ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS

TÉZISFÜZETE

BAK DORINA GERDA

A felhőhasználat információbiztonsági aspektusai a kkv-knál

Témavezető: Dr. habil Reicher Regina Zsuzsánna

BIZTONSÁGTUDOMÁNYI
DOKTORI ISKOLA

Budapest, 2025.09.08

Tartalomjegyzék

1 Summary 3

2 A kutatás előzményei 4

3 Célkitűzések 5

4 Vizsgálati módszerek 6

6 Új tudományos eredmények 9

7 Az eredmények hasznosítási lehetősége 14

8 Irodalmi hivatkozások listája/ Irodalomjegyzék 14

9 Publikációk 37

9.1 A tézispontokhoz kapcsolódó tudományos közlemények 37

9.2 További tudományos közlemények (opcionális) 37

1 Summary

Small and medium-sized enterprises (SMEs) are essential drivers of economic growth, innovation, employment, and social cohesion at all levels. In Hungary, they represent 99% of businesses and employ two-thirds of the workforce. The crucial factor determining their competitiveness and market reach is the adoption of digital technologies, but this is slowed by financial constraints, lack of expertise, and insufficient risk management. Cybersecurity is a growing threat, often driven by human error. While SMEs have the advantage of flexibility and rapid response, these strengths are undermined by limited resources, a lack of clear digital strategy, and challenges aligning technology with business goals. The constantly changing work environment requires the development of digital skills and digital intelligence. Human behavior can both strengthen and weaken information security. Security awareness depends on several factors: age, gender, education, experience, employee engagement, and organizational culture. Cybersecurity awareness can be improved through training, and practical experience. SMEs need to adopt a comprehensive cybersecurity approach, including the integrated management of technological tools and the human factor. Effective digital transformation for SMEs hinges on understanding why they adopt or reject cloud services.

I collected the primary data through semi-structured interviews, where applying content analysis methodology, the study covered not only the direct content of the texts, but also their contextual relationships. I used the following methods to analyze the interviews:

1. Coding – organizing the data and identifying themes.
2. Code frequency analysis – highlighting the main themes.
3. Context analysis (code network) – exploring relationships and causal connections.
4. Sentiment analysis – identifying hidden attitudes and emotional aspects.

This research identifies a key finding: while service providers focus on organizational and cultural factors, SMEs prioritize tangible benefits and daily operational challenges. The primary barriers to SME cloud adoption include reactive decision-making, limited expertise, concerns about costs, and a lack of trust. Progress in cybersecurity and digitalization is shaped by both technological readiness and human factors. To address skepticism regarding digital tools, SMEs require a human-centered and integrated transformation strategy that emphasizes employee attitudes, targeted training, and effective internal communication.

2 A kutatás előzményei

A kis- és középvállalkozások digitalizációja

A kis- és középvállalkozások (kkv-k) kulcsszerepet töltenek be a globális, uniós és hazai gazdaságokban, hozzájárulva a gazdasági növekedéshez, foglalkoztatáshoz és innovációhoz [35–41]. Magyarországon a vállalkozások 99%-a kkv, és a foglalkoztatottak mintegy kétharmada ebben a szektorban dolgozik [40, 41]. A kkv-k digitális technológiák, például felhőszolgáltatások, mesterséges intelligencia és robotika alkalmazásával fejleszthetik működésüket és versenyképességüket [42–44]. Az EU-ban és Magyarországon a kkv-k teljesítményét eltérő gazdasági, szabályozási és társadalmi tényezők befolyásolják, például a pénzügyi forrásokhoz való hozzáférés és a GDPR-megfelelés [45–48]. A magyar kkv-k gyakran költséghatékony megoldásokat részesítenek előnyben, míg az EU-s vállalkozások fejlettebb információbiztonsági rendszereket, például nyílt forráskódú SIEM-megoldásokat alkalmaznak [48, 50].

A kkv-k rugalmassága és dinamikája előnyt jelent a gyors alkalmazkodásban, azonban méretükből adódóan korlátozottak az erőforrásaik [51, 52]. A digitális infrastruktúra kiépítését pénzügyi korlátok és technikai ismeretek hiánya fékezi, a kockázatkezelési folyamatok bevezetését gyakran a megfelelő eszközök és technikák hiánya gátolja [57–62]. A digitalizáció előnyei ellenére a magyar kkv-k digitalizáltsága az EU-átlag alatt van, különösen a mikro- és kisvállalkozások esetében [71–77]. A vállalati digitalizációt befolyásolja a szervezet mérete, kora, az alkalmazottak digitális készsége, valamint a döntéshozatali és kutatás-fejlesztési együttműködések [72–75].

A kiberbiztonság kritikus terület, mivel a kkv-k ki vannak téve kibertámadásoknak, vírusoknak, adathalászatnak és social engineering támadásoknak [65–68]. A támadások többségét emberi hiba okozza, ezért a munkavállalók biztonságtudatossága és képzése alapvető fontosságú [66, 67, 118]. Az ISO 27001:2022 bevezetése segíti az információbiztonsági robusztusság növelését és az alkalmazottak tudatosságát [79].

Információbiztonság és biztonságtudatosság

Az információbiztonság az adatok, rendszerek és eszközök védelmét jelenti, míg az emberi tényezők kritikus szerepet játszanak annak fenntartásában [117, 118]. A biztonságtudatosság az egyén tudását, készségeit és képességét jelenti a fenyegetések felismerésére és kezelésére [132–135]. A munkavállalók kognitív képességei, életkora, iskolázottsága és szakmai tapasztalata

befolyásolják az információbiztonsági magatartást [131, 169–172]. A tapasztalat, oktatás és kiberbiztonsági képzés pozitívan hat a tudatosságra [174–175]. A közösségi média és az OSINT-források jelentős kockázatot hordoznak, ezért a munkavállalók folyamatos tájékoztatása és oktatása kiemelt feladat [176–183].

Kiberbiztonság

A kiberbiztonság az informatikai rendszerek, adatok és hálózatok védelmét jelenti a támadásoktól, jogosulatlan hozzáféréstől és károsodástól [198]. Magyarország a 2024-es Global Cybersecurity Index alapján a Tier 2 – Advancing kategóriába tartozik, és leginkább technikai intézkedések fejlesztésére van szükség [189]. A kiberbiztonsági célok a CIA-elven alapulnak: bizalmasság (confidentiality), sértetlenség (integrity) és rendelkezésre állás (availability) [202, 203]. A kkv-k számára a kiberbiztonság kritikus, mivel az internetre csatlakoztatott eszközök és felhőszolgáltatások növelik a sebezhetőséget, és az emberi tényezők jelentik a legnagyobb kockázatot [65–68, 159–166].

3 Célkitűzések

A hazai kis- és középvállalkozások (kkv-k) digitális jelenléte sok esetben hiányos vagy nem megfelelő: közel felük nem rendelkezik saját honlappal vagy webáruházzal, illetve ha van is, annak karbantartása rendszertelen A hazai kis- és középvállalkozások (kkv-k) digitális jelenléte sok esetben hiányos vagy nem megfelelő: közel felük nem rendelkezik saját honlappal vagy webáruházzal, illetve ha van is, annak karbantartása rendszertelen [4]. A közösségi médiában való megjelenés hiánya, valamint a dolgozók otthoni munkavégzését támogató digitális infrastruktúra kiépítetlensége tovább erősíti az alacsony digitalizáltsági szintet. Szerb és munkatársai [5] rámutattak, hogy a magyar kkv-k számára a legnagyobb problémát a termékinnováció és a versenyelőny hiánya jelenti.

A digitális infrastruktúra kialakítása érdekében elengedhetetlen a stratégiaváltás [6, 7]. A kkv-k ugyanakkor korlátozott emberi és pénzügyi erőforrásokkal rendelkeznek, ami megnehezíti hosszabb távú stratégiák kidolgozását [8]. További kihívást jelent a meglévő rendszerek integrálása, a szállítói kockázatok kezelése, valamint az ügyfelek bizalmának fenntartása az információbiztonság követelményei mellett [9]. A kiberbiztonsági trendek közé tartozik a felhőszolgáltatások és intelligens szoftvercsomagok egyre szélesebb körű alkalmazása, még akkor is, ha ezek jelentős költségekkel és szakképzett személyzet szükségességével járnak [10, 11]. A kkv-k gyakran alábecsülik a kiberbiztonsági fenyegetéseket, ami fokozott sebezhetőséghez vezet [10]. Más vizsgálatok ugyanakkor azt mutatják, hogy az

információbiztonsági intézkedések pozitívan kapcsolódhatnak a digitalizációhoz [12], jól érzékeltetve a biztonsági aggályok és a digitális fejlesztések közötti komplex kapcsolatot.

A felhőhasználat a kkv-k számára több szempontból előnyös – hozzájárulhat a működési hatékonyság növeléséhez és az innováció erősödéséhez [13] –, ugyanakkor a bevezetést jelentősen befolyásolják a biztonsági kihívások. A kkv-knak olyan stratégiákat kell alkalmazniuk, mint a robusztus hozzáférés-ellenőrzés, a fenyegetések folyamatos nyomon követése, az alkalmazottak képzése, az irányítási keretrendszereknek való megfelelés és az adatok titkosítása [9]. A felhőszolgáltatások testreszabása és a biztonságos integráció átfogó ütemtervének kidolgozása kulcsfontosságú [13].

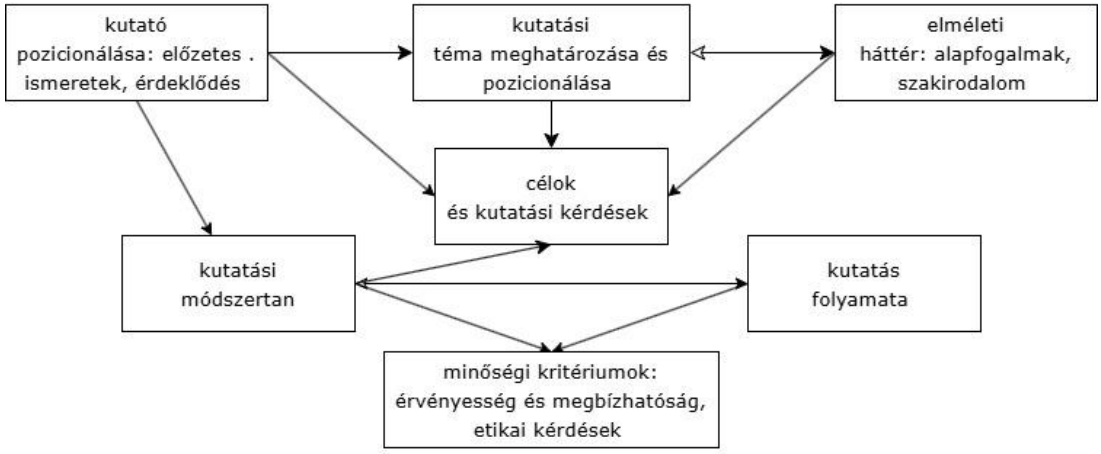
A kutatásban a felhő fogalmát a National Institute of Standards and Technology (NIST) meghatározása alapján értelmezem, amely szerint a felhő egy olyan modell, amely bárhonnan, bármikor, kényelmesen hozzáférést biztosít testre szabható digitális erőforrásokhoz, a szolgáltató közvetlen közreműködése nélkül [14].

A szakirodalmi áttekintés alapján a hazai kkv-k felhőhasználatával kapcsolatban több kutatási hiányosság azonosítható. Ide tartozik a felhő alkalmazásának akadályai, a szolgáltatáshoz kapcsolódó biztonsági és adatvédelmi kérdések, a szolgáltatás gazdasági előnyei, a bevezetés technológiai és technikai kihívásai, valamint az adatvédelmi előírások és szabályozások köre [15]. Kutatásom célja a magyarországi kkv-k esetében azoknak a tényezőknek a feltárása, amelyek az alacsony információbiztonsági tudás és tudatosság mellett is ösztönözhetik a felhőszolgáltatások tudatos és biztonságos használatát. További cél a kkv-k versenyképességének növelése a felhő igénybevételével, miközben az információbiztonsági szint is emelkedik. A kutatás során külön figyelmet kapnak azok a bizonytalanságok és visszatartó tényezők, amelyek elhárítása elősegítheti a felhőszolgáltatások szélesebb körű adaptációját.

4 Vizsgálati módszerek

Jelen kutatás szakértői interjúkra épült, amelyek elsődleges célja a kis- és középvállalkozások, valamint a felhőszolgáltatások közötti kapcsolat feltárása és megértése volt. Az elemzés során nem alkalmaztam előzetesen kidolgozott kódrendszert; a kódok az interjúszövegek iteratív feldolgozásának eredményeként alakultak ki [261]. A kutatás egyik célkitűzése annak vizsgálata volt, hogy a megkérdezett szakértők milyen ismeretekkel rendelkeznek a felhőszolgáltatásokról. A választott módszertan további előnye, hogy lehetővé tette a szövegek kontextuális elemeinek figyelembevételét is, amelyek jelentős befolyást gyakorolhattak a

vizsgált témák értelmezésére [262]. A kutatási keret és folyamat, valamint az ezek közötti összefüggések szemléltetésére a 1. ábra nyújt áttekintést. A kutatási folyamat több egymással szorosan összekapcsolódó elemből épül fel, amelyek kölcsönösen hatást gyakorolnak egymásra.



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

A primer adatokat félig strukturált interjúk révén gyűjtöttem, amelyeket az ATLAS.ti szöveganalitikai szoftver segítségével dolgoztam fel. A tartalomelemzés módszertanát alkalmazva a vizsgálat nem csupán a szövegek közvetlen tartalmára, hanem azok kontextuális összefüggéseire is kiterjedt. Az elemzés fókusza nem a nyelvtani szerkezeten, hanem a szavak, mondatok és bekezdések jelentésén alapult, lehetővé téve a szövegen túlmutató, általánosabb jelenségekre vonatkozó következtetések levonását [261]. A kutatás során 2024 januárja és októbere között összesen 34 félig strukturált interjút készítettem: 18 kkv-val és 16 felhőszolgáltatóval/disztribútorral. A válaszadók kiválasztása személyes szakmai kapcsolatok, ajánlások, valamint a Nemzeti Cégtár online adatbázisa alapján történt. A kkv-k esetében törekedtem vezető beosztású munkavállalók megszólítására, míg a szolgáltatói oldalon a felhőszolgáltatások és a kkv-szektor ismerete jelentette a fő kiválasztási szempontot. Az interjúk online formában zajlottak, átlagosan 1–1,5 órás időtartamban. Nyitott kérdések és rugalmas interjúvázlat biztosították a témák alapos feltárását, miközben lehetőség nyílt az egyéni tapasztalatok részletes kifejtésére. Az interjúalanyok számára bizalmas, nyitott légkört teremtettem, amely elősegítette a mélyebb tartalmak megosztását.

A beszélgetések a következő főbb témakörökre terjedtek ki:

1. **Demográfiai adatok** (nem, kor, beosztás, munkatapasztalat),
2. **Vállalati jellemzők** (iparági besorolás, cégméret, IT-tapasztalat),

3. **Információbiztonsági helyzet** (hazai és nemzetközi összevetésben),
4. **Felhőszolgáltatások ismerete** és tájékozottság,
5. **Trendek és motivációk**,
6. **Akadályok és kihívások** a felhőhasználatban.

A kkv-válaszadók között 12 férfi (70,6%) és 5 nő (29,4%) szerepelt, átlagéletkoruk 43,6 év (28–58 év közötti). A beosztások ügyvezetőktől és IT-vezetőktől szakmai pozíciókig terjedtek, az iparági eloszlás széles skálát fedett le (pl. programozás, építőipar, gyógyszeripar, élelmiszeripar).

A kutatás során a Grounded Theory (GT) módszertant alkalmaztam, amely az interjúadatok induktív feldolgozására épül. Az ATLAS.ti szoftver hatékonyan támogatta az elemzést, lehetővé téve a nagymennyiségű kvalitatív adat (interjúátiratok) rendszerezését, kódolását és a mintázatok feltárását [266, 271, 273].

Az interjúk elemzése során az alábbi módszereket alkalmaztam:

1. **Kódolás** – az adatok rendszerezése és a témák azonosítása.
2. **Kódgyakoriság elemzés** – a főbb témák kiemelése.
3. **Kontextuselemzés (kódhálózat)** – a kapcsolatok és ok-okozati összefüggések feltárása.
4. **Szentimentelemzés** – a rejtett attitűdök és érzelmi aspektusok azonosítása.

A több szintű elemzés lehetővé tette, hogy ne csak a felhőszolgáltatásokkal kapcsolatos tudatos véleményeket, hanem a mélyebb attitűdöket és percepciókat is feltárjam, amelyek alapvetően befolyásolják a kkv-k felhőhasználathoz való hozzáállását.

A kódolás fő lépései

1. **Nyílt kódolás** – a szövegrészletek azonosítása, összehasonlítása, kategorizálása; kulcsfogalmak feltárása [267, 274].
2. **Axiális kódolás** – a kategóriák közötti összefüggések, kontextusok és feltételek azonosítása, mélyebb értelmezés kialakítása [268, 275].
3. **Szelektív kódolás** – a központi kategória kijelölése, a kategóriák integrálása koherens elméletbe [276, 277].

A folyamat iteratív, az új adatok fényében a kódok és kapcsolatok folyamatosan finomodtak, amíg el nem értem az elméleti telítődést.

5 Az interjúadatok feldolgozásának fázisai

1. **Adatok megismerése** – átiratok olvasása, tisztítása, ATLAS.ti-be importálás.
2. **Kezdeti kódolás** – szakirodalomra építve, induktív folyamatban 94 kód, 654 szövegrészlet azonosítása.
3. **Témák keresése** – kódok összevonása, átalakítása; 3 információbiztonsági és 6 felhőszolgáltatási téma létrehozása.
4. **Kódok felülvizsgálata** – újbóli kódolás, alkódok kialakítása a mélyebb jelentések feltárására.
5. **Kódcsoportok létrehozása** – a kutatási célkitűzésekhez kapcsolódó fő kategóriák azonosítása (motiváció, előnyök, akadályok, elvárások, információbiztonsági kérdések).
6. **Kódok véglegesítése** – az empirikus megállapítások összefoglalása, vizualizált kódstruktúra létrehozása.

A végleges kódfa két fő ágra épült: információbiztonság és felhőszolgáltatás. Mindkettő további alcsoportokra bomlott (pl. vállalati kultúra, partneri kapcsolatok, kihívások, előnyök), amelyek komplex képet adnak a kkv-k informatikai és biztonsági gyakorlatáról.

6 Új tudományos eredmények

Az interjúk alapján az információbiztonság és a felhőhasználat kapcsolata összetett és dinamikus jelenség. A belső folyamatok, a vezetői döntések és a szervezeti kultúra meghatározó szerepet játszanak a biztonsági gyakorlatok kialakításában. A felhő legfontosabb előnye a rugalmasság, ugyanakkor alkalmazását gyakran hátráltatja a szakértelem hiánya és a költségterhek. A vezetőség szerepe kiemelkedő, mivel döntéseik alakítják a szabályozást és a belső kommunikációt, amelyek az információbiztonság alapját képezik.

Tézis 1 A kkv vezetőivel folytatott interjúk szövegelemzése során azonosítottam a felhőszolgáltatás bevezetésének releváns akadályait, melyek felismerése hozzájárul a felhőszolgáltatás bevezetés hatékony leküzdéséhez. [15, 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. [15, 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.[15, 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.

A bemutatott kutatási eredményeket és a hozzájuk kapcsolódó kutatási kérdéseket, előfeltevéseket az alábbi táblázat foglalja össze. A kkv-k felhőszolgáltatás-bevezetését számos szervezeti, technológiai és pszichológiai akadály befolyásolja, mint a reaktív döntéshozatal, szaktudáshiány, költségfókusz és bizalomhiány. A szolgáltatók a szervezeti és kulturális kihívásokat, míg a kkv-k a gyakorlati előnyöket és működési szempontokat emelik ki. Az eltérő szemlélet miatt gyakran kommunikációs és elvárásbeli félreértések alakulnak ki a felhőhasználat során. A sikeres digitális és biztonsági átállás érdekében integrált, emberközpontú megközelítés szükséges, amely figyelembe veszi a munkavállalói attitűdöket, képzési igényeket és belső kommunikációt, ezzel elősegítve az elkötelezettséget és a technológiák elfogadását. Továbbá a rövid távú költségmegtakarításra fókuszáló döntések a hosszú távú biztonsági és működési előnyöket veszélyeztetik. A kódhálózati elemzés szerint a kkv-k információbiztonságát a szervezeti és technológiai tényezők, a felhőhasználatot pedig motivációk, előnyök, akadályok és elvárások együttese alakítja. Érzelmi mintázatok nem

azonosíthatók a felhőszolgáltatások kapcsán; a szentiment elemzés szerint a kkv-k hozzáállása óvatos, ambivalens, gyakran negatív vagy semleges. A következőkben 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.	kód-gyakoriság	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

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

A modern vállalatok működésében az információbiztonság és a folyamatos elérhetőség kulcsfontosságú tényezőkké váltak. A digitális transzformáció és a mesterséges intelligencia terjedésével a szervezetek egyre nagyobb mértékben támaszkodnak informatikai megoldásokra, amelyek ugyan előnyöket kínálnak, de fokozott kockázatokat is jelentenek. A felhőszolgáltatások különösen a kkv-k számára kínálnak rugalmasságot és költséghatékonyságot, elősegítve a versenyképesség megőrzését. Ugyanakkor a biztonságtudatosság hiánya sebezhetővé teszi a vállalatokat a kibertámadásokkal szemben. A

kutatás és az interjúk alapján a kockázatok mérséklésére a következő lépések kiemelten fontosak:

- Információbiztonsági képzések kiterjesztése a munkavállalók körében,
- Biztonsági intézkedések (pl. többfaktoros hitelesítés, rendszeres mentések) bevezetése,
- Kockázatelemzés a digitális átállás előtt,
- Rendszeres biztonsági auditok a folyamatos fejlesztés érdekében.

Az interjúk elemzését a 2. táblázat foglalja össze három gondolat mentén, amelyek összhangban állnak a TOE-modell szerkezetével:

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	-	-

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

Az interjúk alapján a kkv-k stratégiai döntéseit leginkább a technológiai innováció, az információbiztonság és a költséghatékonyság határozza meg. A digitális átalakulás és a felhőszolgáltatások alkalmazása kulcsfontosságú a versenyképesség megőrzésében, miközben a képzés és tudatosság erősítése elengedhetetlen. A vállalatok számára a hibrid megoldások és a versenyelőny megtartása jelentik a hosszú távú siker alapját.

7 Az eredmények hasznosítási lehetősége

A felhőszolgáltatások stratégiai szintű bevezetése a kkv-k számára gyakorlati jelentőséggel bír, mivel hozzájárulhat a működési hatékonyság, a skálázhatóság és az adatok hozzáférhetőségének javításához. Emellett olyan kritikus kihívásokat is kezel, mint az információbiztonság, valamint a meglévő rendszerekkel való integráció. A vezetők és döntéshozók számára elengedhetetlen, hogy mérlegeljék a felhő bevezetésének szükségességét, az érzékelt előnyöket, valamint a teljesítménynövekedés mérhetőségének módjait. A felhő alkalmazását elsősorban olyan észlelt előnyök mozgatják, mint a tranzakciós költségek csökkenése, a szolgáltatásminőség javulása és az adatok jobb hozzáférhetősége [302]. Ezek a tényezők hosszabb távon hozzájárulhatnak a kkv-k gazdasági teljesítményének növeléséhez és versenypozíciójuk erősítéséhez [303, 304]. Ugyanakkor a bevezetés sikeressége több feltételtől is függ: a szervezeti felkészültségtől, a felsővezetés támogatásától és az észlelt hasznosságtól [303, 305]. A kkv-knak figyelembe kell venniük saját erőforráskorlátaikat, a biztonsági kihívásokat és az egyedi igényeket, amikor a felhőtechnológiák alkalmazásáról döntenek [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 Irodalmi hivatkozások listája/ Irodalomjegyzék

[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] 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

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

[6] 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)

[7] 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)

[8] 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)

[9] 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

[10] 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

[11] 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)

[12] 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

[13] 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

[14] 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

[15] 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

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

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

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

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

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

[21] 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

[22] 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

[23] 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

[24] 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

[25] 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

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

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

[28] 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

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

[30] 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

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

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

[33] 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

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

[35] 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

[36] 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

[37] 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/

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

[39] 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

[40] 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

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

[42] 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)

[43] 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

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

[45] 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

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

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

[48] 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

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

[50] 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

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

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

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

[54] 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

[55] 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

[56] 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

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

[58] 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

[59] 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

[60] 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

[61] 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

[62] 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

[63] 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

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

[65] 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

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

[67] 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)

[68] 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

[69] 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)

[70] 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)

[71] 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

[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 2024) 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., VAJJHALA, 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

9 Publikációk

9.1 A tézispontokhoz kapcsolódó tudományos közlemények

[1] 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

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

[3] 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

[4] 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

[5] 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

[6] 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

9.2 További tudományos közlemények (opcionális)

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

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

[9] 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