levont tanulságokból és tapasztalataiból, valamint a szakemberekkel, szolgáltatókkal folytatott beszélgetésekből indul majd ki. A kkv technológiai fejlődésének hatékony előmozdítása érdekében elengedhetetlen egy jól strukturált lépéssorozat kialakítása, amely a stratégiai célok meghatározásától kezdve a technológiai megoldások implementálásáig terjed. Az alábbiakban bemutatott folyamat kiindulópontot nyújt a kkv-k számára, hogy sikeresen integrálják az informatikai újításokat a vállalati működésükbe. A felhő bevezetése és működtetése a kkv-knál több kulcsfontosságú lépést és mérföldkövet foglal magában:

1-2. Értékelés és tervezés; szolgáltató kiválasztása

A felhőre való átállás első lépése a jelenlegi IT-infrastruktúra és az üzleti igények felmérése, majd a különböző felhőmegoldások (IaaS, PaaS, SaaS) azonosítása. Ezt követi a célkitűzések és az elvárt eredmények meghatározása, amelyekre építve kidolgozható egy átfogó migrációs stratégia. A stratégia megvalósításának egyik kulcseleme a megfelelő szolgáltató kiválasztása: ebben fontos szerepet játszik a potenciális felhőszolgáltatók összehasonlítása, a biztonsági, megfelelőségi és adatvédelmi szempontok értékelése, az árképzési modellek és SLA-k elemzése, majd annak eldöntése, hogy melyik szolgáltató felel meg leginkább a vállalkozás igényeinek.

3-4. Kísérleti/pilot projekt és Adatmigráció és integráció

Az éles átállás előtt érdemes egy kisebb léptékű pilot projektet indítani, amelyben egy kevésbé kritikus alkalmazás vagy folyamat migrációja zajlik. Ez lehetőséget ad arra, hogy ellenőrizzük a teljesítményt, a funkcionalitást és az integrációs lehetőségeket, majd a visszajelzések alapján azonosítsuk a szükséges fejlesztési irányokat. A sikeres teszt után következhet az adatmigráció és a meglévő rendszerekkel való integráció. Ehhez elengedhetetlen az adatok előkészítése – tisztítás, formázás és priorizálás –, majd a szakaszos migrációs terv végrehajtása, amely biztosítja a zökkenőmentes átállást.

5. Személyzeti képzés és változásmenedzsment

A technikai folyamat mellett kulcsszerepe van a szervezeti felkészítésnek is. A munkatársak képzését célzott programok, workshopok és gyakorlati foglalkozások segíthetik, amelyek nemcsak az új technológiák elsajátítását támogatják, hanem a változással kapcsolatos aggályok kezelését és az új munkafolyamatok bevezetését is.

6-7. Teljes körű megvalósítás és Biztonság és megfelelés

A teljes körű megvalósítás szakaszában a fennmaradó alkalmazások és adatok áttelepítése zajlik, miközben folyamatosan figyelni kell a teljesítményt, optimalizálni az erőforrások elosztását, és biztosítani a biztonsági mentési és katasztrófa-helyreállítási megoldások működését. Ezzel párhuzamosan kiemelt fontosságú a biztonság és megfelelőség: a felhőspecifikus biztonsági intézkedések bevezetése, az iparági előírásoknak való megfelelés, a hozzáférés- és identitáskezelés kialakítása, valamint a rendszeres auditálás és irányelvfrissítés.

8-9. Teljesítményfelügyelet és optimalizálás; Forgalmazói menedzsment

Az üzemeltetés során a teljesítményfelügyelet és optimalizálás folyamatos feladat. Ennek alapját a monitoring eszközök és dashboardok adják, amelyek segítségével nyomon követhetők a kulcsfontosságú mutatók. A hangsúly itt az erőforrások és költségek optimalizálásán, valamint a szolgáltatás minőségének és hatékonyságának javításán van. Ehhez szorosan kapcsolódik a szolgáltatóval való együttműködés: elengedhetetlen a világos kommunikáció, az SLA-k és teljesítménymutatók rendszeres áttekintése, a szerződéses feltételek időbeni aktualizálása, valamint az esetleges problémák gyors kezelése.

10. Folyamatos fejlesztés és innováció

Végül fontos megjegyezni, hogy a felhőstratégia nem statikus, hanem folyamatosan fejlődő terület. A sikeres működéshez szükséges az új technológiák és szolgáltatások nyomon követése, az automatizálási és optimalizálási lehetőségek kihasználása, valamint az innováció és kísérletezés ösztönzése a szervezeten belül.

Az előbb felvázolt lépéseket, illetve annak folyamatábráját a 6.sz melléklet tartalmazza.

Kapcsolatok és összefüggések

A felmérési és tervezési szakasz minden további lépést megalapoz, biztosítva az üzleti célkitűzésekkel való összhangot. A szállító kiválasztása közvetlenül befolyásolja a kísérleti/pilot projekt és a teljes körű megvalósítás sikerét. A kísérleti/pilot projekt értékes

betekintést nyújt a végrehajtási stratégia és a képzési programok finomításához. Az adatmigráció és -integráció szorosan kapcsolódik a biztonsági és megfelelőségi intézkedésekhez. A személyzet képzése és a változások kezelése döntő fontosságú a teljes körű bevezetés és a folyamatos teljesítmény-ellenőrzés sikeréhez. A teljesítményfigyelés és -optimalizálás a folyamatos fejlesztés és innováció részét képezi, és így a folyamatos fejlesztés körforgása jön létre. A szállítói menedzsment összekapcsolódik a biztonsággal és a megfelelőséggel, valamint a teljesítményfigyeléssel és -optimalizálással. Ezt a folyamatot követve és a lépések közötti összefüggések megértésével a kkv-k hatékonyan tudják megvalósítani a felhőszolgáltatásokat, javítva működési hatékonyságukat, skálázhatóságukat és versenyképességüket a piacon.

A felhő kkv-kban történő bevezetése több, egymással összefüggő szakaszból álló szisztematikus megközelítést foglal magában. A folyamat a szervezeti igények átfogó felmérésével és egy stratégiai terv kidolgozásával kezdődik. Ez magában foglalja a meglévő rendszerek értékelését, víziók végiggondolását és a megfelelő felhőmegoldások kiválasztását. Ezt követően a felhőszolgáltató kiválasztása alapos kutatással történik, figyelembe véve olyan tényezőket, mint a biztonsági intézkedések, a költséghatékonyság és a szerződéses megállapodások. A körültekintő megközelítés magában foglalja egy kis léptékű tesztüzem indítását, jellemzően egyetlen alkalmazással, a felhőmegoldás hatékonyságának értékelésére. A sikeres tesztelést követően megkezdődik az adatmigráció, amely magában foglalja az adatok előkészítését és átvitelét a felhőkörnyezetbe, miközben biztosítja a meglévő rendszerekkel való zökkenőmentes integrációt. Ezzel a technikai átállással párhuzamosan elengedhetetlen a személyzet képzése, hogy az alkalmazottak megismerkedjenek az új felhőszolgáltatásokkal, és kezeljék az esetleges aggályokat vagy fenntartásokat. A teljes megvalósítási szakasz az összes alkalmazás fokozatos átállítását jelenti a felhőbe, amelyet folyamatos teljesítmény-ellenőrzés kísér. A robusztus, felhő-specifikus biztonsági intézkedések kialakítása és a vonatkozó szabályozásoknak való megfelelés biztosítása kiemelkedő fontosságú. A felhőalapú erőforrások folyamatos felügyelete és optimalizálása kulcsfontosságú a teljesítmény fokozása és a működési költségek csökkentése szempontjából.

A felhőszolgáltatói kapcsolat hatékony kezelése rendszeres kommunikációval, a megállapodások rendszeres felülvizsgálatával és az esetlegesen felmerülő problémák gyors megoldásával valósul meg. A felhő bevezetéséből származó előnyök maximalizálása érdekében elengedhetetlen, hogy lépést tartsunk a felhőtechnológiák

fejlődésével, és folyamatosan keressük az innovációs lehetőségeket. Ez az átfogó megközelítés az egymással összefüggő lépésekkel megkönnyíti a kkv-k számára a felhőszolgáltatásokra való zökkenőmentes és hatékony átállást.

Kérdéscsomag a folyamat elindításához

A technológiai fejlődés sikeres elindítása érdekében nemcsak egy strukturált lépéssorozatra van szükség, hanem a megfelelő kérdések felvetésére is, amelyek segítenek a vállalat helyzetének és igényeinek mélyebb megértésében. Az alábbi kérdéssor arra szolgál, hogy feltárja a vállalat jelenlegi működését, stratégiáját, valamint a technológiai megoldásokkal és a felhőalapú rendszerekkel kapcsolatos elképzeléseit, kihívásait és lehetőségeit. Ezek a kérdések irányt mutatnak a fejlesztési döntések előkészítéséhez és a folyamatok optimalizálásához. Egy cég jelenlegi állapotának, stratégiai céljainak és potenciális felhő bevezetésének elemzése több okból is kulcsfontosságú. A kkv-k számára a felhőmegoldások bevezetése előtt elengedhetetlen a cég jelenlegi állapotának, stratégiai céljainak és a felhő bevezetésének potenciális hatásának elemzése. Ez a folyamat segít biztosítani, hogy a felhő bevezetése összhangban legyen a szervezet célkitűzéseivel, és maximalizálja annak előnyeit [12, 307].

Először is, a cég jelenlegi állapotának megértése lehetővé teszi a kkv-k számára, hogy azonosítsák azokat a területeket, ahol a felhőszolgáltatások javíthatják a működési hatékonyságot és az innovációt [12]. A stratégiai célok értékelésével a vállalatok a felhőt egyedi igényeikre szabhatják, és konkrét kihívásokat kezelhetnek [12, 307]. Ez az elemzés segít az üzleti teljesítményre gyakorolt potenciális hatások értékelésében is, beleértve a költségelőnyöket, a skálázhatóságot és a katasztrófa utáni helyreállítási képességek javítását [308]. A kkv-k felhőhasználatának javítása érdekében több tényezőt is figyelembe lehet venni. A felsővezetés támogatása, a külső nyomás és a szolgáltatók támogatása jelentős befolyásoló tényezői a felhő bevezetési szándéknak [307]. Emellett a biztonsági aggályok kezelése és a relatív előnyök hangsúlyozása ösztönözheti az elfogadást [308]. A kkv-k a felhőt a nagy adatelemzés előnyeinek kihasználására is felhasználhatják jelentős technológiai és munkaerő-beruházások nélkül [309]. Végül pedig egy átfogó, a szervezeti stratégiai kezdeményezéseket figyelembe vevő megvalósítási keretrendszer kidolgozása segíthet a kkv-knak abban, hogy hatékonyan integrálják a felhőt üzleti tevékenységükbe [308, 310].

A kkv-k számára a digitalizáció jelenlegi helyzetének és stratégiai céljainak megértése elengedhetetlen a megfelelő felhőalapú megoldások azonosításához. Ahogy Hojnik és Huđek [311] javasolja, a különböző méretű vállalatok különböző kihívásokkal szembesülnek, és személyre szabott támogatási mechanizmusokra van szükségük. A jelenlegi állapotuk és céljaik elemzésével a cégek jobban összehangolhatják a felhőimplementációkat sajátos igényeikkel, például az alkalmazottak digitális kompetenciáinak javításával vagy a pénzügyi korlátok kezelésével. A felhő bevezetéséből származó potenciális javulás mérése kulcsfontosságú a beruházások igazolásához és a stratégiai összehangolás biztosításához. Ahogy Snee [312] kiemeli, a szervezeteknek holisztikusan kell megközelíteniük a fejlesztést, a szervezet minden részével foglalkozva. Ez magában foglalja az adatalapú folyamatirányítási rendszerek kialakítását és a fejlesztési kezdeményezések vezetői fejlődési eszközként való felhasználását. Az egyértelmű mérési kritériumok meghatározásával a cégek nyomon követhetik a felhő bevezetésének hatását a stratégiai céljaikra és az általános teljesítményre.

Az előbb elmondottak alapján a következőkben a felhő bevezetése és működtetése kapcsán megválaszolandó kérdések következnek, melyek segítséget nyújthatnak a felhő bevezetése kapcsán.

Stratégia és célok

- Mi a vállalat hosszú távú célja, és hogyan segítheti ezt az IT-fejlődés?
- Hogyan határozható meg a jelenlegi technológiai érettségi szint a szervezetnél?
- Melyek a legfontosabb üzleti kihívások, amelyekben a technológia segíthet megoldani?

Működés és folyamatok

- Milyen jelenlegi IT-megoldásokat használ a szervezet, és ezek milyen mértékben támogatják a napi működést?
- Mennyire rugalmas a szervezet a változásokhoz való alkalmazkodásban?

Felhőmegoldások értékelése

- Mely területeken érzékelhető a felhőalapú szolgáltatások hiánya?
- Hogyan tudnának a felhőmegoldások javítani a hatékonyságon vagy csökkenteni a költségeket?

- Szervezeti és egyéni szinten milyen aggályok vannak a felhőalapú technológiák biztonságával és kontrolljával kapcsolatban?

Vezetői és szervezeti kérdések

- A vezetőség mennyire támogatja az IT-fejlesztéseket és a technológiai innovációt?
- Hogyan lehetne javítani a szervezeti kultúrán, hogy támogassa a technológiai fejlődést?

Tanácsadók és implementáció

- A szervezet rendelkezik-e olyan partnerekkel, akik tudják támogatni az implementálás folyamatát vagy külsős tanácsadóra van szükség?
- Hogyan mérhető a bevezetett technológiai megoldások sikeressége?

Ez a lépéssorozat és kérdéscsomag segíthet strukturáltan megközelíteni a technológiai fejlődés kérdését, miközben figyelembe veszi a kkv-k egyedi kihívásait és lehetőségeit.

Összefoglalva, a sikeres bevezetés biztosításához és a felhőből származó érték maximalizálásához a cég jelenlegi állapotának, stratégiai céljainak és a felhő bevezetésének potenciális előnyeinek átfogó elemzésére van szükség. Ez a megközelítés lehetővé teszi a szervezetek számára, hogy felhőstratégiáikat saját igényeikhez igazítsák, a fejlesztéseket hatékonyan mérjék, és a technológiai fejlesztéseket összehangolják általános üzleti célkitűzéseikkel.

Kutatás lezárásának időpontja: 2025.05.13.

Irodalomjegyzék

Felhasznált kutatások

[1] CHOI, M., LEE, C.: Information Security Management as a Bridge in Cloud Systems from Private to Public Organizations, Sustainability, 2015, 7, (9), pp. 12032-12051

[2] KHAYER, A., JAHAN, N., HOSSAIN, M.N., HOSSAIN, M.Y.: The adoption of cloud computing in small and medium enterprises: a developing country perspective, VINE Journal of Information and Knowledge Management Systems, 2020, 51, (1), pp. 64-91

[3] BELLO, S.A., OYEDELE, L.O., AKINADE, O.O., BILAL, M., DAVILA DELGADO, J.M., AKANBI, L.A., AJAYI, A.O., OWOLABI, H.A.: Cloud computing in construction industry: Use cases, benefits and challenges, Automation in Construction, 2021, 122, pp. 103441

[4] SZERB, L., LAUFENTE, E., RAPPAI, G., KEHL, D.: Összetett indexek gazdaságpolitikai alkalmazása: a Globális Vállalkozói Index, Szigma, 2021, 52, (3), pp. 213-229

[5] BOUNCKEN, R., SCHMITT, F.: SME Family Firms and Strategic Digital Transformation: Inverting Dualisms Related to Overconfidence and Centralization, Journal of Small Business Strategy, 2022, 32, (3)

[6] WANG, S., ZHANG, H.: Digital Transformation and Innovation Performance in Small- and Medium-Sized Enterprises: A Systems Perspective on the Interplay of Digital Adoption, Digital Drive, and Digital Culture, Systems, 2025, 13, (1)

[7] DÖRR, L., FLIEGE, K., LEHMANN, C., KANBACH, D.K., KRAUS, S.: A Taxonomy on Influencing Factors Towards Digital Transformation in SMEs, Journal of Small Business Strategy, 2023, 33, (1)

[8] WANG, S., ASIF, M., SHAHZAD, M.F., ASHFAQ, M.: Data privacy and cybersecurity challenges in the digital transformation of the banking sector, Computers & Security, 2024, 147

[9] ALAHMARI, A., DUNCAN, B.: Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence: '2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)' IEEE, 2020, pp. 1-5

[10] RAWINDARAN, N., JAYAL, A., PRAKASH, E., HEWAGE, C.: Perspective of small and medium enterprise (SME's) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales, International Journal of Information Management Data Insights, 2023, 3, (2)

[11] ARROYABE, M.F., ARRANZ, C.F.A., ARROYABE, I.F.D., ARROYABE, J.C.F.D.: The effect of IT security issues on the implementation of industry 4.0 in SMEs: Barriers and challenges, Technological Forecasting and Social Change, 2024, 199

[12] SEKHAR, K.C., BOOPATHI, S., YUVASRI, B., BATHRINATH, S., PREMNATH, D., RANGANATHAN, L.: Cloud Computing Adoption for Small and Medium Enterprises in Mechanical Engineering, in Ortiz-Rodriguez, F., Leyva-Mederos, A., Tiwari, S., Hernandez-Quintana, A., and J. Martinez-Rodriguez, J. (Eds.): 'Semantic Web Technologies and Applications in Artificial Intelligence of Things' IGI Global Scientific Publishing, 2024, pp. 219–247

[13] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY'S: Final Version of NIST Cloud Computing Definition Published. 2011 Letöltve: 27.01.2022, https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published

[14] BAK, G., REICHER, R.: Challenges of the SMEs in the 21st century, Scientific Papers of Silesian University of Technology – Organization and Management Series, 2022, (166), pp. 31-47

[15] CRESWELL, J.W., POTH, C.N.: Qualitative Inquiry and Research Design: Choosing Among Five Approaches. SAGE Publications, 2016, 4th edn

[16] DENZIN, N.K., LINCOLN, Y.S.: The SAGE handbook of qualitative research. Sage Publisher, 2018, 5th edn

[17] FLICK, U.: An Introduction to Qualitative Research. London: SAGE, 2018, 5th edn

[18] PATTON, M.Q.: Qualitative Research and Evaluation methods. London: SAGE Publications, 2015, 4th edn

[19] PETERS, K., HALCOMB, E.: Interviews in qualitative research, Nurse Res, 2015, 22, (4), pp. 6-7

[20] ALSHAMAILA, Y., PAPAGIANNIDIS, S., LI, F.: Cloud computing adoption by SMEs in the north east of England, Journal of Enterprise Information Management, 2013, 26, (3), pp. 250-275

[21] TEOH, M.F., AHMAD, N.H., ABDUL-HALIM, H., KAN, W.H.: Digital business model innovation among small and medium-sized enterprises (SMEs), Global Business and Organizational Excellence, 2023, 42, (6), pp. 5-18

[22] NYAMWESA, A.: Cloud Computing Technology Adoption: Challenges for SMEs, A Case of Selected SMEs in Tanzania, International Journal of Advanced Business Studies, 2025, 3, (2), pp. 1-12

[23] KHAN, N., AL-YASIRI, A.: Framework for Cloud Computing Adoption: A Roadmap for Smes to Cloud Migration, International Journal on Cloud Computing: Services and Architecture, 2015, 5, (5/6), pp. 01-15

[24] NAGAHAWATTA, R., WARREN, M., SALZMAN, S., LOKUGE, S.: Towards an Understanding of Cloud Computing Adoption in SMEs, International Journal of Cyber Warfare and Terrorism, 2024, 14, (1), pp. 1-13

[25] MOHAMMAD, A., ABBAS, Y.: Key Challenges of Cloud Computing Resource Allocation in Small and Medium Enterprises, Digital, 2024, 4, (2), pp. 372-388

[26] ACOCELLA, I.: The focus groups in social research: advantages and disadvantages, Quality & Quantity, 2011, 46, (4), pp. 1125-1136

[27] LOBE, B., MORGAN, D.L.: Assessing the effectiveness of video-based interviewing: a systematic comparison of video-conferencing based dyadic interviews and focus groups, International Journal of Social Research Methodology, 2020, 24, (3), pp. 301-312

[28] CHARMAZ, K., THORNBERG, R.: The pursuit of quality in grounded theory, Qualitative Research in Psychology, 2020, 18, (3), pp. 305-327

[29] CHARMAZ, K.: The Genesis, Grounds, and Growth of Constructivist Grounded Theory, in Morse, J.M., Bowers, B.J., Charmaz, K., Clarke, A.E., Corbin, J., Porr, C.J., and Stern, P.N. (Eds.): 'Developing Grounded Theory' Routledge, 2021, 2nd edn., pp. 153-187

[30] CHARMAZ, K.: Constructing grounded theory: A practical guide through qualitative analysis. London: SAGE, 2006

[31] GLASER, B., G., STRAUSS., A.L.: The Discovery of Grounded Theory: Strategies for Qualitative Research. Chicago: Aldine Publishing, 1967

[32] KELEMEN-ERDŐS, A., MOLNÁR, A.: Cooperation or Conflict? The Nature of the Collaboration of Marketing and Sales Organizational Units, Economics and Culture, 2019, 16, (1), pp. 58-69

[33] CHARMAZ, K.: The Power of Constructivist Grounded Theory for Critical Inquiry, Qualitative Inquiry, 2016, 23, (1), pp. 34-45

[34] VIESI, D., POZZAR, F., FEDERICI, A., CREMA, L., MAHBUB, M.S.: Energy efficiency and sustainability assessment of about 500 small and medium-sized enterprises in Central Europe region, Energy Policy, 2017, 105, pp. 363-374

[35] JEPPESEN, S.: Enhancing competitiveness and securing equitable development: Can small, micro, and medium-sized enterprises (SMEs) do the trick?, Development in Practice, 2007, 15, (3-4), pp. 463-474

[36] CLARK, D.: Number of small and medium-sized enterprises (SMEs) in the European Union (EU27) from 2008 to 2021, by size. 2021 Letöltve: 02.04.2022, https://www.statista.com/statistics/878412/number-of-smes-in-europe-by-size/

[37] BATRANCEA, L.M.: Determinants of Economic Growth across the European Union: A Panel Data Analysis on Small and Medium Enterprises, Sustainability, 2022, 14, (8)

[38] ROTAR, L.J., PAMIĆ, R.K., BOJNEC, Š.: Contributions of small and medium enterprises to employment in the European Union countries, Economic Research-Ekonomska Istraživanja, 2019, 32, (1), pp. 3302-3314

[39] POLITICAL CAPITAL: In the shadows of coronavirus: Where is Hungarian companies' competitiveness heading? 2021 Letöltve: 15.01.2022, https://visegradinfo.eu/index.php/national-policy-reports/619-what-makes-an-economy-resilient-lessons-learned-after-the-2008-crisis-and-what-it-means-for-today

[40] KSH: A kis- és középvállalkozások jellemzői, 2018. 2018 Letöltve: 15.01.2022, https://www.ksh.hu/docs/hun/xftp/idoszaki/pdf/kkv18.pdf

[41] BRODNY, J., TUTAK, M.: Digitalization of Small and Medium-Sized Enterprises and Economic Growth: Evidence for the EU-27 Countries, Journal of Open Innovation: Technology, Market, and Complexity, 2022, 8, (2)

[42] KÄÄRIÄINEN, J., PUSSINEN, P., SAARI, L., KUUSISTO, O., SAARELA, M., HÄNNINEN, K.: Applying the positioning phase of the digital transformation model in practice for SMEs: toward systematic development of digitalization, International Journal of Information Systems and Project Management, 2021, 8, (4), pp. 24-43

[43] ULAS, D.: Digital Transformation Process and SMEs, Procedia Computer Science, 2019, 158, pp. 662-671

[44] CICEA, C., POPA, I., MARINESCU, C., ȘTEFAN, S.C.: Determinants of SMEs' performance: evidence from European countries, Economic Research-Ekonomska Istraživanja, 2019, 32, (1), pp. 1602-1620

[45] BRODIN, M.: A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises, European Journal for Security Research, 2019, 4, (2), pp. 243-264

[46] BURINSKIENĖ, A., NALIVAIKĖ, J.: Digital and Sustainable (Twin) Transformations: A Case of SMEs in the European Union, Sustainability, 2024, 16, (4)

[47] MANZOOR, J., WALEED, A., JAMALI, A.F., MASOOD, A.: Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs, PLoS One, 2024, 19, (3), pp. e0301183

[48] KLJUČNIKOV, A., MURA, L., SKLENÁR, D.: Information security management in SMEs: factors of success, Entrepreneurship and Sustainability Issues, 2019, 6, (4), pp. 2081-2094

[49] CHAUDHARY, S., GKIOULOS, V., KATSIKAS, S.: A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises, Computer Science Review, 2023, 50

[50] SHETTY, J.P., PANDA, R.: An overview of cloud computing in SMEs, Journal of Global Entrepreneurship Research, 2021, 11, (1), pp. 175-188

[51] ROTHWELL, R., DODGSON, M.: External linkages and innovation in small and medium-sized enterprises, R&D Management, 1991, 21, (2), pp. 125-138

[52] KSH: A vállalkozások teljesítménymutatói kis- és középvállalkozási kategória szerint. 2020 Letöltve: 15.01.2022, https://www.ksh.hu/stadat_files/gsz/hu/gsz0018.html

[53] KSH: A vállalkozások foglakoztatottainak megoszlása kis-és középvállalkozási kategória és régió szerint. 2020 Letöltve: 15.01.2022, https://www.ksh.hu/stadat_files/gsz/hu/gsz0047.html

[54] JI, H., LIN, L., WAN, J., ZANG, J.: Can digital technology adoption promote environmental innovation in small and medium-sized enterprises (SMEs)? Evidence from China, Sci Total Environ, 2024, 955, pp. 176887

[55] CRAGG, P., MILLS, A., SURAWEERA, T.: The Influence of IT Management Sophistication and IT Support on IT Success in Small and Medium-Sized Enterprises, Journal of Small Business Management, 2013, 51, (4), pp. 617-636

[56] CHIBELUSHI, C., COSTELLO, P.: Challenges facing W. Midlands ICT-oriented SMEs, Journal of Small Business and Enterprise Development, 2009, 16, (2), pp. 210-239

[57] SINGH, R.K., LUTHRA, S., MANGLA, S.K., UNIYAL, S.: Applications of information and communication technology for sustainable growth of SMEs in India food industry, Resources, Conservation and Recycling, 2019, 147, pp. 10-18

[58] ROSTAMI, A., SOMMERVILLE, J., WONG, I.L., LEE, C.: Risk management implementation in small and medium enterprises in the UK construction industry, Engineering, Construction and Architectural Management, 2015, 22, (1), pp. 91-107

[59] NEIROTTI, P., RAGUSEO, E., PAOLUCCI, E.: How SMEs develop ICT-based capabilities in response to their environment, Journal of Enterprise Information Management, 2018, 31, (1), pp. 10-37

[60] RYMASZEWSKA, A., HELO, P., GUNASEKARAN, A.: IoT powered servitization of manufacturing – an exploratory case study, International Journal of Production Economics, 2017, 192, pp. 92-105

[61] SHIN, D.-H., JIN PARK, Y.: Understanding the Internet of Things ecosystem: multi-level analysis of users, society, and ecology, Digital Policy, Regulation and Governance, 2017, 19, (1), pp. 77-100

[62] SCHMEINK, A., DRASKOVIC, M., BAUK, S.: Challenges of Tagging Goods in Supply Chains and a Cloud Perspective with Focus on Some Transitional Economies, PROMET - Traffic&Transportation, 2017, 29, (1), pp. 109-120

[63] ONGORI, H., MIGIRO, S.O.: Information and communication technologies adoption in SMEs: literature review, Journal of Chinese Entrepreneurship, 2010, 2, (1), pp. 93-104

[64] SUKUMAR, A., MAHDIRAJI, H.A., JAFARI-SADEGHI, V.: Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors, Risk Anal, 2023, 43, (10), pp. 2082-2098

[65] ALSHARIF, M., MISHRA, S., ALSHEHRI, M.: Impact of Human Vulnerabilities on Cybersecurity, Computer Systems Science and Engineering, 2022, 40, (3), pp. 1153-1166

[66] PAWAR, S., PALIVELA, D.H.: LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs), International Journal of Information Management Data Insights, 2022, 2, (1)

[67] LE, T.D., LE-DINH, T., UWIZEYEMUNGU, S.: Search engine optimization poisoning: A cybersecurity threat analysis and mitigation strategies for small and medium-sized enterprises, Technology in Society, 2024, 76

[68] AL-DOSARI, K., FETAIS, N.: Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach, Electronics, 2023, 12, (17)

[69] NAUDE, M.J., CHIWESHE, N.: A proposed operational risk management framework for small and medium enterprises, South African Journal of Economic and Management Sciences, 2017, 20, (1)

[70] EUROPEAN COMMISSION: Integration of Digital Technology. 2018 Letöltve: 16.01.2022, https://ec.europa.eu/information_society/newsroom/image/document/2018-20/4_desi_report_integration_of_digital_technology_B61BEB6B-F21D-9DD7-72F1FAA836E36515_52243.pdf

[71] EUROSTAT: Digital Intensity by size class of enterprise. 2024 Letöltve: 15.01.2025, https://ec.europa.eu/eurostat/databrowser/view/isoc_e_dii__custom_15190030/default/table?lang=en

[72] LOVE, P.E.D., IRANI, Z., EDWARDS, D.J.: Industry-centric benchmarking of information technology benefits, costs and risks for small-to-medium sized enterprises in construction, Automation in Construction, 2004, 13, (4), pp. 507-524

[73] ACAR, E., KOÇAK, I., SEY, Y., ARDITI, D.: Use of information and communication technologies by small and medium-sized enterprises (SMEs) in building construction, Construction Management and Economics, 2007, 23, (7), pp. 713-722

[74] BOLAT, P., KAYIŞOĞLU, G.: Antecedents and Consequences of Cybersecurity Awareness: A Case Study for Turkish Maritime Sector, Journal of ETA Maritime Science, 2019, 7, (4), pp. 344-360

[75] CONSOLI, D.: Literature Analysis on Determinant Factors and the Impact of ICT in SMEs, Procedia - Social and Behavioral Sciences, 2012, 62, pp. 93-97

[76] OECD: The Digital Transformation of SMEs. Paris: OECD, 2021

[77] EUROPEAN COMMISSION: The Digital Economy and Society Index — Countries' performance in digitisation. 2022 Letöltve: 15.05.2023, https://digital-strategy.ec.europa.eu/en/policies/countries-digitisation-performance

[78] HERMAN, E.: The Influence of ICT Sector on the Romanian Labour Market in the European Context, Procedia Manufacturing, 2020, 46, pp. 344-351

[79] ANTUNES, M., MAXIMIANO, M., GOMES, R., PINTO, D.: Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal, Journal of Cybersecurity and Privacy, 2021, 1, (2), pp. 219-238

[80] FREGAN, B., KOCSIS, I., RAJNAI, Z.: Az IPAR 4.0 és a digitalizáció kockázatai, Műszaki Tudományos Közlemények, 2018, 9, (1), pp. 87-90

[81] OECD: Skills for a Digital World. 2016 Letöltve: 02.02.2023, https://www.oecd.org/els/emp/Skills-for-a-Digital-World.pdf

[82] MIRIGLIANO, M.: New step towards the Digital Decade targets: the policy programme 2030 comes into force. 2023 Letöltve: 02.02.2023, https://digital-skills-jobs.europa.eu/en/latest/news/new-step-towards-digital-decade-targets-policy-programme-2030-comes-force

[83] BAK, G., KELEMEN-ERDŐS, A.: Stressz, opportunizmus és bizalom a szervezeti információs és kommunikációs technológiabiztonság tükrében, Információs Társadalom, 2023, 23, (2)

[84] SOJA, E., SOJA, P.: Fostering ICT use by older workers, Journal of Enterprise Information Management, 2020, 33, (2), pp. 407-434

[85] HARDY, B.W., CASTONGUAY, J.: The moderating role of age in the relationship between social media use and mental well-being: An analysis of the 2016 General Social Survey, Computers in Human Behavior, 2018, 85, pp. 282-290

[86] MAHMOUD, A.B., FUXMAN, L., MOHR, I., REISEL, W.D., GRIGORIOU, N.: "We aren't your reincarnation!" workplace motivation across X, Y and Z generations, International Journal of Manpower, 2020, 42, (1), pp. 193-209

[87] BENNETT, M.M., BEEHR, T.A., IVANITSKAYA, L.V.: Work-family conflict: differences across generations and life cycles, Journal of Managerial Psychology, 2017, 32, (4), pp. 314-332

[88] HARRINGTON, B., VAN DEUSEN, F., FRAONE, J.S., MORELOCK, J.: How Millennials Navigate Their Careers - Young Adult Views on Work, Life and Success, in Editor (Ed.)^(Eds.): 'Book How Millennials Navigate Their Careers - Young Adult Views on Work, Life and Success' Boston College Center for Work & Family, 2015, edn., pp.

[89] SPANOS, G., ANGELIS, L.: The impact of information security events to the stock market: A systematic literature review, Computers & Security, 2016, 58, pp. 216-229

[90] BROUS, P., JANSSEN, M., HERDER, P.: The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations, International Journal of Information Management, 2020, 51, pp. 101952

[91] JACKSON, J.C., CASTELO, N., GRAY, K.: Could a rising robot workforce make humans less prejudiced?, American Psychologist, 2020, 75, (7), pp. 969-982

[92] MCCLURE, P.K.: "You're Fired," Says the Robot, Social Science Computer Review, 2017, 36, (2), pp. 139-156

[93] KOC, M., BARUT, E.: Development and validation of New Media Literacy Scale (NMLS) for university students, Computers in Human Behavior, 2016, 63, pp. 834-843

[94] HELSPER, E.J., SMAHEL, D.: Excessive internet use by young Europeans: psychological vulnerability and digital literacy?, Information, Communication & Society, 2019, 23, (9), pp. 1255-1273

[95] DQ INSTITUTE: What is the DQ Framework?, 2018

[96] ADAMS, N.B.: Digital Intelligence Fostered by Technology , Journal of Technology Studies, 2004, 30, (2), pp. 93-97

[97] EUROPEAN COMMISSION: Digital Education Action Plan (2018- 2020). 2018 Letöltve: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0022&from=EN

[98] LAW, N., WOO, D., WONG, G.: A Global Framework of Reference on Digital Literacy Skills for Indicator 4.4.2, in Editor (Ed.)^(Eds.): 'Book A Global Framework of Reference on Digital Literacy Skills for Indicator 4.4.2' UNESCO, 2018, edn., pp.

[99] RUPIETTA, K., BECKMANN, M.: Working from Home, Schmalenbach Business Review, 2017, 70, (1), pp. 25-55

[100] MADSEN, D.Ø.: The Evolutionary Trajectory of the Agile Concept Viewed from a Management Fashion Perspective, Social Sciences, 2020, 9, (5), pp. 69

[101] BEJAKOVIĆ, P., MRNJAVAC, Ž.: The importance of digital literacy on the labour market, Employee Relations: The International Journal, 2020, 42, (4), pp. 921-932

[102] YOUNG, J.A.: Equipping Future Nonprofit Professionals With Digital Literacies for the 21st Century, Journal of Nonprofit Education and Leadership, 2018, 8, (1), pp. 4-15

[103] BAUER, W., HÄMMERLE, M., SCHLUND, S., VOCKE, C.: Transforming to a Hyper-connected Society and Economy – Towards an "Industry 4.0", Procedia Manufacturing, 2015, 3, pp. 417-424

[104] VAN LAAR, E., VAN DEURSEN, A.J.A.M., VAN DIJK, J.A.G.M., DE HAAN, J.: Determinants of 21st-Century Skills and 21st-Century Digital Skills for Workers: A Systematic Literature Review, SAGE Open, 2020, 10, (1), pp. 1-14

[105] TAN, L.M., LASWAD, F., CHUA, F.: Bridging the employability skills gap: going beyond classroom walls, Pacific Accounting Review, 2021, 34, (2), pp. 225-248

[106] SOULÉ, H., WARRICK, T.: Defining 21st century readiness for all students: What we know and how to get there, Psychology of Aesthetics, Creativity, and the Arts, 2015, 9, (2), pp. 178-186

[107] SILLAT, L.H., TAMMETS, K., LAANPERE, M.: Digital Competence Assessment Methods in Higher Education: A Systematic Literature Review, Education Sciences, 2021, 11, (8), pp. 402

[108] FREY, C.B., OSBORNE, M.A.: The future of employment: How susceptible are jobs to computerisation?, Technological Forecasting and Social Change, 2017, 114, pp. 254-280

[109] VAN LAAR, E., VAN DEURSEN, A.J.A.M., VAN DIJK, J.A.G.M., DE HAAN, J.: The relation between 21st-century skills and digital skills: A systematic literature review, Computers in Human Behavior, 2017, 72, pp. 577-588

[110] LISSITSA, S., CHACHASHVILI-BOLOTIN, S., BOKEK-COHEN, Y.A.: Digital skills and extrinsic rewards in late career, Technology in Society, 2017, 51, pp. 46-55

[111] MIRRA, N., GARCIA, A.: In Search of the Meaning and Purpose of 21st-Century Literacy Learning: A Critical Review of Research and Practice, Reading Research Quarterly, 2020, 56, (3), pp. 463-496

[112] SIDDIQ, F., GOCHYYEV, P., WILSON, M.: Learning in Digital Networks – ICT literacy: A novel assessment of students' 21st century skills, Computers & Education, 2017, 109, pp. 11-37

[113] VOOGT, J., ROBLIN, N.P.: A comparative analysis of international frameworks for 21stcentury competences: Implications for national curriculum policies, Journal of Curriculum Studies, 2012, 44, (3), pp. 299-321

[114] GILSTER, P.: Digital literacy. New York: Wiley Computer Pub, 1997

[115] BAWDEN, D.: Origins and concepts of digital literacy, in Lankshear, C., and Knobel, M. (Eds.): 'Digital Literacies: Concepts, Policies and Practices' Peter Lang Inc, 2008, pp. 17-32

[116] PANGRAZIO, L., GODHE, A.-L., LEDESMA, A.G.L.: What is digital literacy? A comparative review of publications across three language contexts, E-Learning and Digital Media, 2020, 17, (6), pp. 442-459

[117] DAWSON, J., THOMSON, R.: The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance, Front Psychol, 2018, 9, pp. 744

[118] BAK, G., KELEMEN-ERDŐS, A.: Információbiztonság-tudatosság az Y generáció szemszögéből, kvalitatív megközelítés alapján, Hadmérnök, 2022, 17, (3), pp. 81-95

[119] EVANS, M., MAGLARAS, L.A., HE, Y., JANICKE, H.: Human behaviour as an aspect of cybersecurity assurance, Security and Communication Networks, 2016, 9, (17), pp. 4667-4679

[120] WERLINGER, R., FURNELL, S.M., HAWKEY, K., BEZNOSOV, K.: An integrated view of human, organizational, and technological challenges of IT security management, Information Management & Computer Security, 2009, 17, (1), pp. 4-19

[121] STEWART, H., JÜRJENS, J.: Information security management and the human aspect in organizations, Information & Computer Security, 2017, 25, (5), pp. 494-534

[122] KOMATSU, A., FURNELL, S.M., TAKAGI, D., TAKEMURA, T.: Human aspects of information security, Information Management & Computer Security, 2013, 21, (1), pp. 5-15

[123] EVANS, M.G., HE, Y., YEVSEYEVA, I., JANICKE, H.: Published incidents and their proportions of human error, Information & Computer Security, 2019, 27, (3), pp. 343-357

[124] UCHENDU, B., NURSE, J.R.C., BADA, M., FURNELL, S.: Developing a cyber security culture: Current practices and future needs, Computers & Security, 2021, 109, pp. 102387

[125] DJAJADIKERTA, H.G., RONI, S.M., TRIREKSANI, T.: Dysfunctional information system behaviors are not all created the same: Challenges to the generalizability of security-based research, Information & Management, 2015, 52, (8), pp. 1012-1024

[126] D'ARCY, J., HERATH, T., SHOSS, M.K.: Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective, Journal of Management Information Systems, 2014, 31, (2), pp. 285-318

[127] HWANG, I., KIM, D., KIM, T., KIM, S.: Why not comply with information security? An empirical approach for the causes of non-compliance, Online Information Review, 2017, 41, (1), pp. 2-18

[128] HUGHES-LARTEY, K., LI, M., BOTCHEY, F.E., QIN, Z.: Human factor, a critical weak point in the information security of an organization's Internet of things, Heliyon, 2021, 7, (3), pp. e06522

[129] DALLAT, C., SALMON, P.M., GOODE, N.: Risky systems versus risky people: To what extent do risk assessment methods consider the systems approach to accident causation? A review of the literature, Safety Science, 2019, 119, pp. 266-279

[130] MAYER, P., KUNZ, A., VOLKAMER, M.: Reliable Behavioural Factors in the Information Security Context. Proc. Proceedings of the 12th International Conference on Availability, Reliability and Security, Reggio Calabria, Italy2017 pp. 1-10

[131] BAK, G., KISS, S.: A biztonságtudatosság szisztematikus szakirodalmi áttekintése, Hadmérnök, 2021, 16, (4), pp. 85-99

[132] BAK, G., VELENCEI, J.: Information security awareness vs cyber security awareness vs internet safety awareness, in Fehér-Polgár, P., Keszthelyi, A., and Szikora, P. (Eds.): 'MEB — 20th International Conference on Management, Enterprise, Benchmarking Proceedings (MEB 2022)' Óbuda University Keleti Károly Faculty of Business and Management, 2022, pp. 47-55

[133] BULGURCU, B., CAVUSOGLU, H., BENBASAT, I.: Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness, MIS Quarterly, 2010, 34, (3), pp. 523-548

[134] D'ARCY, J., HOVAV, A., GALLETTA, D.: User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach, Information Systems Research, 2009, 20, (1), pp. 79-98

[135] TSOHOU, A., KARYDA, M., KOKOLAKIS, S., KIOUNTOUZIS, E.: Managing the introduction of information security awareness programmes in organisations, European Journal of Information Systems, 2017, 24, (1), pp. 38-58

[136] SPEARS, J., BARKI, H.: User Participation in Information Systems Security Risk Management, MIS Quarterly, 2010, 34, (3), pp. 503-522

[137] LOWRY, P.B., DINEV, T., WILLISON, R.: Why security and privacy research lies at the centre of the information systems (IS) artefact: proposing a bold research agenda, European Journal of Information Systems, 2018, 26, (6), pp. 546-563

[138] SIPONEN, M., ADAM MAHMOOD, M., PAHNILA, S.: Employees' adherence to information security policies: An exploratory field study, Information & Management, 2014, 51, (2), pp. 217-224

[139] SOOMRO, Z.A., SHAH, M.H., AHMED, J.: Information security management needs more holistic approach: A literature review, International Journal of Information Management, 2016, 36, (2), pp. 215-225

[140] PARSONS, K., CALIC, D., PATTINSON, M., BUTAVICIUS, M., MCCORMAC, A., ZWAANS, T.: The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies, Computers & Security, 2017, 66, pp. 40-51

[141] CURRY, S.: Boards Should Take Responsibility for Cybersecurity. Here's How to Do It. 2017 Letöltve: 19.05.2022, https://hbr.org/2017/11/boards-should-take-responsibility-for-cybersecurity-heres-how-to-do-it

[142] JAEGER, J.: Human error, not hackers, cause most data breaches, Compliance Week, 2013, 10, (110), pp. 56-57

[143] THOMPSON, N., MCGILL, T.J., WANG, X.: "Security begins at home": Determinants of home computer and mobile device security behavior, Computers & Security, 2017, 70, pp. 376-391

[144] TSAI, H.-Y.S., JIANG, M., ALHABASH, S., LAROSE, R., RIFON, N.J., COTTEN, S.R.: Understanding online safety behaviors: A protection motivation theory perspective, Computers & Security, 2016, 59, pp. 138-150

[145] DUPUIS, M.J., CROSSLER, R.E., ENDICOTT-POPOVSKY, B.: Measuring the Human Factor in Information Security and Privacy: '2016 49th Hawaii International Conference on System Sciences (HICSS)' IEEE, 2016, pp. 3676-3685

[146] TU, Z., TUREL, O., YUAN, Y., ARCHER, N.: Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination, Information & Management, 2015, 52, (4), pp. 506-517

[147] MYLONAS, A., KASTANIA, A., GRITZALIS, D.: Delegate the smartphone user? Security awareness in smartphone platforms, Computers & Security, 2013, 34, pp. 47-66

[148] ALBRECHTSEN, E.: A qualitative study of users' view on information security, Computers & Security, 2007, 26, (4), pp. 276-289

[149] BOSS, S.R., KIRSCH, L.J., ANGERMEIER, I., SHINGLER, R.A., BOSS, R.W.: If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security, European Journal of Information Systems, 2009, 18, (2), pp. 151-164

[150] CROSSLER, R.E.: Protection Motivation Theory: Understanding Determinants to Backing Up Personal Data: '2010 43rd Hawaii International Conference on System Sciences' IEEE, 2010, pp. 1-10

[151] BURNS, A.J., POSEY, C., ROBERTS, T.L., BENJAMIN LOWRY, P.: Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals, Computers in Human Behavior, 2017, 68, pp. 190-209

[152] KRITZINGER, E., SMITH, E.: Information security management: An information security retrieval and awareness model for industry, Computers & Security, 2008, 27, (5-6), pp. 224-231

[153] LIANG, H., XUE, Y.: Avoidance of Information Technology Threats: A Theoretical Perspective, MIS Quarterly, 2009, 33, (1), pp. 71-90

[154] PAHNILA, S., SIPONEN, M., MAHMOOD, A.: Employees' Behavior towards IS Security Policy Compliance: '2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)' IEEE, 2007, pp. 156b-156b

[155] RHEE, H.-S., RYU, Y.U., KIM, C.-T.: Unrealistic optimism on information security management, Computers & Security, 2012, 31, (2), pp. 221-232

[156] SIPONEN, M., VANCE, A.: Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations, European Journal of Information Systems, 2014, 23, (3), pp. 289-305

[157] WOON, I., TAN, G.-W., LOW, R.: A Protection Motivation Theory Approach to Home Wireless Security: 'Proceedings of the International Conference on Information Systems' AIS, 2005, pp. 367-380

[158] FLOYD, T., GRIECO, M., REID, E.F.: Mining hospital data breach records: Cyber threats to U.S. hospitals: '2016 IEEE Conference on Intelligence and Security Informatics (ISI)' IEEE, 2016, pp. 43-48

[159] RAHMAN, T., ROHAN, R., PAL, D., KANTHAMANON, P.: Human Factors in Cybersecurity: A Scoping Review: 'The 12th International Conference on Advances in Information Technology (IAIT2021)' ACM, 2021, pp. 1-11

[160] ANI, U.D., HE, H., TIWARI, A.: Human factor security: evaluating the cybersecurity capacity of the industrial workforce, Journal of Systems and Information Technology, 2019, 21, (1), pp. 2-35

[161] TRIPLETT, W.J.: Addressing Human Factors in Cybersecurity Leadership, Journal of Cybersecurity and Privacy, 2022, 2, (3), pp. 573-586

[162] EVANS, M., HE, Y., MAGLARAS, L., JANICKE, H.: HEART-IS: A novel technique for evaluating human error-related information security incidents, Computers & Security, 2019, 80, pp. 74-89

[163] LIGINLAL, D., SIM, I., KHANSA, L.: How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management, Computers & Security, 2009, 28, (3-4), pp. 215-228

[164] SPEED, A.E., WOO, B.L., KOUHESTANI, C.G., STUBBS, J.J., BIRCH, G.C.: Human Factors in Security: '2018 International Carnahan Conference on Security Technology (ICCST)' IEEE, 2018, pp. 1-5

[165] KRUGER, H.A., DREVIN, L., FLOWERDAY, S., STEYN, T.: An assessment of the role of cultural factors in information security awareness: '2011 Information Security for South Africa' IEEE, 2011, pp. 1-7

[166] WILEY, A., MCCORMAC, A., CALIC, D.: More than the individual: Examining the relationship between culture and Information Security Awareness, Computers & Security, 2020, 88, pp. 101640

[167] HANUS, B., WINDSOR, J.C., WU, Y.: Definition and Multidimensionality of Security Awareness, ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 2018, 49, (SI), pp. 103-133

[168] ALI, R.F., DOMINIC, P.D.D., ALI, S.E.A., REHMAN, M., SOHAIL, A.: Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance, Applied Sciences, 2021, 11, (8), pp. 3383

[169] CHUA, H.N., WONG, S.F., LOW, Y.C., CHANG, Y.: Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations, Telematics and Informatics, 2018, 35, (6), pp. 1770-1780

[170] HADLINGTON, L., POPOVAC, M., JANICKE, H., YEVSEYEVA, I., JONES, K.: Exploring the role of work identity and work locus of control in information security awareness, Computers & Security, 2019, 81, pp. 41-48

[171] HAJLI, N., LIN, X.: Exploring the Security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information, Journal of Business Ethics, 2016, 133, (1), pp. 111-123

[172] ANWAR, M., HE, W., ASH, I., YUAN, X., LI, L., XU, L.: Gender difference and employees' cybersecurity behaviors, Computers in Human Behavior, 2017, 69, pp. 437-443

[173] HADLINGTON, L., PARSONS, K.: Can Cyberloafing and Internet Addiction Affect Organizational Information Security?, Cyberpsychol Behav Soc Netw, 2017, 20, (9), pp. 567-571

[174] ZWILLING, M., KLIEN, G., LESJAK, D., WIECHETEK, Ł., CETIN, F., BASIM, H.N.: Cyber Security Awareness, Knowledge and Behavior: A Comparative Study, Journal of Computer Information Systems, 2020, 62, (1), pp. 82-97

[175] ZOLAIT, A.H.S., ANIZI, R.R.A., ABABNEH, S., BUASALLI, F., BUTAIBA, N.: User awareness of social media security: the public sector framework, International Journal of Business Information Systems, 2014, 17, (3), pp. 261-282

[176] CAVUSOGLU, H., PHAN, T.Q., CAVUSOGLU, H., AIROLDI, E.M.: Assessing the Impact of Granular Privacy Controls on Content Sharing and Disclosure on Facebook, Information Systems Research, 2016, 27, (4), pp. 848-879

[177] RØNN, K.V., SØE, S.O.: Is social media intelligence private? Privacy in public and the nature of social media intelligence, Intelligence and National Security, 2019, 34, (3), pp. 362-378

[178] WEEGER, A., WANG, X., GEWALD, H., RAISINGHANI, M., SANCHEZ, O., GRANT, G., PITTAYACHAWAN, S.: Determinants of Intention to Participate in Corporate BYOD-Programs: The Case of Digital Natives, Information Systems Frontiers, 2018, 22, (1), pp. 203-219

[179] SALAHDINE, F., KAABOUCH, N.: Social Engineering Attacks: A Survey, Future Internet, 2019, 11, (4), pp. 89

[180] SYAFITRI, W., SHUKUR, Z., MOKHTAR, U.A., SULAIMAN, R., IBRAHIM, M.A.: Social Engineering Attacks Prevention: A Systematic Literature Review, IEEE Access, 2022, 10, pp. 39325-39343

[181] GARBA, F.A., JUNAIDU, S.B., AHMAD, I., TEKANYI, M.: Proposed Framework for Effective Detection and Prediction of Advanced Persistent Threats Based on the Cyber Kill Chain, Scientific and Practical Cyber Security Journal, 2018, 3, (3), pp. 1-11

[182] HAYES, D.R., CAPPA, F.: Open-source intelligence for risk assessment, Business Horizons, 2018, 61, (5), pp. 689-697

[183] NIFAKOS, S., CHANDRAMOULI, K., NIKOLAOU, C.K., PAPACHRISTOU, P., KOCH, S., PANAOUSIS, E., BONACINA, S.: Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review, Sensors (Basel), 2021, 21, (15)

[184] BOSMAN, L., HARTMAN, N., SUTHERLAND, J.: How manufacturing firm characteristics can influence decision making for investing in Industry 4.0 technologies, Journal of Manufacturing Technology Management, 2019, 31, (5), pp. 1117-1141

[185] WEISHÄUPL, E., YASASIN, E., SCHRYEN, G.: Information security investments: An exploratory multiple case study on decision-making, evaluation and learning, Computers & Security, 2018, 77, pp. 807-823

[186] VON SOLMS, R., VAN NIEKERK, J.: From information security to cyber security, Computers & Security, 2013, 38, pp. 97-102

[187] CHATTERJEE, R.: Difference Between Cybersecurity & Information Security. 2020 Letöltve: 15.05.2022, https://analyticsindiamag.com/difference-between-cybersecurity-information-security/

[188] KORPELA, K.: Improving Cyber Security Awareness and Training Programs with Data Analytics, Information Security Journal: A Global Perspective, 2015, 24, (1-3), pp. 72-77

[189] ITU: Global Cybersecurity Index 2024. 2024 Letöltve: 03.12.2021, https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf

[190] IMD: World Digital Competitiveness Ranking 2024. 2024 Letöltve: 2024.12.15, https://www.imd.org/centers/world-competitiveness-center/rankings/world-digital-competitiveness/

[191] KOVÁCS, L.: Kiberbiztonság és -stratégia. Budapest: Dialóg Campus Kiadó, 2018

[192] BERKI, G.: A kibertér, annak veszélyei és a kibervédelem jelenlegi helyzete Magyarországon, Nemzetbiztonsági Szemle, 2018, 6, (3), pp. 5-21

[193] ACCENTURE: Securing the digital economy. 2018 Letöltve: 02.12.2021, https://www.accenture.com/us-en/insights/cybersecurity/_acnmedia/Thought-Leadership-Assets/PDF/Accenture-Securing-the-Digital-Economy-Reinventing-the-Internet-for-Trust.pdf#zoom=50

[194] SASI, T., LASHKARI, A.H., LU, R., XIONG, P., IQBAL, S.: A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges, Journal of Information and Intelligence, 2024, 2, (6), pp. 455-513

[195] SUN, N., ZHANG, J., RIMBA, P., GAO, S., ZHANG, L.Y., XIANG, Y.: Data-Driven Cybersecurity Incident Prediction: A Survey, IEEE Communications Surveys & Tutorials, 2019, 21, (2), pp. 1744-1772

[196] IBM: Cost of a data breach 2022. 2022 Letöltve: 02.02.2023, https://www.ibm.com/reports/data-breach

[197] AV-TEST INSTITUTE: Malware. 2019 Letöltve: 02.02.2023, https://www.av-test.org/en/statistics/malware/

[198] BEDERNA, Z., RAJNAI, Z.: Analysis of static and dynamic parameters of players in cyberspace, in Rajnai, Z., Schmidt, P., and Jurík, P. (Eds.): 'Eighth International Scientific Web-conference of Scientists and PhD. students or candidates - „Trends and Innovations in E-business, Education and Security "' Óbuda University, 2020

[199] BENDIEK, A.: The EU as a force for peace in international cyber diplomacy, in Editor (Ed.)^(Eds.): 'Book The EU as a force for peace in international cyber diplomacy' Stiftung Wissenschaft und Politik -SWP- Deutsches Institut für Internationale Politik und Sicherheit, 2018, edn., pp.

[200] CALDERARO, A., CRAIG, A.J.S.: Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building, Third World Quarterly, 2020, 41, (6), pp. 917-938

[201] KRASZNAY, C.: Kiberbiztonsági kompetencia hálózatok Európában – K+F+I lehetőségek a következő évtizedben, Scientia et Securitas, 2020, 1, (1), pp. 43-48

[202] ITU: Definition of Cybersecurity. 2017 Letöltve: 02.02.2023, https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

[203] HORVÁTH, G.K.: Közérthetően (nem csak) az IT biztonságról. Budapest: KIFÜ, 2013

[204] FERNANDEZ DE ARROYABE, I., FERNANDEZ DE ARROYABE, J.C.: The severity and effects of Cyber-breaches in SMEs: a machine learning approach, Enterprise Information Systems, 2021, 17, (3)

[205] KABANDA, S., TANNER, M., KENT, C.: Exploring SME cybersecurity practices in developing countries, Journal of Organizational Computing and Electronic Commerce, 2018, 28, (3), pp. 269-282

[206] FERNANDEZ DE ARROYABE, J.C., ARROYABE, M.F., FERNANDEZ, I., ARRANZ, C.F.A.: Cybersecurity Resilience in SMEs. A Machine Learning Approach, Journal of Computer Information Systems, 2023, 64, (6), pp. 711-727

[207] MUNK, S.: A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései, Hadtudomány: A Magyar Hadtudományi Társaság Folyóirata, 2018, 28, (1), pp. 113-131

[208] KRALOVÁNSZKY, K.: A kibertér fejlődése, Hadmérnök, 2019, 14, (4), pp. 197-212

[210] OFFICE OF THE CHAIRMAN OF THE JOINT CHIEFS OF STAFF: DOD Dictionary of Military and Associated Terms. 2021 Letöltve: 02.12.2021, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2018-07-25-091749-087

[211] TESSIAN: The Psychology of Human Error. 2020 Letöltve: 02.12.2021, https://library.cyentia.com/report/report_005259.html

[212] MALWAREBYTES: Enduring from home: COVID-19's impact on business security. 2020 Letöltve: 03.12.2021, https://www.malwarebytes.com/resources/files/2020/08/malwarebytes_enduringfromhome_report_final.pdf

[213] ARONOVICH, A.: Why Educating Your Employees on Cyber Intelligence And Security Will Reduce Risk. 2018 Letöltve: 01.12.2021, https://www.cybintsolutions.com/employee-education-reduces-risk/

[214] FEKETE-KARYDIS, K., LÁZÁR, B.: A kibervédelmi stratégiák fejlődése, kibervédelmi kihívások, aktualitások (1.), Honvédségi Szemle–Hungarian Defence Review, 2019, 147, (4), pp. 38-49

[215] EURÓPAI BIZOTTSÁG: Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér. 2013 Letöltve: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52013JC0001&from=EL

[217] CYBER RISK, G.: The NIS 2 Directive. 2023 Letöltve: 2024.11.15, https://www.nis-2-directive.com/. 2024

[218] MARKOPOULOU, D., PAPAKONSTANTINOU, V., DE HERT, P.: The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, Computer Law & Security Review, 2019, 35, (6)

[219] RIZOS, V., BEHRENS, A., VAN DER GAAST, W., HOFMAN, E., IOANNOU, A., KAFYEKE, T., FLAMOS, A., RINALDI, R., PAPADELIS, S., HIRSCHNITZ-GARBERS, M., TOPI,

C.: Implementation of Circular Economy Business Models by Small and Medium-Sized Enterprises (SMEs): Barriers and Enablers, Sustainability, 2016, 8, (11)

[220] RAJNAI, Z., FREGAN, B.: Új alapokon a magyarországi kibervédelmi stratégia Műszaki tudományos közlemények, 2017, (7), pp. 351-354

[221] KOVÁCS, L.: A kiberbiztonság és a kiberműveletek megjelenése Magyarország új Nemzeti Biztonsági Stratégiájában, Honvédségi Szemle, 2020, 148, (5), pp. 3-18

[223] KOVÁCS, L., KRASZNAY, C.: Digitális Mohács: Egy kibertámadási forgatókönyv Magyarország ellen, Nemzet és Biztonság–Biztonságpolitikai Szemle, 2010, 1, pp. 44-56

[224] KOVÁCS, L., KRASZNAY, C.: Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint, Nemzet és Biztonság–Biztonságpolitikai Szemle, 2017, 10, (1), pp. 3-16

[225] IDG: IDG Cloud Computing Survey. 2020 Letöltve: https://resources.idg.com/download/2020-cloud-computing-executive-summary-rl?utm_campaign=2020%20Cloud%20Computing%20Study&utm_source=twitter&utm_medium=social&utm_term=2020%20Cloud%20Executive%20Summary&utm_content=2020%20Cloud%20Executive%20Summary

[226] MLITZ, K.: Public cloud services end-user spending worldwide from 2017 to 2022. 2021 Letöltve: https://www.statista.com/statistics/273818/global-revenue-generated-with-cloud-computing-since-2009/

[227] GANZAROLI, A., MARINOS, L., NASI, G., PASIC, A., SILVIA, P.: Cloud cybersecurity market analysis. 2023 Letöltve: 07.07.2025, https://www.enisa.europa.eu/sites/default/files/publications/Cloud%20Cybersecurity%20Market%20Analysis.pdf

[228] CEPTUREANU, E.G., CEPTUREANU, S.I.: The impact of adoptive management innovations on medium-sized enterprises from a dynamic capability perspective, Technology Analysis & Strategic Management, 2019, 31, (10), pp. 1137-1151

[229] HASHIZUME, K., ROSADO, D.G., FERNÁNDEZ-MEDINA, E., FERNANDEZ, E.B.: An analysis of security issues for cloud computing, Journal of Internet Services and Applications, 2013, 4, (1), pp. 5

[230] ABDOLLAHZADEGAN, A., CHE HUSSIN, A.R., MOSHFEGH GOHARY, M., AMINI, M.: The organizational critical success factors for adopting cloud computing in SMEs, Journal of Information Systems Research and Innovation (JISRI), 2013, 4, (1), pp. 67-74

[231] EUROSTAT: Cloud computing services. 2021 Letöltve: https://ec.europa.eu/eurostat/databrowser/view/isoc_cicce_use/default/table?lang=en

[232] EUROSTAT: Cloud computing - statistics on the use by enterprises. 2021 Letöltve: 15.05.2022, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises&stable=0&redirect=no

[233] XU, X.: From cloud computing to cloud manufacturing, Robotics and Computer-Integrated Manufacturing, 2012, 28, (1), pp. 75-86

[234] BAYRAMUSTA, M., NASIR, V.A.: A fad or future of IT?: A comprehensive literature review on the cloud computing research, International Journal of Information Management, 2016, 36, (4), pp. 635-644

[235] ABBAS, A., BILAL, K., ZHANG, L., KHAN, S.U.: A cloud based health insurance plan recommendation system: A user centered approach, Future Generation Computer Systems, 2015, 43-44, pp. 99-109

[236] OREHOVAČKI, T., BABIĆ, S., ETINGER, D.: Identifying Relevance of Security, Privacy, Trust, and Adoption Dimensions Concerning Cloud Computing Applications Employed in Educational Settings, in Nicholson, D. (Ed.): 'Advances in Human Factors in Cybersecurity. AHFE 2017' Springer, 2018, pp. 308-320

[237] SCHUBERT, T., PÓSER, V., ÁCS, S., PRÉM, D., MÁRTON, J., KOZLOVSZKY, M.: Számítási felhő biztonsági kérdései, Műszaki Katonai Közlöny, 2012, 22, (2), pp. 86-103

[238] MELL, P., GRANCE, T.: The NIST Definition of Cloud Computing. Gaithersburg: National Institute of Standards and Technology, 2011

[239] IBM: What are Iaas, Paas and Saas? 2021 Letöltve: 12.12.2024, https://www.ibm.com/think/topics/iaas-paas-saas

[240] AWS: Types of Cloud Computing. 2021 Letöltve: 12.12.2024, https://aws.amazon.com/types-of-cloud-computing/

[241] GOOGLE: What are the different types of cloud computing? 2021 Letöltve: 12.12.2024, https://cloud.google.com/discover/types-of-cloud-computing

[242] VINOTH, S., VEMULA, H.L., HARALAYYA, B., MAMGAIN, P., HASAN, M.F., NAVED, M.: Application of cloud computing in banking and e-commerce and related security threats, Materials Today: Proceedings, 2022, 51, pp. 2172-2175

[243] SAHANDI, R., ALKHALIL, A., OPARA-MARTINS, J.: SMEs' Perception of Cloud Computing: Potential and Security, in Camarinha-Matos, L.M., Xu, L., and Afsarmanesh, H. (Eds.): 'FIP Advances in Information and Communication Technology' Springer, 2012, pp. 186-195

[244] ATTARAN, M., WOODS, J.: Cloud computing technology: improving small business performance using the Internet, Journal of Small Business & Entrepreneurship, 2018, 31, (6), pp. 495-519

[245] YIMAM, D., FERNANDEZ, E.B.: A survey of compliance issues in cloud computing, Journal of Internet Services and Applications, 2016, 7, (1)

[246] DI MARTINO, B., CRETELLA, G., ESPOSITO, A.: Cloud Portability and Interoperability, in SMurugesan, S., and Bojanova, I. (Eds.): 'Encyclopedia of Cloud Computing' John Wiley & Sons Ltd., 2016, pp. 163-177

[247] MEZGÁR, I., RAUSCHECKER, U.: The challenge of networked enterprises for cloud computing interoperability, Computers in Industry, 2014, 65, (4), pp. 657-674

[248] GOZMAN, D., WILLCOCKS, L.: The emerging Cloud Dilemma: Balancing innovation with cross-border privacy and outsourcing regulations, Journal of Business Research, 2019, 97, pp. 235-256

[249] ORZES, G., RAUCH, E., BEDNAR, S., POKLEMBA, R.: Industry 4.0 Implementation Barriers in Small and Medium Sized Enterprises: A Focus Group Study: '2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)' IEEE, 2018, pp. 1348-1352

[250] LEUPRECHT, C., SKILLICORN, D.B., TAIT, V.E.: Beyond the Castle Model of cyber-risk and cyber-security, Government Information Quarterly, 2016, 33, (2), pp. 250-257

[251] ALOUFFI, B., HASNAIN, M., ALHARBI, A., ALOSAIMI, W., ALYAMI, H., AYAZ, M.: A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies, IEEE Access, 2021, 9, pp. 57792-57807

[252] BLONDEAU, C., RUIZ, J.: Cybersecurity Assessment - Evaluations & Certifications - State of Play 2018-2022 2024 Letöltve: 07.07.2025, https://www.enisa.europa.eu/sites/default/files/publications/Cybersecurity%20Certification%20Statistics%20Report.pdf

[253] SEETHAMRAJU, R.: Adoption of Software as a Service (SaaS) Enterprise Resource Planning (ERP) Systems in Small and Medium Sized Enterprises (SMEs), Information Systems Frontiers, 2014, 17, (3), pp. 475-492

[254] BARBIERI, L.M., SOTT, M.K., MONTICELLI, J.M.: Critical Success Factors for Implementing Cloud ERP in SMEs: A Systematic Review, International Journal of Innovation and Technology Management, 2023, 21, (02)

[255] BHATT, N., GURU, S., THANKI, S., SOOD, G.: Analysing the factors affecting the selection of ERP package: a fuzzy AHP approach, Information Systems and e-Business Management, 2021, 19, (2), pp. 641-682

[256] KOVALEV, V., NOVIKOVA, K., DOBROVLYANIN, V.: ERP systems in small and medium-sized enterprises: Barriers and prospects, Upravlenets, 2024, 14, (6), pp. 77-90

[257] SCHAEFER, J.L., BAIERLE, I.C., SELLITTO, M.A., SILUK, J.C.M., FURTADO, J.C., NARA, E.O.B.: Competitiveness Scale as a Basis for Brazilian Small and Medium-Sized Enterprises, Engineering Management Journal, 2020, 33, (4), pp. 255-271

[258] LAFUENTE, E., SZERB, L., RIDEG, A.: A system dynamics approach for assessing SMEs' competitiveness, Journal of Small Business and Enterprise Development, 2020, 27, (4), pp. 555-578

[259] CHATZOGLOU, P., CHATZOUDES, D., FRAGIDIS, L., SYMEONIDIS, S.: Critical success factors for ERP implementation in SMEs. Proc. Proceedings of the 2016 Federated Conference on Computer Science and Information Systems2016 pp. 1243-1252

[260] HÉRA, G., LIGETI, G.: Módszertan – A társadalmi jelenségek kutatása. Budapest: Osiris Kiadó, 2014

[261] GÉRING, Z.: Kevert szövegelemzési módszertan alkalmazása gazdasági és társadalmi jelenségek vizsgálatához - Online CSR-kommunikáció vizsgálata tartalomelemzéssel és diskurzuselemzéssel, Vezetéstudomány / Budapest Management Review, 2017, 48, (4), pp. 55-66

[262] ELO, S., KÄÄRIÄINEN, M., KANSTE, O., PÖLKKI, T., UTRIAINEN, K., KYNGÄS, H.: Qualitative Content Analysis, Sage Open, 2014, 4, (1)

[263] ROWLANDS, T., WADDELL, N., MCKENNA, B.: Are We There Yet? A Technique to Determine Theoretical Saturation, Journal of Computer Information Systems, 2015, 56, (1), pp. 40-47

[264] CHOULIARAS, N., KANTZAVELOU, I., MAGLARAS, L., PANTZIOU, G., AMINE FERRAG, M.: A novel autonomous container-based platform for cybersecurity training and research, PeerJ Comput Sci, 2023, 9, pp. e1574

[265] MENG, S., GAO, Z., LI, Q., WANG, H., DAI, H.-N., QI, L.: Security-Driven hybrid collaborative recommendation method for cloud-based iot services, Computers & Security, 2020, 97

[266] BARRY, C.A.: Choosing Qualitative Data Analysis Software: Atlas/ti and Nudist Compared, Sociological Research Online, 1998, 3, (3), pp. 16-28

[267] BRINGER, J.D., JOHNSTON, L.H., BRACKENRIDGE, C.H.: Using Computer-Assisted Qualitative Data Analysis Software to Develop a Grounded Theory Project, Field Methods, 2006, 18, (3), pp. 245-266

[268] HODDY, E.T.: Critical realism in empirical research: employing techniques from grounded theory methodology, International Journal of Social Research Methodology, 2018, 22, (1), pp. 111-124

[269] ZHU, P., LUKE, M., BELLINI, J.: A Grounded Theory Analysis of Cultural Humility in Counseling and Counselor Education, Counselor Education and Supervision, 2021, 60, (1), pp. 73-89

[270] SONY, M., MEKOTH, N.: A qualitative study on electricity energy-saving behaviour, Management of Environmental Quality: An International Journal, 2018, 29, (5), pp. 961-977

[271] PUPPIS, M.: Analyzing Talk and Text I: Qualitative Content Analysis: 'The Palgrave Handbook of Methods for Media Policy Research', 2019, pp. 367-384

[272] GREEN, J., WILLIS, K., HUGHES, E., SMALL, R., WELCH, N., GIBBS, L., DALY, J.: Generating best evidence from qualitative research: the role of data analysis, Aust N Z J Public Health, 2007, 31, (6), pp. 545-550

[273] GIESEN, L., ROESER, A.: Structuring a Team-Based Approach to Coding Qualitative Data, International Journal of Qualitative Methods, 2020, 19

[274] GILES, T.M., DE LACEY, S., MUIR-COCHRANE, E.: Coding, Constant Comparisons, and Core Categories: A Worked Example for Novice Constructivist Grounded Theorists, ANS Adv Nurs Sci, 2016, 39, (1), pp. E29-44

[275] SARKER, S., LAU, F., SAHAY, S.: Using an adapted grounded theory approach for inductive theory building about virtual team development, ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 2000, 32, (1), pp. 38-56

[276] ROY-DAVIS, K., WADEY, R., EVANS, L.: A grounded theory of sport injury-related growth, Sport, Exercise, and Performance Psychology, 2017, 6, (1), pp. 35-52

[277] SARKER, S., LAU, F., SAHAY, S.: Building an inductive theory of collaboration in virtual teams: an adapted grounded theory approach. Proc. Proceedings of the 33rd Annual Hawaii International Conference on System Sciences2000

[278] MELLION, L.R., TOVIN, M.M.: Grounded theory: a qualitative research methodology for physical therapy, Physiotherapy Theory and Practice, 2009, 18, (3), pp. 109-120

[279] WILSON, H.S., HUTCHINSON, S.A.: Triangulation of Qualitative Methods: Heideggerian Hermeneutics and Grounded Theory, Qualitative Health Research, 1991, 1, (2), pp. 263-276

[280] AHMAD, S.R., BAKAR, A.A., YAAKUB, M.R.: Metaheuristic algorithms for feature selection in sentiment analysis. Proc. 2015 Science and Information Conference (SAI)2015 pp. 222-226

[281] TAN, K.L., LEE, C.P., LIM, K.M.: A Survey of Sentiment Analysis: Approaches, Datasets, and Future Research, Applied Sciences, 2023, 13, (7)

[282] ABUALIGAH, L., ALFAR, H.E., SHEHAB, M., HUSSEIN, A.M.A.: Sentiment Analysis in Healthcare: A Brief Review: 'Recent Advances in NLP: The Case of Arabic Language', 2020, pp. 129-141

[283] BEHDENNA, S., BARIGOU, F., BELALEM, G.: Document Level Sentiment Analysis: A survey, EAI Endorsed Transactions on Context-aware Systems and Applications, 2018, 4, (13)

[284] POORNIMA, A., PRIYA, K.S.: A Comparative Sentiment Analysis Of Sentence Embedding Using Machine Learning Techniques. Proc. 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)2020 pp. 493-496

[285] SHAIK, T., TAO, X., DANN, C., XIE, H., LI, Y., GALLIGAN, L.: Sentiment analysis and opinion mining on educational data: A survey, Natural Language Processing Journal, 2023, 2

[286] SONI, P.K., RAMBOLA, R.: A Survey on Implicit Aspect Detection for Sentiment Analysis: Terminology, Issues, and Scope, IEEE Access, 2022, 10, pp. 63932-63957

[287] FARHADLOO, M., ROLLAND, E.: Fundamentals of Sentiment Analysis and Its Applications: 'Sentiment Analysis and Ontology Engineering', 2016, pp. 1-24

[288] CHEN, T., XU, R., HE, Y., WANG, X.: Improving sentiment analysis via sentence type classification using BiLSTM-CRF and CNN, Expert Systems with Applications, 2017, 72, pp. 221-230

[289] LI, L., LIU, Y., ZHOU, A.: Hierarchical Attention Based Position-Aware Network for Aspect-Level Sentiment Analysis. Proc. Proceedings of the 22nd Conference on Computational Natural Language Learning2018 pp. 181-189

[290] LU, Q., ZHU, Z., ZHANG, D., WU, W., GUO, Q.: Interactive Rule Attention Network for Aspect-Level Sentiment Analysis, IEEE Access, 2020, 8, pp. 52505-52516

[291] BAK, G., REICHER, R.: A vállalkozások és a digitális fejlődés, in Baráth, N.E., and Mezei, J. (Eds.): 'Rendészet-Tudomány-Aktualitások 2022' Doktoranduszok Országos Szövetsége, 2022, pp. 82-97

[292] BAK, G., REICHER, R.: Small and Medium-Sized Enterprises' Perceptions of the Use of Cloud Services, Interdisciplinary Description of Complex Systems, 2023, 21, (2), pp. 131-140

[293] BAK, G., REICHER, R.: Relationship of the Security Awareness and the Value Chain, Engineering Proceedings Sustainable Mobility and Transportation Symposium (SMTS 2025) MEGJELENÉS ALATT, 2025

[294] RUTKOWSKI, R.A., LEE, J.D., COLLER, R.J., WERNER, N.E.: How can text mining support qualitative data analysis?, Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 2022, 66, (1), pp. 2319-2323

[295] YE, R., XU, J., ZHANG, N.: A Qualitative Comparative Analysis of the Academic Media Using Frequency on Networking Platforms, Journal of Physics: Conference Series, 2021, 1952, (4)

[296] HOSKING, J.R.M., WALLIS, J.R.: Some statistics useful in regional frequency analysis, Water Resources Research, 1993, 29, (2), pp. 271-281

[297] EL-GAZZAR, R., HUSTAD, E., OLSEN, D.H.: Understanding cloud computing adoption issues: A Delphi study approach, Journal of Systems and Software, 2016, 118, pp. 64-84

[298] UDDIN, A., CETINDAMAR, D., HAWRYSZKIEWYCZ, I., SOHAIB, O.: The Role of Dynamic Cloud Capability in Improving SME's Strategic Agility and Resource Flexibility: An Empirical Study, Sustainability, 2023, 15, (11)

[299] SUBASHINI, S., KAVITHA, V.: A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, 2011, 34, (1), pp. 1-11

[300] CHANG, V., KUO, Y.-H., RAMACHANDRAN, M.: Cloud computing adoption framework: A security framework for business clouds, Future Generation Computer Systems, 2016, 57, pp. 24-41

[301] BAK, G., REICHER, R.: A felhőszolgáltatás a kkv szemével, in Szikora, P. (Ed.): 'Társadalom, Informatika és Gazdaság Kutatócsoport Konferencia kiadvány. TIGKONF 2025' Óbudai Egyetem, Keleti Károly Gazdasági Kar 2025 MEGJELENÉS ALATT

[302] AL HADWER, A., TAVANA, M., GILLIS, D., REZANIA, D.: A Systematic Review of Organizational Factors Impacting Cloud-based Technology Adoption Using Technology-Organization-Environment Framework, Internet of Things, 2021, 15

[303] ALI, O., SHRESTHA, A., OSMANAJ, V., MUHAMMED, S.: Cloud computing technology adoption: an evaluation of key factors in local governments, Information Technology & People, 2020, 34, (2), pp. 666-703

[304] CHEN, M., WANG, H., LIANG, Y., ZHANG, G.: Net and configurational effects of determinants on cloud computing adoption by SMEs under cloud promotion policy using PLS-SEM and fsQCA, Journal of Innovation & Knowledge, 2023, 8, (3)

[305] GANGWAR, H., DATE, H., RAMASWAMY, R.: Understanding determinants of cloud computing adoption using an integrated TAM-TOE model, Journal of Enterprise Information Management, 2015, 28, (1), pp. 107-130

[306] ORIZA, R., MAULIDAR: Adoption and Impact of Cloud Computing in Small and Medium Enterprises A Systematic Review, Journal Informatic, Education and Management (JIEM), 2024, 6, (2), pp. 8-15

[307] KUMAR, D., SAMALIA, H.V., VERMA, P.: Factors Influencing Cloud Computing Adoption by Small and Medium-Sized Enterprises (SMEs) In India, Pacific Asia Journal of the Association for Information Systems, 2017, pp. 25-48

[308] KUMAR, D., SAMALIA, H.V., VERMA, P.: Exploring suitability of cloud computing for small and medium-sized enterprises in India, Journal of Small Business and Enterprise Development, 2017, 24, (4), pp. 814-832

[309] RAMOLLARI, E., VAJHALA, N.R.: Big Data using Cloud Computing - Opportunities for Small and Medium-sized Enterprises, European Journal of Economics and Business Studies, 2016, 4, (1)

[310] DEY, P.K., MALESIOS, C., CHOWDHURY, S., SAHA, K., BUDHWAR, P., DE, D.: Adoption of circular economy practices in small and medium-sized enterprises: Evidence from Europe, International Journal of Production Economics, 2022, 248

[311] BRADAČ HOJNIK, B., HUĐEK, I.: Small and Medium-Sized Enterprises in the Digital Age: Understanding Characteristics and Essential Demands, Information, 2023, 14, (11)

[312] SNEE, R.D.: Lean Six Sigma – getting better all the time, International Journal of Lean Six Sigma, 2010, 1, (1), pp. 9-29

Jogszabályok

[209] Magyarország Nemzeti Kiberbiztonsági Stratégiájáról, 2013

[216] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)Text with EEA relevance, 2022

[222] Magyarország Nemzeti Biztonsági Stratégiája „Biztonságos Magyarország egy változékony világban”, 2020

Táblázatjegyzék

Ábrajegyzék

Mellékletek

1. számú melléklet: Interjúvázlat – kkv oldal

A Kkv-k és a felhőszolgáltatás viszonya – IT cloud szolgáltató

Interjú segédanyag-kérdéskörök

1. Demográfiai kérdések
    a. Neme:
    b. Kor
    c. Beosztás:
    d. Munkatapasztalat években:
    e. Cég iparági besorolása:
    f. Cég mérete:
    g. Jelen cégnél mióta dolgozik
    h. IT vonalon mennyi a tapasztalata (év)
2. Hogy írná le az Önökhöz forduló kkv-kat információbiztonsági szempontból általánosan, országos viszonylatban, illetve többiekhez képest?
3. Hogyan látja az Önökhöz forduló kkv-kat a felhőszolgáltatással kapcsolatos ismereteik alapján?
4. Milyen tendenciákat tapasztal a felhőszolgáltatást igénybe vevő vállalatoknál?
5. Mit gondol, mi motiválja a kkv-kat a felhőszolgáltatás igénybevételére?
6. Mit gondol, mi tartja vissza a kkv-kat a felhőszolgáltatás igénybevételére?
7. Milyen helyzetek, tényezők jelentenek kihívást a kkv-knak a felhőszolgáltatás kapcsán?
8. Milyen helyzetek, tényezők jelentenek előnyt/lehetőséget a kkv-knak a felhőszolgáltatás kapcsán?
9. Ön szerint mit várnak el egy felhőszolgáltatástól a kkv-k?

2. számú melléklet: Interjúvázlat – szolgáltatói oldal

A Kkv-k és a felhőszolgáltatás viszonya – IT cloud szolgáltató

Interjú segédanyag-kérdéskörök

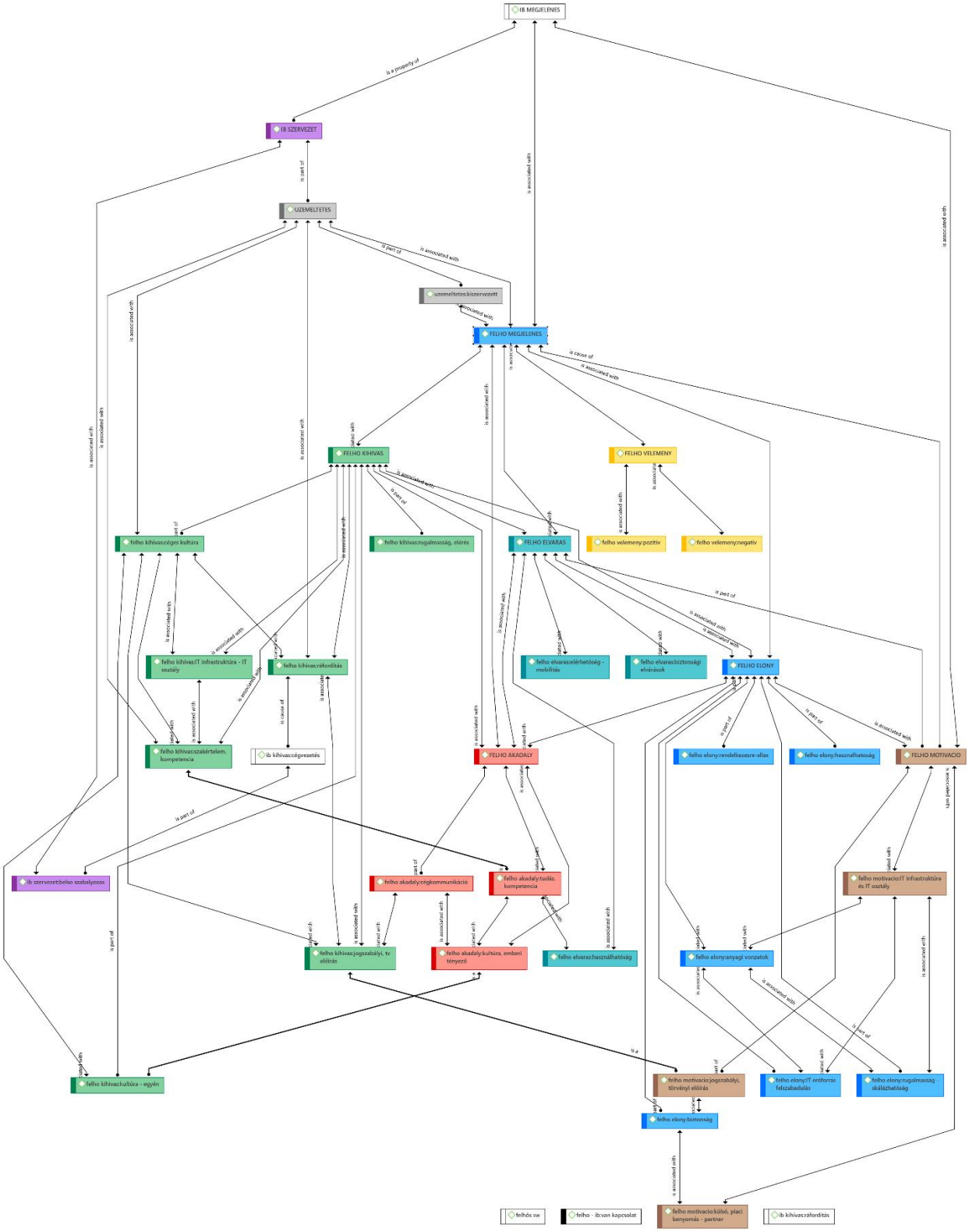
1. Demográfiai kérdések
    a. Neme:
    b. Kor
    c. Beosztás:
    d. Munkatapasztalat években:
    e. Cég iparági besorolása:
    f. Cég mérete:
    g. Jelen cégnél mióta dolgozik
    h. IT vonalon mennyi a tapasztalata (év)
2. Hogy írná le az Önökhöz forduló kkv-kat információbiztonsági szempontból általánosan, országos viszonylatban, illetve többiekhez képest?
3. Hogyan látja az Önökhöz forduló kkv-kat a felhőszolgáltatással kapcsolatos ismereteik alapján?
4. Milyen tendenciákat tapasztal a felhőszolgáltatást igénybe vevő vállalatoknál?
5. Mit gondol, mi motiválja a kkv-kat a felhőszolgáltatás igénybevételére?
6. Mit gondol, mi tartja vissza a kkv-kat a felhőszolgáltatás igénybevételére?
7. Milyen helyzetek, tényezők jelentenek kihívást a kkv-knak a felhőszolgáltatás kapcsán?
8. Milyen helyzetek, tényezők jelentenek előnyt/lehetőséget a kkv-knak a felhőszolgáltatás kapcsán?
9. Ön szerint mit várnak el egy felhőszolgáltatástól a kkv-k?

3. számú melléklet: Az interjúalanyok részletesebb bemutatása

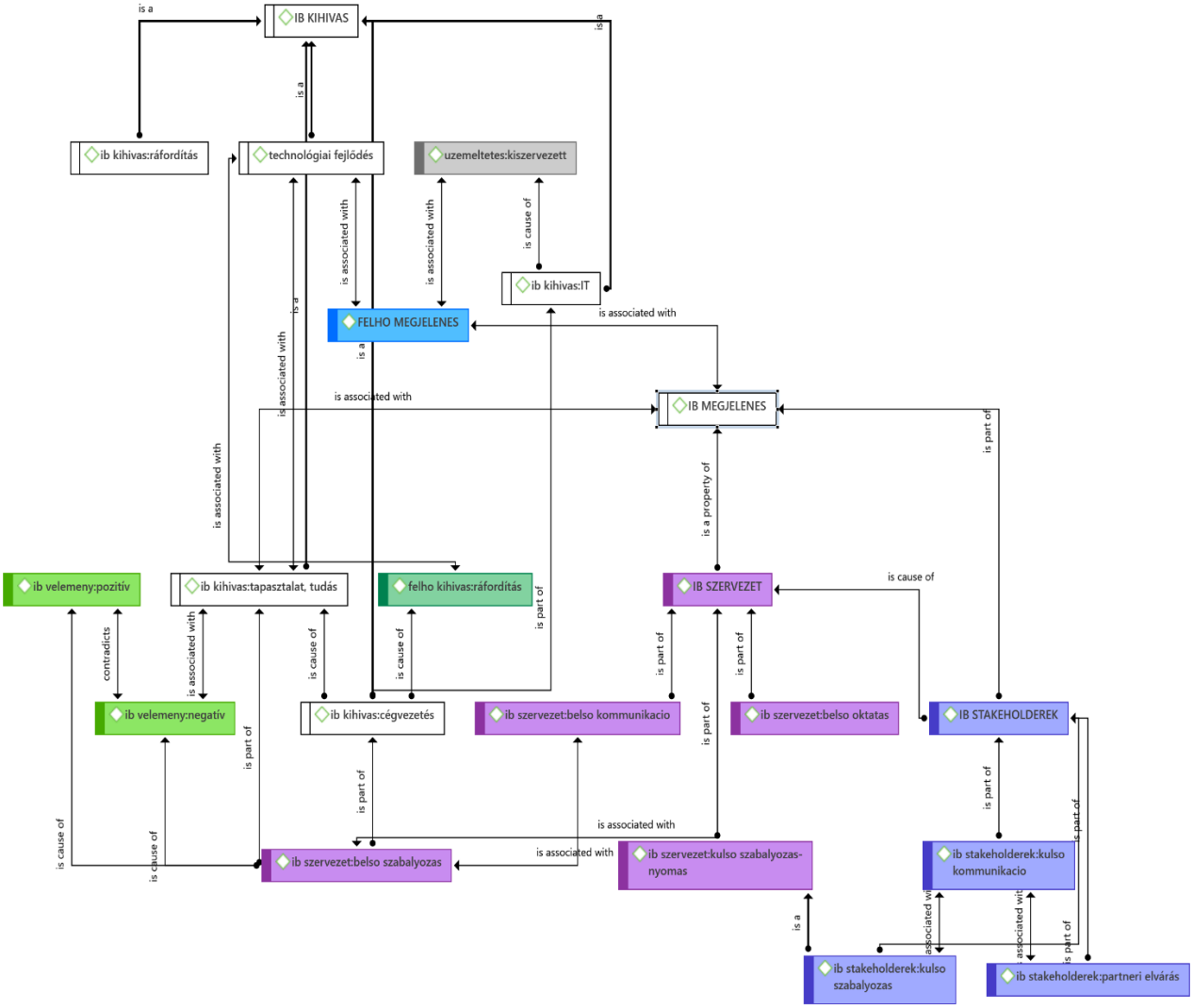
Kkv oldal				Szolgáltatói oldal			
Nem	**Kor**	**Beosztás**	**Iparági besorolás**	**Nem**	**Kor**	**Beosztás**	**Iparági besorolás**
Férfi	28	security architect	Számítógépes programozás	Férfi	36	technikai csoportvezető	Informatika
Férfi	47	IT üzemeltetési vezető	Számítógép-üzemeltetés	Férfi	40	IT manager	IT security megoldások disztribúció
Férfi	33	Group ISO és DPO	Számítógépes programozás	Férfi	33	Group ISO és DPO	Számítógépes programozás
Nő	37	Információbiztonsági tanácsadás üzletágvezető	Információ-technológiai szaktanácsadás	Férfi	50	Műszaki igazgató	Információ-technológiai szaktanácsadás
Nő	35	vezető közgazdász	Számviteli, könyvvizsgálói, adószakértői tevékenység	Férfi	51	üzleti konzultáns	Informatika szállító
Férfi	50	Műszaki igazgató	Információ-technológiai szaktanácsadás	Férfi	37	IT biztonsági vezető	Információ-technológiai szaktanácsadás
Férfi	42	Local IT	Építőipar	Férfi	50	Sales	IT szaktanácsadás
Nő	57	külsős szerződéses munkatárs	gyógyszeripar	Férfi	44	IT Security és presales tech	IT disztribútor
Férfi	44	IT koordinátor	Egyéb ipari, kereskedelmi, navigációs gép nagyker	Férfi	55	Vezető	IT szolgáltató
Férfi	45	ügyvezető	Acél nagyker és feldolgozóipar	Férfi	46	Rendszergazda	Szoftverfejlesztés
Nő	33	IB tanácsadó	Számítógép-üzemeltetés	Férfi	27	Vezető rendszergazda	IT, hosting
Férfi	58	tulajdonos ügyvezető	Gépgyártás	Férfi	37	CEO	Online infrastruktúra szolgáltató
Férfi	35	Ügyvezető	élelmiszeripar	Férfi	28	security architect	Számítógépes programozás
Férfi	58	ügyvezető	egészségügyi szolgáltató	Férfi	43	tulajdonos, IT vezető	IT szolgáltató
Férfi	44	pénzügyi vezető	mezőgazdaság	Nő	47	Group Manager	Telekommunikáció
Férfi	53	ügyvezető	egyedigép gyártás	Férfi	51	rendszergazda	Szoftverfejlesztés

Férfi	50	ügyvezető	Ipari elektronika, automatizálás				
Nő	38	cégvezető	HR tanácsadás				

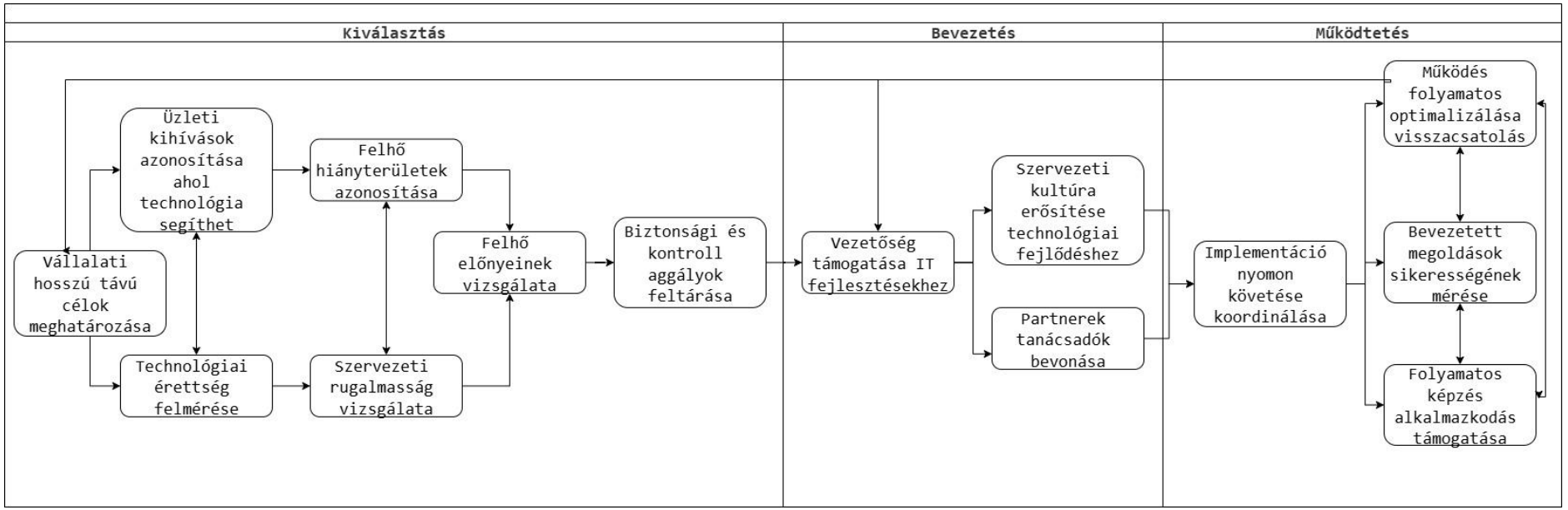
4.számú melléklet: Részletes kódhálózat a felhő megjelenése kapcsán



5.számú melléklet: Részletes kódhálózat az információbiztonság kapcsán



6.számú melléklet: A felhőszolgáltatás kiválsztásának, bevezetésének és működtetésének folyamata a kutatás alapján



Köszönetnyilvánítás

Szeretném megköszönni Dr. habil Reicher Regina Zsuzsannának, hogy a doktori kutatásom megvalósulásáig minden szakaszban mellettem állt, és nem csak tudását és tapasztalatát osztotta meg velem, hanem mindig támogatott, bíztatott és hitt bennem.

Köszönöm Dr. habil Velencei Jolánnak az önzetlen támogatást és azt a rengeteg értékes gondolatot, valamint ajánlást, amelyekkel hozzájárult az értekezésem sikeréhez.

Szeretnék köszönetet mondani a Biztonságtudományi Doktori Iskolának, valamint az ott dolgozóknak és mindenkinek, aki segített és támogatott a doktori tanulmányom során.

Szintén szeretném megköszönni az összes interjúalanyomnak, akik a publikációk és az értekezés megvalósulásához hozzájárultak értékes ötleteikkel, tapasztalataikkal és gondolataikkal.