ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS

MÓDNÉ TAKÁCS JUDIT

Generációs sajátosságok és kiberbiztonsági tudatosság: A Z és Alfa generáció kiberbiztonsági attitűdjének és rezilienciájának integrált vizsgálata

Témavezető: Dr. Pogátsnik Monika

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2026.03.20.

Nyilvános védés teljes bizottsága:

Elnök:
Prof. Dr. Berek Lajos
Titkár:
Dr. Herr Orsolya
Tagok:
Dr. habil Tóth András
Piglerné Dr. habil. Lakner Rozália
Dr. Horváth Richárd
Bírálók:
Dr. habil Pődör Andrea
Dr. Kattein-Pornói Rita

Nyilvános védés időpontja:
2026.

Nyilatkozat a munka önállóságáról, irodalmi források megfelelő módon történt idézéséről

NYILATKOZAT

A MUNKA ÖNÁLLÓSÁGÁRÓL, IRODALMI FORRÁSOK

MEGFELELŐ MÓDON TÖRTÉNT IDÉZÉSÉRŐL

Alulírott Módné Takács Judit kijelentem, hogy a Generációs sajátosságok és kiberbiztonsági tudatosság: A Z és Alfa generáció kiberbiztonsági attitűdjének és rezilienciájának integrált vizsgálata című benyújtott doktori értekezést magam készítettem, és abban csak az irodalmi hivatkozások listáján megadott forrásokat használtam fel. Minden olyan részt, amelyet szó szerint, vagy azonos tartalomban, de átfogalmazva más forrásból átvettem, a forrás megadásával egyértelműen megjelöltem.

Budapest, 2026. március 20.

.....

név

TARTALOMJEGYZÉK

BEVEZETÉS

„Minden ember két univerzumba születik:
a fizikai valóságba és a kibervilágba.”
- Marcel Danesi

A digitális korban a felnövekvő generációk tagjai számára az információs technológia, az online kapcsolattartás és az azzal járó kockázatok, veszélyek mindennapi életük elengedhetetlen részét képezik. A Digital 2024 jelentése alapján [1] az internetezők száma világszerte 5,35 milliárdra tehető, mely a vizsgált évben 1,8 százalékkal növekedett. Magyarországon a fiatalok átlagos napi internethasználati ideje folyamatosan emelkedő tendenciát mutat, a 14–24 éves korosztályban napi 6,23 óra, az Alfa generáció körében 7–8 óra [1], [2]. A közösségi média platformok használata jelentősen növekszik évről évre, a fiatalok 85%-a aktív felhasználója legalább egy közösségi média felületnek [1]. A fokozott és egyre korábbi életkorban megjelenő online jelenlét következtében a fiatal, sebezhető generációk kiberbiztonsági tudatosságának megalapozott fejlesztése kiemelt társadalmi jelentőséggel bír. A kiberbiztonsági tudatosság fejlesztése azonban nem csupán az iskoláskorú fiatalok védelme szempontjából elengedhetetlen, hanem a munkaerőpiacra való felkészítés tekintetében is komoly jelentőséggel bír, hiszen a Z generáció tagjai már jelen vannak a munkaerőpiacon, az Alfa generáció tagjai belátható időn belül a munka világába lépnek.

Ahogy a kibertérben zajló munkafolyamatok mennyisége és komplexitása folyamatosan nő, az emberi tényező egyre inkább a középpontba került. Az emberi tényező az informatikai biztonság egyik legkritikusabb eleme, így a védekezés szempontjából is kiemelt jelentőségű, hiszen sikeressége nagymértékben azon múlik, hogy az egyén milyen tudatosan kezeli, mennyire biztonságtudatosan jár el [S-1]. A kiberbiztonsági oktatás viszont nem korlátozódhat csupán technikai kompetenciák fejlesztésére, és tudásátadásra. A technológiai fejlődés gyors ütemét figyelembe vevő, a puha készségek fejlesztését integráló [S-3], generációspecifikus pedagógiai módszereket követő, Ipar 4.0 és 5.0 elvárásaihoz illeszkedő, folyamatos fejlesztést célzó, gyakorlatorientált, élményalapú oktatási programok kialakítása szükséges [3], [4], [5].

A digitális írástudás tantervi integrációja hazánkban is megkezdődött, ugyanakkor bizonyos elemek, például a kibertudatossági kompetencia fejlesztése még korlátozottan jelenik meg az oktatási rendszerben [6]. Hatékony, generációspecifikus és egyéni tanulási utat támogató képzésfejlesztés azonban csak megalapozott empirikus ismeretek

birtokában valósítható meg, az érintett generáció felmérését, megismerését követően. Jelenleg a hazai kutatási környezet módszertani korlátai, a nem validált mérőeszközök alkalmazása és a reprezentativitás hiánya miatt, jelenleg nem áll rendelkezésre megfelelő empirikus alap az evidenciaalapú programfejlesztéshez. A kutatás célja ezért egy átfogó kiberreziliencia modell kidolgozása és validálása, amely integrálja a kiberbiztonsági tudatosság, a személyes reziliencia és a problémás internethasználat dimenzióit, feltérképezve a digitális bennszülött generációk valós kompetenciáinak és kockázati profiljait.

A tudományos probléma megfogalmazás, háttér és kontextus

A 21. században elterjedt digitális technológiák, a kiberfizikai rendszerek, 5G és a mesterséges intelligencia, mindennapi életünkbe való integrációjával a kiberbiztonsági fenyegetések is exponenciálisan növekedtek [7]. Az Ipar 4.0 és 5.0 elvárja az emberközpontú megközelítés fókuszba helyezését, ezáltal új kihívásokat eredményezve a munkaerő-piacon, az ember-gép kollaboráció és az etikai szempontok hangsúlyozása terén [8]. Az Ipar 5.0 túllép az automatizáción és a technológiai integráción, emberközpontú szemlélete a humán tényezőt helyezi előtérbe, így a jövő munkavállalóitól a technikai tudás mellett a kiberbiztonsági tudatosság, a reziliencia és az adaptív problémamegoldó képesség is alapelvárássá válik [S-1], [S-2], [9]. A kutatási eredmények [10] hangsúlyozzák a kibertér kettős természetét, mely egyszerre teszi lehetővé a globális kapcsolódást és egyúttal pszichoszociális kockázatokat is rejt. Az online világ veszélyei az egyénekre nézve bizonyítottan számos negatív mentális hatással jár, mint például a FOMO[1] effektus megjelenése, személyiségtorzulás, a szociális készségek és személyes kapcsolatok csökkenése, az online kirekesztés és bántalmazás, technostressz, technoszorongás, félelem, technofóbia, feszültség, kiégés, különféle függőségek kialakulása, a pszichés működésre gyakorolt negatív hatások, a mentális egészség sérülékenysége, valamint a kiberbiztonsági fenyegetésekkel szembeni sebezhetőség [11], [12]. A felhasználókra nézve a fokozott és kifinomult kibertámadások, illetve a manipulációs eszközök használata komoly érzelmi terhet jelent. Különösen a fiatalokat érinti érzékenyebben, hiszen ők még nem rendelkeznek megfelelő védelmi ismeretekkel és szokásokkal a digitális világ fenyegetéseivel szemben. Kiemelten fontos a digitális készségeik, tudatosságuk, attitűdjük, gyakorlati jártasságuk folyamatos, célzott fejlesztése a megfelelő védelmük, mentális és digitális jóllétük érdekében [13]. A digitális

[1] Fear Of Missing Out, félelem a kimaradástól

készségek, a biztonságtudatos attitűd nem csupán a technikai ismereteket, kockázatok felismerését, és azok kezelését, megelőzését jelenti, hanem azon mentális készségeket is, amelyek segítenek a támadások során ért stresszt, érzelmi reakciókat kezelni és feldolgozni. Emellett jelenti még a folyamatosan változó környezethez való alkalmazkodás képességét, a reziliens magatartást, a tiszta gondolkodást érzelmi terhelés mellett is [S-1], [14]. Hangsúlyt kell fektetni a reflektív készségek, megküzdési stratégiák és az adaptív gondolkodás fejlesztése mellett [15], a digitális stresszkezelés képességének biztosítására [16], [17], [S-4]. A kiberbiztonsági tudatosság, stresszkezelés és reziliencia fejlesztése tehát kiegészítik, erősítik egymást, hiszen a lelki egyensúly, a higgadtság megőrzése, a kognitív egészség kulcsfontosságú lehet az online fenyegetések hatékony megelőzésében és a kezelése során [18], [19]. A puha készségek, a digitális írástudás, az empátia, az alkalmazkodóképesség, valamint a naprakész tudás átadását és integrált fejlesztését célzó programok kialakítása elengedhetetlen ahhoz, hogy a felnövekvő generációkban kialakuljanak ezek az átfogó kompetenciák és a digitális ellenállóképesség [20].

A digitális átalakulás biztonsága a munkaerő folyamatos fejlesztését, rendszeres kiberbiztonsági ellenőrzéseket és tudatosságnövelő képzéseket igényel. A virtuális és fizikai környezet egyensúlyának megteremtése elengedhetetlen a technológiai előnyök maximalizálásához és a káros mentális hatások mérsékléshez. Az oktatási rendszer feladata a jövő generációinak felkészítése ezekre a kihívásokra. Magyarországon 2025 márciusában elfogadott új Kiberbiztonsági Stratégia [21] a tudatos, reziliens és biztonságos digitális társadalom megteremtését célozza. A digitalizáció a társadalmi fejlődés és jóllét alapvető eleme, amelyben kiemelt figyelmet kap a kiskorúak internetfüggősége, az információs csatornák veszélyei, a manipulatív tartalmak, az adatbiztonsági sérülékenységek és a kiberbiztonság tudatosságának folyamatos fejlesztése. A digitális világ veszélyei miatt fontos, hogy az emberek már korán megtanulják a kiberbiztonság alapjait, és több szakembert képezzünk ezen a területen. Ez alapvető feltétele annak, hogy társadalmunk biztonságosan és jól működjön.

Az Európai Bizottság cselekvési terve [22] és a NAT[2] 2020 [6] rendelkezései értelmében a magyarországi köznevelési intézményekben kötelezően bevezetésre került a digitális kultúra tantárgy, amely az alapvető digitális kompetenciák fejlesztését és a digitális

[2] Nemzeti Alaptanterv

írástudás megerősítését szolgálja. A tananyag lefedi az informatikai eszközhasználatot, hardver és szoftver ismereteket, vírusvédelmet, digitális írástudást, adatvédelmi alapelveket, problémamegoldást, algoritmizálást, programozást, valamint a web és mobiltechnológiákat. A kiberbiztonsági ismeretek, tudatosságfejlesztés azonban csupán felszínesen jelenik meg, nem a valós élethelyzetekben és munkaerőpiacon elvárható mélységben. A 32/2024. (VIII.8.) BM rendelet 12.§-a [23] előírja, hogy a közoktatási rendszerben kötelező a tanulók digitális kompetenciájának mérése az 5-11. évfolyamon, amelyet a 2023/24-es tanévtől kísérleti jelleggel vezettek be. Az Oktatási Hivatal által közzétett országos mérési eredmények azonban csak 2023-ig állnak rendelkezésre. A 2024-es digitális kultúra kompetenciamérés eredményei 2025. március 20-tól kizárólag egyéni vagy intézményi szinten érhetők el, nyilvános összefoglaló adatok nem hozzáférhetők [24]. A tanulók valós digitális felkészültségének mérési eredményeiről tehát nincs naprakész, átfogó kép, mely adathiányt okoz a területen.

A lakosság felmérését célozva a Nemzeti Kibervédelmi Intézet 2020-ban végzett egy országos lakossági felmérést [25] a biztonságtudatosság felmérése céljából. Az eredmények azt mutatják, hogy a kiberbiztonsági hozzáállás más és más a nők és férfiak, valamint a különböző korcsoportok esetében. A férfiak a biztonságosabb jelszavakra, a nők az adatvédelemre figyelnek jobban, kevesebb információt osztanak meg magukról, ezzel védve magukat a profil-alapú támadásokkal, személyazonosság lopással szemben, valamint az idősebbek a biztonsági frissítések telepítésében fegyelmezettebbek a fiataloknál. A felmérés eredménye kis mértékben hasznosítható a Z és Alfa generáció vizsgálatához, hiszen a fiatal generációk tagjai természetes könnyedséggel navigálnak a digitális térben, viszont hajlamosak kockázatos online viselkedésre, ami veszélyezteti digitális jóllétüket és biztonságukat [29].

Jelenleg hiányoznak azok az empirikus kutatások, amelyek átfogóan vizsgálják a Z és különösen az Alfa generáció kiberbiztonsági tudatosságát, és feltárják a technikai kompetenciákat, a puha készségek és a biztonsági attitűd közötti komplex összefüggésrendszert, ami elengedhetetlen a jövő digitális rendszereinek biztonságos működtetéséhez. A Z és Alfa generáció körében eddig nem készült Magyarország vonatkozásában multidimenziós kiberreziliencia modell és hiányoznak azok a generációspecifikus, holisztikus pedagógiai megközelítések, amelyek a kiberbiztonsági attitűdöt komplex módon, annak kognitív (a kiberveszélyekkel kapcsolatos tudást), affektív (az online kockázatokkal kapcsolatos érzelmi reakciók, stressz, szorongás és

aggodalom), valamint konatív (viselkedési szándék a preventív, megelőzésen alapuló biztonsági magatartás elérésére) dimenzióit integrálva fejlesztenék.

Célkitűzés(ek)

Mivel az online támadások elsősorban az emberi gyengeségeket célozzák, a hatékony kiberbiztonság viselkedésalapú kérdés, amelyben központi szerepet játszik a biztonsági attitűdök megértése és fejlesztése. A kutatás első szakasza vegyes logikájú, ahol a deduktív kvantitatív szakaszt induktív kvalitatív fázis követi az eredmények mélyebb értelmezése céljából. A vizsgálat a Z és Alfa generáció kiberbiztonsági attitűdjét, problémás internethasználati szokásait, pszichológiai rezilienciáját és generációspecifikus viselkedési mintázatait térképezi fel Fejér vármegyében magyar nyelvű mérőeszköz adaptálásával és validálásával.

A kutatás további célja egy többdimenziós kiberreziliencia-modell kidolgozása és validálása a Z és Alfa generációs fiatalok körében. A kutatás kvantitatív módszertant alkalmaz, amely egy induktív, feltáró szakaszból és egy deduktív, megerősítő szakaszból épül fel. A vizsgálat középpontjában a kiberbiztonsági attitűd, a pszichológiai reziliencia és a problémás internethasználat komplex kapcsolatrendszerének feltárása áll, különös tekintettel a generációk közötti különbségekre. Elméleti szinten a kutatás célja, hogy egy átfogó, reflektív mérési modellen alapuló strukturális keretet biztosítson a digitális bennszülött generációk kiberrezilienciájának megértéséhez. Ez a modell abból indul ki, hogy a kiberreziliencia összetett jelenség, amelyet több különálló, de összefüggő tényező együttesen jellemez. A modellben a reziliencia egy fontos prediktorként, míg a problémás internethasználat egy releváns kockázati tényezőként jelenik meg a kiberbiztonsági attitűd alakulásában. Gyakorlati szempontból a kutatás célja, hogy azonosítsa a generációspecifikus kiberreziliencia profilokat, összefüggéseket és elősegítse a generációspecifikus prevenciós programok tervezését.

A kutatás eredményei tehát empirikus alapot biztosítanak a Z és Alfa generáció online térbeli szokásainak feltérképezésében, kiberreziliencia-profiljának megértéséhez, valamint validált mérőeszközt nyújtanak a magyar oktatási és szervezeti kontextusban történő további alkalmazáshoz. Az azonosított generációspecifikus mintázatok hozzájárulhatnak az evidenciaalapú prevenciós programok és oktatási intervenciók kidolgozásához.

A téma kutatásának hipotézisei, kutatási kérdések

A modell központi elmélete, hogy az egyének esetében magas kiberreziliencia akkor alakul ki, amikor erős kiberbiztonsági tudatosság párosul magas rezilienciával és alacsony problémás internethasználattal. A kiberreziliencia tehát három kulcskomponensből épül fel. A kiberbiztonsági tudatosság, reziliencia és az inverz problémás internethasználat együttesen alkotják a kiberreziliencia multidimenziós modelljét, amely előre jelezheti az egyén adaptív és biztonságos online attitűdjét, egészséges működését a kiberfenyegetésekkel szemben. A kutatás kiberreziliencia koncepcionális modelljét az 1. ábra szemlélteti, mely a Z és Alfa generáció kiberbiztonsági attitűdjét és dimenzióit, a rezilienciáját és a problémás internethasználatát integrálja egy egységes keretrendszerben.

1. ábra Kiberreziliencia koncepcionális modellje a komponensek pszichológiai funkciója alapján [forrás: saját szerkesztés]

A kiberreziliencia a kiberbiztonsági tudatosság és reziliencia komponensek integrációja, melynek az egyik negatív prediktora a problémás internethasználat. A kiberreziliencia nem csupán technikai tudás, hanem az alkalmazkodóképesség, tudatos attitűdök és egészséges internethasználati szokások szinergiájából alakul ki. A modell

generációspecifikus megközelítést alkalmaz, hiszen a digitális világban születettek eltérő kihívásokkal és lehetőségekkel szembesülnek. A kutatásban a kiberreziliencia formatív konstrukcióként kerül értelmezésre, mivel a modell három különböző faktorból épül fel. A kiberbiztonsági tudatosság, mint tudás, attitűd és viselkedés, a reziliencia, mint megküzdési képesség és rugalmasság, valamint a problémás internethasználat, mint önszabályozási hiány együttesen határozzák meg a kiberreziliencia szintjét, nem egy egységes látens faktor indikátorai.

Kutatási kérdések és hipotézisek

K1: Milyen különbségek, összefüggések és ok-okozati kapcsolatok (direkt és indirekt hatások) figyelhetők meg a Z és Alfa generációk kiberbiztonsági tudatossága, rezilienciája és problémás internethasználata között, valamint hogyan befolyásolják ezeket a mintázatokat a demográfiai tényezők (nem, generáció, internethasználati idő)?

H1: A napi internethasználati idő és a problémás internethasználat közötti összefüggés erőssége szignifikánsan eltér nemek és generációs hovatartozás szerint.

H2: A reziliencia szintje szignifikáns különbségeket mutat a generációs hovatartozás és a nemek függvényében.

H3: A kiberbiztonsági tudatosság szintje szignifikáns eltéréseket mutat az internethasználat ideje, a nemek és a generációs hovatartozás függvényében.

K2: Milyen online helyzetek okoznak leggyakrabban szorongást vagy bizonytalanságot a fiatalok körében, és hogyan kezelik ezeket?

K3: Hogyan jellemezhetők a Z és Alfa generációs internetezők kiberreziliencia-profiljai, és milyen szignifikáns különbségek mutatkoznak a két generáció között ezen profilok és a kiberreziliencia aldimenziói mentén?

H4: A kiberbiztonsági tudatosság, pszichológiai reziliencia és problémás internethasználat alapján szignifikánsan elkülönülő kiberreziliencia-profilok azonosíthatók.

H5: Az Alfa generáció tagjai szignifikánsan eltérő kiberreziliencia profilt mutatnak a Z generációhoz képest.

Kutatási módszertan és a kutatás felépítése

A kutatás elsődleges célja Fejér vármegye Z és Alfa generációs diákjainak kiberbiztonsági attitűdjének, pszichológiai reziliencia szintjének, kiberrezilienciájának

valamit problémás internethasználatának integrált vizsgálata. A kutatási folyamat több módszertani elemet foglalt magába. A kutatás első szakasza az alapos **szakirodalomelemzés**, mely feltérképezi a digitális kor generációs kihívásait, definiálja a kiberbiztonsági tudatosság fogalmait, bemutatja a kiberbiztonsági kompetenciamérés nemzetközi és hazai eszközeit, valamint feltárja a generációs jellemzőket, a reziliencia humán és kiber aspektusait a stresszkezelés oldaláról, és feltérképezi a problémás internethasználat kockázatait (1. fejezet). A szakirodalom elemzés célja, hogy megteremtse az elméleti keretet a kutatásokhoz, és feltárja a legfontosabb tényezőket és összefüggéseket. Ezt követően bemutatásra kerülnek az **alkalmazott vegyes kutatási módszer metodológiai kerete, az alkalmazott mérési eszközök és adatelemzési stratégiák** (2. fejezet).

A kutatás második szakasza az **empirikus vizsgálat, amely kvalitatív és kvantitatív módszerekkel végzett felmérésből áll**. A 3. fejezet a **kérdőíves adatgyűjtés kvantitatív eredményeit** mutatja be, elemezve a generációs különbségeket a kiberbiztonsági tudatosság, reziliencia és problémás internethasználat területén, valamint korrelációs és prediktív elemzéseket végez. A 4. fejezet a **kvalitatív eredményeket** mutatja be az asszociációs technikát alkalmazó fókuszcsoportos interjúk alapján. A kvalitatív eredmények segítenek megérteni a generációspecifikus kiberbiztonsági szokásainak jellemzőit a résztvevők kiberrezilienciájának aspektusából.

A kutatás harmadik szakaszában **kialakításra** kerül a **kiberreziliencia multidimenziós modellje** (5. fejezet). Ezt követően bemutatásra kerülnek a **szintetizált eredmények**, amelyekkel párhuzamosan ismertetem a disszertáció **elméleti hozzájárulását és gyakorlati relevanciáját**, továbbá azonosítom a kutatás korlátait, és kijelölöm a jövőbeli kutatási irányokat (6. fejezet). A 7. fejezet röviden **összefoglalja** a főbb megállapításokat.

Az átfogó vizsgálat és az ebből levont következtetések olyan alapot nyújtanak az oktatási és képzési programokat jövőbeli kialakításához, melyek elősegítik a Z és Alfa generációk tagjainak biztonságos és tudatos online jelenlétét, és a 21. század elvárt készségeinek fejlesztését. A kutatásomat 2025. szeptemberében lezártam.

1 DIGITÁLIS KIHÍVÁSOK GENERÁCIÓS SZEMSZÖGBŐL

A digitális kor alapvetően meghatározza az egyének információhoz való hozzáférését, a kommunikációt és az ehhez kapcsolódó biztonsági intézkedéseket. A különböző generációk eltérő módon alkalmazkodnak az online tér kihívásaihoz és lehetőségeihez. Ebben a fejezetben a kiberbiztonsági tudatosság jelentőségét, a Z és Alfa generáció sajátosságait, különbségeit, a túlzott internethasználat kérdéskörét, a mindennapi életet átszövő stressz kezelésében fontos reziliencia készség online aspektusát térképezem fel a szakirodalom elemzés segítségével.

1.1 A kiberbiztonság jelentősége a 21. században, fogalmi és elméleti keretek

A kiberbiztonság a 21. században túlmutat a technológiai dimenzión, és a társadalmi, gazdasági stabilitás meghatározó tényezőjévé vált. A következőkben a terület fogalmi és elméleti keretei kerülnek bemutatásra, a kulcskoncepciók és a jelenkori, generációspecifikus kihívások tükrében.

1.1.1 Kibertér, kiberbiztonság és kiberbiztonsági tudatosság

A szakirodalomban a kibertérnek számos meghatározása olvasható. A kibertér (angolul cyberspace) kifejezés eredete a görög „*kyber*” szóból származik, amelynek jelentése hajózni vagy navigálni [26]. Maga a fogalom nehezen definiálható, hiszen ez egy összetett, globális és dinamikusan változó digitális ökoszisztéma, amelyben az emberek, számítógépek, hálózati rendszerek és eszközök egy információs környezeten keresztül kommunikálnak, itt tárolják az adatokat és dolgozzák fel azokat. Tehát a kiberbiztonság a kibertér, az informatikai rendszerek és adatok védelmét szolgáló technikai, szervezeti és jogi intézkedések összessége [27]. A kibertér fogalmát Magyarország Nemzeti Kiberbiztonsági Stratégiája (2025) definiálja [21], mely szerint a kibertér globális, összekapcsolt elektronikus rendszerek hálózata, ahol adatok és információk áramlanak, a társadalmi és gazdasági folyamatainkat érintően. Ennek a globális hálózatnak a része a magyar kibertér, ahol az elektronikus rendszerek sebezhetősége, a kiberbűnözés és a biztonsági incidensek száma évről évre folyamatosan növekszik [21], [27].

A kiberbiztonság a dinamikus, rizikó-alapú, társadalmi-technikai kihívásokkal teli globális digitális környezetben folyamatos adaptációt igényel, és a modern társadalom

működésének kulcsterülete. Célja az adatok, rendszerek és hálózatok bizalmasságának, sérthetetlenségének és rendelkezésre állásának védelme technikai, stratégiai és nemzetközi együttműködésen alapuló intézkedésekkel [9], [28].

A 21. századi kiberfenyegetések dinamikus és adaptív természete miatt a védekezés sem lehet statikus. A kiberbiztonsági tudatosság egy kompetencia, mely folyamatos fejlesztést igényel [29]. Jelentősége abban áll, hogy képessé teszi az egyéneket és szervezeteket a kockázatok proaktív felismerésére, kezelésére mielőtt a kár bekövetkezne. Ez a fajta védekező attitűd, gondolkodásmód és viselkedéskultúra csak folyamatos, a változásokra reagáló, személyre szabott oktatással és a modern technológia tudatos használatával érhető el [30], [S-4].

A kiberbiztonsági tudatosság egyrészt a kibertér és annak veszélyeivel kapcsolatos tudást, az ismeretek szerzésének, megértésének és feldolgozásának képességét, valamint annak gyakorlati megvalósításának igényét jelenti [31]. A kiberbiztonsági tudatosság képzésének, fejlesztésének célja az egyének felelős magatartásának biztosítása a kiberbiztonság terén, így fontos megérteni, a tudatosság, az egyéni jellemzők és az oktatás összefüggéseit a magatartásra gyakorlat hatásának szempontjából [32]. A tudatosság fejlesztése és mérése, a biztonságtudatosabb gondolkodásmód és magatartás kialakítása egy ciklikus, adaptív folyamat [33], mely túlmutat csak a képzésen, vagy a szabályozási követelmények betartásának képességén. A kutatások egyértelműen alátámasztják, hogy a felhasználói tudatosság növelése a megfelelő technikai védelmi intézkedések mellett az egyik leghatékonyabb kiberbiztonsági védelem [34].

1.1.2 A kiberbiztonsági tudatosság dimenziói és mérési modelljei

A szakirodalom [35], [36] egybehangzóan hangsúlyozza, hogy a humán tényező az egyik kritikus eleme a kiberbiztonságnak, az incidensek túlnyomó többségét (74%) [37] emberi mulasztások idézik elő. Az alacsony kiberbiztonsági tudatosság hozzájárul a kiberfáradtság kialakulásához és csökkenti a proaktív védekezési hajlandóságot, miközben az orosz-ukrán háború kezdete óta a kiberfenyegetettség 97 százalékkal növekedett a szervezeteknél [38]. A pszichológiai, viselkedési, demográfiai és generációs különbségek jelentősen növelik a felhasználók sebezhetőségét a social engineering, a kognitív torzításokon alapuló manipuláció és a bennfentes fenyegetések ellen.

A biztonsági tudatosság vizsgálatában két fő megközelítés különíthető el. Az első a *technológiai kontroll központú*, amely külső ellenőrzésre és technológiai korlátozásokra

épít, illetve a *humánközpontú*, amely az egyéni képzésre és tudatosságfejlesztésre fókuszál. Az utóbbi esetében a fejlesztést nem kizárólag a tudásszerzés, hanem komplex pszichológiai és kulturális tényezők, mint motiváció, érzelmek, viselkedési minták és érdeklődés együttesen határozzák meg [39].

Az elmúlt évek felmérési eredményei [25], [40], [41] különböző számú és fajtájú dimenziókban mérték a biztonsági tudatosságot, hozzáállást és viselkedést az online térben, melyek nagyrészt az információbiztonsági tudatosság, ISA[3] fő dimenzióinak feleltethetők meg személyes adatvédelemre, adathalászatra, jelszókezelésre, proaktív védelmi stratégiára, online védelmi szokásokra, pénzügyi tudatosságra épülnek.

Az ISA mérése két dimenzióra koncentrál, a tudás-tudatosság és a viselkedés-megfelelőség aspektusaira. A validált mérőeszközök túlnyomórészt az első dimenzióra fókuszálnak, míg a tényleges viselkedési komponensek alulreprezentáltak [42]. Az ISA-mérés relatív fiatal kutatási területnek tekinthető, mivel a releváns mérőeszközök többsége az elmúlt évtizedben került kifejlesztésre. Rohan és munkatársai [43] szisztematikus szakirodalomelemzést végeztek az ISA mérőeszközök módszertani minőségének értékelésére. Háromfázisú, 19 kritériumos keretrendszerük szerint a jelenlegi ISA skálák jelentős validitási hiányosságokat mutatnak, ami új mérőeszközök fejlesztésének szükségességét jelzi. Egy 2023-as szisztematikus szakirodalomelemzés [44] eredményei alapján a kiberbiztonsági viselkedést több elméleti modell is magyarázza, de nincs egyetlen elmélet sem, amely lefedi az összes kiberbiztonsági viselkedést befolyásoló tényezőt. A biztonságtudatosság mérésében a KAB modell az egyik legegyszerűbb és leggyakoribb alkalmazott keretrendszer, hiszen tudás, attitűd és viselkedés három pillérére épít. A PMT[4] modell azt magyarázza, hogy az emberek hogyan reagálnak félelmet keltő üzenetekre, hogyan azonosítják a fenyegetéseket és miként küzdenek meg ezekkel. A TTAT[5] modell középpontjában a technológiai fenyegetésekkel kapcsolatos felhasználói tudatosság és az elkerülésre irányuló motiváció áll. A TPB[6] modell az észlelt viselkedéskontroll és az attitűdök szerepét veszi figyelembe a viselkedés befolyásolásában. Ugyan mindegyik modell széles spektrumát öleli fel a felhasználói tudatosság vizsgálatának, de mindegyiknek vannak korlátai. A PMT nem veszi figyelembe a társadalmi normákat és az egyéni különbségeket, feltételezve, hogy

[3] Information Security Awareness – Információbiztonsági tudatosság
[4] Protection Motivation Theory – Védelmi motivációs elmélet
[5] Technology Threat Avoidance Theory – Technológiai fenyegetések elkerülésének elmélete
[6] Theory of Planned Behavior – Tervezett viselkedés elmélet

mindenki hasonlóan reagál a fenyegetésekre, hiányoznak belőle a kognitív változók. A TTAT főleg a technikai intézkedésekre fókuszál, a TPB nem veszi figyelembe a motivációt és a szándékot befolyásoló személyes tényezőket.

1.1.3 Kiberbiztonsági kompetenciamérés módszerei és eszközei

Az egyik legnagyobb hazai felmérést Palicz és munkatársai [25] végezték, a Nemzetbiztonsági Szolgálat Nemzeti Kibervédelmi Intézet által végzett 2020-as felmérési eredményeinek alapján, mely a lakosság és a kis- és középvállalkozások biztonságtudatossági szintjét mérte. Az Európai Bizottság által működtetett EUSurvey webes platform felhasználásával történt a megkérdezés, amelyet az Európai Uniós Kiberbiztonsági Ügynökség (ENISA[7]) is alkalmaz. Az országos online felmérés ($N = 1104$) a kiberbiztonsági tudatosság, védekező magatartás és fenyegetettség-érzékelés vizsgálatára irányult. Az eredmények pozitív korrelációt mutattak a tudás és biztonsági gyakorlatok között, valamint nemi és generációs különbségeket azonosítottak. Az eredmények alapján a férfiak körében magasabb jelszóbiztonság, nők körében gyakoribb antivírus-használat, idősebb korosztályokban rendszeresebb biztonsági frissítések jellemzőek. A minta ugyan nem reprezentatív, de az eredmények összhangban vannak a hazai és nemzetközi kutatásokkal. Nyikes [45] nagymintás kutatása ($N = 1274$) többdimenziós megközelítésben elemezte a digitális kompetencia és biztonságtudatosság összefüggéseit generációs és területi bontásban, és felhasználói kockázati tipológiát dolgozott ki. Kiemelt eredménye a négykategóriás felhasználói besorolás („*Védendő*”, „*Veszélyes*”, „*Szerény*”, „*Magabiztos*” kategóriák), ahol a „*Veszélyes*” csoportot azonosította a legnagyobb kockázati csoportként. Gyaraki [46] 2022-ben végzett kutatásában saját szerkesztésű kérdőívvel vizsgálta a felhasználói magatartás és kiberbűnözés közötti összefüggéseket, különös tekintettel a humán kockázati tényezőre. A kutatás ellentmondásos biztonsági tudatosságot tárt fel, mivel míg a válaszok alapján 96%-a kerüli a nyilvános WiFi használatot (ami egyfajta biztonságtudatosságra utal), addig mindössze 15,1%-uk alkalmaz egyedi jelszavakat és 77,4%-uk kizárólag kisbetűket használ, ami jelentős jelszókezelési hiányosságokra utal. Továbbá kiemelte a munkahelyi és otthoni biztonságtudatosság közötti eltérést, amely a hibrid munkavégzés kontextusában szervezeti kockázatokat generálhat. A távmunka bevezetése

[7] European Union Agency for Cybersecurity - Európai Uniós Kiberbiztonsági Ügynökség

szignifikánsan növeli az adatszivárgási kockázatokat és az egyes biztonsági incidensek átlagos kárelhárítási költségeit [37].

A hazai kutatási környezetben limitált számú standardizált mérőeszköz elérhető a kiberbiztonsági tudatosság vizsgálatára. A fennálló empirikus tanulmányok túlnyomórészt ad hoc fejlesztésű, nem validált kérdőíveket alkalmaznak demográfiai változók kontrollálása mellett, amelyek nem biztosítanak reprezentatív és pszichometriai szempontból megalapozott eredményeket. A hazai kutatások hiányossága továbbá, hogy nem vizsgálják specifikusan az iskoláskorú, fiatal generációk kiberbiztonsági tudatosságát.

1.1.4 A Z és Alfa generáció digitális szocializációja és pszichológiai sajátosságai

A *Z generáció* (1995–2010 között születettek) az első valódi digitális, internet alapú bennszülött generáció, akiknek az online tér nem csupán egy eszköz, hanem a mindennapi életük alapvető szükséglete. Ebben a környezetben formálódik az identitásuk, kapcsolatokat építenek, tanulnak, tájékozódnak és információt gyűjtenek különféle témákban. A digitális platformok használata tehát befolyásolja a viselkedésüket, értékrendjüket és társadalmi attitűdjeiket [47]. Az *Alfa generáció* (2010-2024 között születettek) tagjai már teljes mértékben a digitális, érintőképernyős korszakba született bele. Számukra az okos, érintőképernyős technológiai eszközhasználat nem tanult, hanem természetes módon elsajátított készség, ami egyedülálló módon formálja kognitív fejlődésüket, társas kapcsolataikat és életmódjukat, miközben az online és offline világ erősen összemosódik az életükben [48].

Annak ellenére, hogy a fiatal generációk tagjai természetesen integrálják a digitális technológiákat mindennapi életükbe, ez nem jár együtt automatikusan a kritikus digitális írástudás és a reflektív médiatudatosság megfelelő szintjével, és sok esetben hiányzik az adatbiztonsági ismeretek megfelelő szintje is [49], [S-8]. A kortársak és az influenszerek meghatározó szerepet játszanak az értékrendjük, attitűdjeik és fogyasztási szokásaik kialakításában. A médiahasználatot egyéni szükségletek vezérlik, amelyek a szórakozást, az információszerzést és a társas kapcsolattartást foglalják magukban. Ezek a motivációk a digitális térben fokozottan személyre szabottá válnak [50]. Az online biztonsági viselkedést elsősorban a társas tanulási folyamatok, az utánzás mechanizmusa és az énhatékonyság-érzet befolyásolja [51], különösen a közösségi média platformokon [52].

Mindkét generációra jellemző, hogy médiahasználatuk adaptív, és gyorsan alkalmazkodik az új platformokhoz és technológiákhoz. A TikTok, Instagram, YouTube és Snapchat dominál a Z generáció körében, ahol a vizuális, gyorsan fogyasztható és beépített algoritmusok által személyre szabott tartalmak meghatározóak. Ez az igény szerinti, algoritmusvezérelt fogyasztási modell alapvetően átalakítja a médiahasználatot. Bár a Z generációhoz tartozó fiatalok digitálisan jártas felhasználók, kritikus médiatudatosságuk és adatvédelmi ismereteik gyakran elmaradnak technikai készségeiktől, ami fokozott sebezhetőséget eredményez [53], [54].

Az Alfa generáció még ezen is túlmutat, tagjai születésüktől fogva ajánlórendszerek által vezérelt, algoritmusok által irányított digitális környezetben nőnek fel [55]. A digitális környezet alapvetően meghatározza a tanulási szokásaikat, stílusukat, identitásformálódásukat és világhoz való viszonyukat. A platformok közül a TikTok, YouTube és Instagram dominál, ahol az Alfa generáció elsősorban humoros, táncos és autentikus reels videókat fogyaszt [56]. E korosztály nemcsak passzív befogadó, hanem aktív tartalomgyártó is, miközben elutasítja a promóciós tartalmakat [57]. Tehát nem passzív fogyasztók, hanem aktív tartalomgyártók, akik egyedi nyelvet és kódokat használnak kommunikációjukban. A fiúk inkább online játékokkal, politikai és sport tartalmak fogyasztásával töltik a szabadidejük nagy részét, míg a lányok személyes jellegű fotókat és videókat osztanak meg, szépségápolási és életstílushoz kapcsolódó influenszereket követnek [58]. Az ajánlórendszerek nemcsak a tartalomhoz való hozzáférést szabályozzák, hanem érdemben befolyásolják a gondolkodásmódot és az értékrendjüket is. Az algoritmusok olyan szűrőbuborékokat alakítanak ki, amelyek korlátozzák az eltérő nézőpontokkal való találkozást[59], [60]. A digitális szocializáció a fiatal generációk társadalmi normáinak, identitásának és fejlődési mintáinak átalakulását eredményezte. A Z és Alfa generációk esetében a digitális környezet már nem csupán kommunikációs eszközként funkcionál, hanem a szocializáció elsődleges színterévé vált. Meghatározó szerepet tölt be a társas kapcsolatok formálódásában, a tanulási szokások kialakulásában és az érzelmi fejlődés alakulásában. A fiatalok szocio-emocionális készségeinek kulcsfontosságú komponensei a késleltetett kielégülés tolerálásának, valamint az érzelmek és viselkedés szabályozásának képessége [55].

A Z generáció szocializációját elsősorban a kortárscsoportok erőteljes befolyása és digitális identitás tudatos kialakulása jellemzi. A digitális önreprezentáció sokszor többféle identitás párhuzamos kezelésével jár, ami komplex pszichoszociális

folyamatokat eredményez. Az influenszerek jelentős hatást gyakorolnak rájuk, míg bizonyos személyiség jellemzők, különösen az érzelmi labilitás, neuroticizmus növeli a befolyásolhatóságot [61]. A generáció tagjait magas szintű digitális kompetencia jellemzi, azonban ez nem minden esetben párosul fejlett kritikai gondolkodással, ami sebezhetőséget eredményezhet. A technológiai jelenlét hatása kettős természetű, mivel digitális kompetenciájuk jelentősen növeli a problémamegoldó és innovációs képességüket, munkavállalói elkötelezettségüket, ugyanakkor hozzájárulhat motivációs és figyelmi nehézségekhez is [55]. A digitális írástudás fejlesztése kulcsfontosságú a kompetenciafejlesztésükben, különösen megfelelő, generációspecifikus pedagógia és szülői támogatás mellett.

Az Alfa generáció esetében a digitális világba való korai belépés új kommunikációs és tanulási mintákat hoz létre, ahol a fizikai és digitális valóság összefonódása (phygital élmény) sajátos kognitív adaptációkat eredményez [55], a személyes interakciók csökkenése hátráltathatja a szociális készségek fejlődését [62]. Ez különösen kritikus a fejlődés korai szakaszaiban, az interperszonális tanulás során, amikor azt tanuljuk meg, hogyan kapcsolódjunk egymáshoz. E generáció digitális kompetenciájának fejlesztése még kialakulóban van, és kevés kutatás vizsgálja az innovációs képesség és a motiváció közötti kapcsolatot körükben. A digitális írástudás fejlesztése szülői irányítással, oktatási alkalmazásokkal és virtuális valósággal történik, azonban az önálló tanulás és a kritikus gondolkodás fejlesztése továbbra is jelentős pedagógiai kihívást jelent [63], [64]. Paradox módon a digitális eszközök, a mesterséges intelligencia alapú chatbotok vagy a virtuális valóság (VR) egyrészt érzelmi támogatást nyújtanak, másrészt túlzott használatuk miatt mentális egészségügyi kockázatot jelent, a valós megküzdési stratégiák elsajátításának gátlásával [65].

Az Alfa generáció esetében már korai életszakaszban megjelenik a digitális eszközhasználat, ami csökkentheti a személyes interakciók számát és befolyásolhatja a szociális készségek kialakulását [62]. Ez a rizikó hatványozottan érvényesül a speciális nevelési igényű gyermekek csoportjában, ahol a szociális tanulás eleve sérülékenyebb [66]. Ugyanakkor a technológia alapú fejlesztési módszerek (*avatar-alapú rendszerek, a VR-szimulációk, viselkedésalapú technológiák*) és a vegyes, blended módszerek bizonyítottan hatékonyan támogathatják a készségfejlesztést, empátiát, önkifejezést [67], [68].

Mindkét generáció mentálhigiénés támogatásában egyre nagyobb szerepet kapnak a digitális megoldások, VR-technológia és mesterséges intelligencia alapú chatbotok [69]. Ezek rövid távon hatékonynak lehetnek a szocio-emocionális készségek fejlesztésében és a mentális jóllét növelésében, azonban hosszú távú eredményességük elsősorban a személyre szabott és kortárs-támogatással integrált alkalmazásuktól függ [70].

1.1.5 A kiberbiztonsági tudatosság fejlesztésének generációs aspektusai

Kiberbiztonsági szempontból a digitális kompetencia és a biztonsági tudatosság közötti szakadék jelentős kockázatot jelent. A Z generáció tagjai technikai értelemben ugyan jártasak, de gyakran hiányzik belőlük a kritikus reflexió, ami sebezhetővé teszi őket adatbiztonsági fenyegetésekkel, manipulációval és félrevezetéssel szemben. A kiberbiztonsági oktatásnak ezért nem csupán technikai készségeket, hanem kritikus gondolkodást is kell fejlesztenie ebben a generációban, hogy képesek legyenek felismerni és kezelni a digitális térben megjelenő komplex biztonsági kihívásokat [49], [S-8].

A mai, technológiavezérelt, gyors ütemű világban a Z és Alfa generációk oktatási igényeinek kielégítésére a hagyományos pedagógiai módszerek már nem alkalmasak. Mindkét generáció számára a hibrid, phygital tanulási modellek támogatják hatékonyan a kognitív fejlődést. A technológiát tudatosan használó pedagógiai megközelítés elengedhetetlen a sikeres fejlesztésük érdekében [55]. A multimédiás eszközök, videók, prezentációk és grafikai elemek bevonása, valamint a rugalmas, adaptív értékelési módszerek elősegítik a digitális tudás gyakorlati alkalmazását [64]. A kutatások hangsúlyozzák [71], hogy a hibákból való tanulás és a gyors tartalomfeldolgozás képessége erősíti a tanulók ellenálló képességét a digitális kihívásokkal szemben, és támogatja a biztonságos, tudatos online jelenlét kialakítását. A gyakorlatorientált, együttműködésen alapuló és alkalmazkodó pedagógiai megközelítések kiemelt jelentőséggel bírnak, mivel ezek képesek a technológiai jelenlét pozitív hatásait maximalizálni, miközben enyhítik a negatív következményeket.

Az Alfa generáció még nagyon fiatal, a legtöbb kutatási adat a Z generáció végéről származik, és jelentős hiányosságok mutatkoznak a hosszú távú tanulmányok terén, különösen a mesterséges intelligencia (MI) hatásairól és az adatvédelemről.

1.2 Problémás internethasználat

A 21. században a problémás internethasználat egyre elterjedtebb jelenség, különösen a fiatalkorúak körében [13]. A COVID-19 pandémia jelentősen felgyorsította az online

világ térnyerését az otthonról végzett munka, home-office, a szabadidős tevékenységek, online játékok és az oktatás, különösen az online oktatás területén. A digitális átállás rugalmasabb munkavégzési és tanulási lehetőségeket teremtett. Ugyanakkor a mértéktelen internethasználat negatív következményekkel jár. Akadályozza az egyéni fejlődést, gyengíti a személyes kapcsolatokat, és a társas interakciók online térbe tolódásával növeli a kiberfenyegetéseknek való kitettséget. Megfelelő készségek, tudatosság, szakmai ismeret, naprakész tájékozottság, a digitális kompetencia folyamatos fejlesztése kulcsfontosságú a résztvevők védelme érdekében, különös tekintettel a fiatalabb korosztályra, akik még nem rendelkeznek a szükséges mértékletességgel és tudatossággal a digitális eszközök használata terén [S-3].

1.2.1 Elméleti modellek és definíciós keretek

A problémás internethasználat (PIH) vagy internetfüggőség (patológiás, maladaptív, túlzott, kompulzív internethasználat) jelenség multidiszciplináris tudományos kutatási terület, melynek definíciója vagy akár az elnevezését tekintve nem egységes [13]. Az internetfüggőség súlyosabb impulzuskontroll zavarnak tekinthető, mely teljes elszigetelődéshez vezethet, míg a problémás internethasználat káros következményekkel járhat a felhasználó életére, de nem feltétlenül eredményez elszigetelődést. Közös jellemzőjük a felhasználói kontroll elvesztése, és az online jelenlét korlátozásakor megjelenő szorongás, pszichés feszültség [72].

A problémás internethasználat az online kapcsolatok előtérbe helyezéséhez vezethet, ami hozzájárul a valós társas interakciók háttérbe szorulásához, fokozva a magányosság és a depresszió tüneteit [73]. Kialakulásának valószínűségét számos tényező növeli, különösen a digitális eszközök korai életkorban történő használata, a gyenge minőségű személyes és családi kapcsolatok, továbbá bizonyos személyiségjellemzők, mint a fokozott érzelmi labilitásra való hajlam és a szociális visszahúzódás. A serdülőkön végzett vizsgálatok kiemelt prediktív tényezők közé sorolják, a digitális eszközökkel való korai találkozást, valamint az iskolai környezethez kapcsolódó pszichológiai stresszt [13].

A problémás internethasználat tehát egy összetett jelenség, mely több formában jelentkezhet, mint a túlzott információszerzés, szerencsejáték függőség, online kapcsolatok, szexuális tartalmak, online vásárlás, valamint a számítógépes játék és virtuális világok terén [74]. A szakirodalom megkülönbözteti a generalizált internetfüggőséget, amely több dimenzióban, átfogó jelleggel nyilvánul meg, valamint a

specifikus internetfüggőséget, amely egy adott online tevékenységre összpontosul [13], [72].

1.2.2 Pszichológiai és kiberbiztonsági kockázatok

A PIH viselkedéses és pszichológiai mintázatokat foglal magában, amelyek során az egyén nem képes kontrollálni az online tevékenységeit, azok kényszeressé válnak, és más fontos életterületek, például az alvás, tanulás vagy társas kapcsolatok háttérbe szorulnak [75], [76], [77], [78]. Három fő dimenziója, a kontrollvesztés, az obszesszió és az elhanyagolás különböző módon növeli a kiberbiztonsági kockázatokat. A kontrollvesztés csökkentheti az önszabályozás képességét, így a gyermekek hajlamosabbá válhatnak impulzív kattintásokra, ismeretlen linkek megnyitására vagy személyes adatok megosztására. Az obszesszív internethasználat során a felhasználók gyakran keresnek intenzív érzelmi ingereket, ami növeli annak esélyét, hogy veszélyes vagy az életkoruknak nem megfelelő tartalmakkal találkoznak. Az elhanyagolás dimenziója arra utal, hogy az online jelenlét más fontos tevékenységek rovására történik, a gyermekek kevésbé vesznek részt olyan offline szociális interakciókban, amelyek akár védőfaktorként működhetnének a digitális térben való eligazodásban.

A fiatal generációkat fokozottan érinti a személyes adatokkal való visszaélés veszélye, az online zaklatás, a nem megfelelő tartalmakhoz való hozzáférés, a digitális függőség kialakulása, valamint a manipuláció és dezinformáció kibertérbeli veszélyei [79], [80]. Ezek a tényezők különösen veszélyesek lehetnek az Alfa generáció számára, akik még nem rendelkeznek a megfelelő kritikai gondolkodással és digitális írástudással ahhoz, hogy felismerjék és kezeljék ezeket a fenyegetéseket [79]. A problémás internethasználat és a kiberbiztonsági kockázatok tehát szorosan összefonódnak, és komplex módon hatnak a gyermekek pszichológiai jóllétére és fejlődésére.

1.2.3 Generációs és nemi kockázati faktorok

A korábbi kutatások [13], [81], [82] egybehangzóan azt mutatják, hogy a serdülők körében különösen gyakori a problémás internethasználat, ami szorosan összefügg a stressz és a depresszió fokozott mértékével. A túlzott online tevékenység negatívan hatással van a serdülők alvásminőségére, önértékelésére, társas kapcsolataira és tanulmányi eredményeire is. Súlyosabb esetekben pszichés zavarok, szomatikus tünetek és társfüggőségek is kialakulhatnak, ezért kritikus fontosságú a korai azonosítás és intervenció.

A Z generáció tagjai fokozottan ki vannak téve az okoseszköz függőség kockázatának a folyamatos online kapcsolattartás, a közösségi média, az online játékok és a virtuális közösségek elvárásainak. Ez a jelenség negatív hatással lehet mentális egészségükre és társas kapcsolataikra [72]. A problémás internethasználat és a magányosság között azonban erős összefüggés figyelhető meg, amelyen belül a PIH érzelmi (affektív) vonatkozása mutatja a legerősebb korrelációt [83]. Ez azzal magyarázható, hogy a magányos egyének az interneten keresnek társaságot és érzelmi kapcsolódást, ami könnyen a problémás internethasználat kialakulásához vezethet. A PIH érzelmi tünetei, mint a szorongás, a depresszió és az alacsony önértékelés tovább súlyosbíthatják a magányosságot, ezzel ördögi kört hozva létre.

Egy 2023-as, szülőkkel együtt végzett felmérés [73] szerint a 3-11 éves korosztály 33%-a rizikós vagy problémás internethasználónak minősül, míg a 12-18 évesek esetében 20% tartozik a mérsékelt[13], 10% pedig a súlyos kategóriába. A vizsgálatok alapján nemi különbségek figyelhetők meg a problémás internethasználat formáiban. Egy 2022-es kutatás [84] alapján a fiúk körében a PIH leginkább az online játékokhoz, míg a lányoknál a közösségi médiához és az okostelefonokhoz kapcsolódik.

A digitális világba beleszületett Alfa generáció tagjai már egészen fiatal korban kapcsolatba kerülnek az internettel, gyakran szülői felügyelet nélkül. Ez a korai és intenzív online jelenlét nemcsak a problémás internethasználat kialakulásának kockázatát növeli, hanem fokozottan kitetté teszi őket különféle kiberbiztonsági fenyegetéseknek is [85]. Már kisgyermekként hozzáférnek az okoseszközökhöz, digitális tartalmakhoz és közösségi platformokhoz, így a digitális kompetenciáik korán fejlődnek, ugyanakkor a kritikai gondolkodás és az önszabályozás képessége még az életkori sajátosságok miatt nem alakult ki teljesen [63], [86]. A generációra jellemző a multimédiás tartalmak iránti magas érzékenység, a gyors információfeldolgozás és a rövid figyelmi idő, amely a rövid tartalmak fogyasztását erősíti, míg a digitális szocializáció gyakran helyettesíti vagy háttérbe szorítja a személyes interakciókat. Ezek a jellemzők önmagukban nem tekinthetők negatívnak, azonban bizonyos kockázati tényezők mellett problémás viselkedésformákhoz vezethetnek. A leggyakoribb kockázati tényezők közé tartozik a szülői kontroll hiánya vagy túlzott engedékenység az eszközhasználat terén, az alacsony szintű digitális írástudás a családi környezetben, valamint a tartalmi szűrés hiánya, amely nem életkornak megfelelő információkhoz való hozzáférést eredményezhet. További rizikófaktorok a szociális izoláció, amely a személyes kapcsolatok helyett az online

interakciókat helyezi előtérbe, valamint az érzelmi szabályozás nehézségei, különösen a megvonásos tünetek esetén. A megfigyelt mintázatok arra utalnak, hogy az Alfa generáció tagjai különösen érzékenyek az online térben megjelenő viselkedéses és pszichológiai hatásokra. A problémás internethasználat kialakulásának kockázata nem csupán az online töltött idő mennyiségétől függ, hanem attól is, hogy milyen családi, társadalmi és oktatási környezetben történik az internethasználat. A demográfiai változók hatásmechanizmusainak feltárása alapvető a problémás internethasználat differenciált értelmezéséhez és empirikus vizsgálatához.

1.3 Reziliencia és kiberreziliencia

A neveléstudományban is egyre hangsúlyosabbá válik a fiatal generációk mentális egészségének és pszichés jóllétének kérdésköre, különösen az oktatási környezetben megjelenő kihívások tükrében. A reziliencia, mint a stresszel, traumával és megterhelő élethelyzetekkel szembeni adaptív megküzdési képesség, kulcsfogalomként jelenik meg a pedagógiai gyakorlatban is, hiszen nemcsak az egyéni fejlődést, hanem az iskolai teljesítményt, a társas kapcsolatok minőségét és a tanulói jóllétet is jelentősen befolyásolja. A reziliencia szociális-érzelmi összetevői pozitív kapcsolatban állnak az együttműködéssel és a segítő magatartással, amelyek a támogató tanulási környezet kulcselemei [87]. A társadalmi és technológiai változások hatására olyan új kihívások jelentek meg, amelyek a tanulók stresszkezelési képességeit és alkalmazkodási stratégiáit is próbára teszik [S-5]. A korai serdülőkorban megfigyelhető stresszterheltség és a digitális környezet hatásai jelentős szerepet játszanak a reziliencia alakulásában, különösen a megküzdési stratégiák fejlődése révén [88]. Hazai kutatások [89] is megerősítik, hogy az oktatási környezetben alkalmazott célzott mentálhigiénés beavatkozások, például mentorprogramok, képesek növelni a fiatalok rezilienciáját és csökkenteni a pszichés terhelésből fakadó tüneteket. A reziliens tanulók nagyobb eséllyel képesek alkalmazkodni a változó körülményekhez, hatékonyabban kezelik az iskolai stresszhelyzeteket, és kevésbé hajlamosak a mentális zavarok kialakulására, ami különösen fontos a serdülőkor érzékeny fejlődési szakaszában [S-5].

1.3.1 A reziliencia pszichológiai alapjai és fogalmi kerete

A reziliencia fogalmának tudományos értelmezése az elmúlt évtizedekben jelentős fejlődésen ment keresztül, a kezdeti egyszerű megközelítésektől a komplex, rendszerszintű modellekig. A kutatások kezdetben a kockázati és védőfaktorok szerepére fókuszáltak, majd egyre inkább előtérbe került az egyén és környezete közötti dinamikus

kölcsönhatás, valamint a pszichológiai és szociális erőforrások fejlesztésének lehetősége. A korai modellek közé tartozik a pszichoszociális reziliencia elmélete, amely a védőmechanizmusok szerepét hangsúlyozta a stresszes élethelyzetek negatív hatásainak csökkentésében [90]. Ezt követően Norman Garmezy [91] a szegénységhez kapcsolódó fejlődési kockázatok és védőfaktorok vizsgálatával járult hozzá a reziliencia kutatásához, kiemelve a családi stabilitás és a támogató környezet jelentőségét. A fejlődéslélektani megközelítést képviseli Urie Bronfenbrenner [92] ökológiai rendszermodellje, amely a rezilienciát több szinten értelmezi, az egyén közvetlen környezetétől, a családtól, az iskolától egészen a társadalmi és kulturális rendszerekig. Ez a modell alapvetően befolyásolta a későbbi reziliencia elméletek rendszerszintű gondolkodását. A 2000-es évek elején végzett kritikai értékelés rámutatott arra, hogy a reziliencia fogalmának megértéséhez elengedhetetlen a szociális kontextus figyelembevétele, különösen a családi és iskolai támogatás, amely kulcsszerepet játszik a reziliencia kialakulásában és fenntartásában [93]. A reziliencia dinamikus, ciklikus természetét hangsúlyozó megközelítés szerint az egyén a stressz hatására kibillen az egyensúlyi állapotából, majd megküzdési stratégiák révén visszanyeri azt, vagy új, magasabb szintű működésbe lép [94]. A reziliencia kognitív megközelítése a pszichés ellenállóképességet az affektív-kognitív rendszerek rugalmas működésén alapulóként értelmezi, amelyben az információfeldolgozás hatékonysága kulcsfontosságú a stresszhez való adaptív alkalmazkodásban [95]. A pozitív pszichológia irányából pedig a pszichológiai tőke, PsyCap modelljében a reziliencia a remény, énhatékonyság és optimizmus mellett az egyén fejleszthető erőforrásaként jelenik meg, amely jelentős hatással van a teljesítményre és a mentális jóllétre [96].

1.3.2 A kiberreziliencia, digitális ellenállóképesség fogalmi áttekintése

A gyorsuló technológiai fejlődés és a kiberfenyegetések ugrásszerű növekedése miatt, a kiberbiztonság és digitális reziliencia központi kérdéskörré nőtte ki magát világszerte és új készségeket követel [29], [97]. A digitális reziliencia definiálása, eredetileg a digitális forradalom által generált új eszközök, rendszerek és szoftverekhez, új körülményekhez való alkalmazkodást célozza meg az egyének oldaláról [98]. Továbbá a digitális reziliencia egy olyan ciklikus folyamat, mely során az egyének felismerik, kezelik az online kockázatot és fenyegetéseket, melyből tanulva, felépülve nagyobb teljesítményre és ellenállóbb funkcionális működésre képesek a digitális kihívásokkal szemben [99]. Ennek szinonimája, vagy továbbfejlesztése a kiberreziliencia definíciója [100], mely

szerint a kiberfenyegetésekre adott pozitív alkalmazkodás kulcsfontosságú a kiberbiztonsági kompetenciafejlesztés során. A kiberreziliencia a biztonságos online működés érdekében proaktív alkalmazkodást és folyamatos tanulást igényel. Mivel a kibertámadások többsége igazoltan emberi hibákra vezethető vissza, ezért a leghatékonyabb védelmi megközelítés az átlagfelhasználók biztonságtudatos magatartásának, kibertérhez köthető készségek, mint az ellenálló képesség, reziliencia folyamatos fejlesztése a biztonságos kibertér megteremtéséhez [25], [34].

Ez az egyéni szintű megközelítés kiegészíti a korábban elsősorban közösségi, szervezeti vagy nemzeti szinten értelmezett kiberreziliencia koncepciókat [101], [102]. A kiberreziliencia egyéni szinten, azt a képességet jelenti, amely lehetővé teszi az online fenyegetésekből, sérülésekből való felépülést és a digitális kihívásokhoz való sikeres alkalmazkodást. A kiberreziliencia a személyiség többdimenziós, összetett építőelemeként definiálható. Ahol a *kognitív komponens* magába foglalja a kibertérrel kapcsolatos naprakész tudást és a kiberbiztonsági tudatosságot. A *pszichológiai komponens* az ellenállóképességet és az adaptív megküzdési stratégiák használatát jelenti. A *viselkedési komponens* a biztonságos és kiegyensúlyozott digitális viselkedési mintázatok megvalósítását foglalja magába.

A biztonságos online jelenlét érdekében egyre fontosabbá válik a digitális reziliencia, vagyis az a képesség, hogy az egyén képes alkalmazkodni, felépülni és megőrizni jóllétét online fenyegetések közepette [99]. A fiatalok esetében különösen fontos az érzelmi reziliencia fejlesztése, mivel érzékenyen reagálnak a kiberbántalmazás pszichológiai hatásaira, ami célzott támogatást igényel [98]. A digitális ellenállóképesség kutatását jelentős akadályok nehezítik. A fogalom viszonylag új, egységes definíció hiányában gyakran összekeverik a digitális írástudással, ami terminológiai bizonytalanságot okoz. További problémát jelent, hogy a terület még nem rendelkezik kellően megalapozott és validált mérőeszközökkel. Éppen azokat a tizenéveseket vizsgálják a legkevésbé, akik a legintenzívebben használják az internetet, holott ebben a korosztályban lenne a legnagyobb szükség az ellenállóképesség fejlesztésére.

Sun és munkatársai [99] átfogó elméleti kerete szerint a digitális reziliencia egyszerre képesség és folyamatos adaptáció, amely meghatározza az emberek digitális stresszhelyzetekre adott reakcióit és ezek viselkedési, pszichoszociális hatásait. Öt alapvető dimenziót azonosítottak. Az első az online fenyegetések megértése, a digitális

kockázatok, mint kiberbántalmazás, információs túlterheltség, online jelenlét mentális hatásainak felismerése. A második az alkalmazott megoldások ismerete, a kritikus helyzetekben való segítségkérés módjai. A harmadik a tudás és készségek elsajátítása, a tapasztalatokból való tanulás és jövőbeli döntések adaptálásának képessége. A negyedik a stresszből való felépülés negatív online élmények után. Az ötödik az énhatékonyság révén történő előrehaladás, tehát nem csak a korábbi állapot visszaállítása, hanem a nehézségeket követő fejlődés és megerősödés. Ez a modell a digitális rezilienciát dinamikus, folyamatosan fejlődő képességként közelíti meg [99].

Qamaria és munkatársai [98] szisztematikus irodalmi áttekintésükben rávilágítottak arra, hogy a kiberreziliencia kutatásában az elmúlt öt évben leggyakrabban az ökológiai elméletet alkalmazták teoretikus keretként. A digitális reziliencia kialakulását külső és belső tényezők együttesen befolyásolják, amelyek az egyén és környezetének különböző szintű kölcsönhatásaiból erednek. Az ökológiai megközelítés szerint a digitális reziliencia egy dinamikus folyamat, amely olyan előzményekkel kezdődik, mint az online fenyegetések, a kiberbántalmazás vagy túlzott internethasználat. Ezeket külső tényezők, mint szociális támogatás és belső egyéni erőforrások, mint az önkontroll, önbizalom, digitális írástudás együttesen alakítják. A kiberreziliencia kialakulása után javul a teljesítmény, mentális egészség és az egészségesebb életmódhoz való alkalmazkodás. A digitális reziliencia lényegében az egyén azon képességét jelöli, ami segít abban, hogy megvédje magát és felépüljön a negatív online tapasztalatokból. Ez olyan konkrét készségeket foglal magában, mint a kiberbántalmazás elleni védekezés, a pornográf tartalom kezelése, a képernyőidő tudatos kezelése, az információk kritikus értékelése és az etikus online viselkedés [98]. A források tehát a digitális reziliencia komplex, dinamikus és sokszínű jellegét emelik ki, hangsúlyozva a kognitív (*online fenyegetések felismerése*), pszichológiai (*énhatékonyság, stresszkezelés*) és viselkedési (*gyakorlati készségek alkalmazása*) komponenseket, valamint a környezeti és egyéni tényezők kölcsönhatását a kialakulásban és fejlődésben.

1.3.3 A kiberreziliencia mérési kihívásai

A kiberreziliencia empirikus vizsgálatát alapvető módszertani nehézségek hátráltatják, amelyek szorosan kapcsolódnak egymáshoz. A mérési megközelítések széttagoltsága megnehezíti az egységes kutatási keret kialakítását, miközben a kontextuális tényezők gyakran figyelmen kívül maradnak az elemzések során. Tovább bonyolítja a helyzetet, hogy a kutatási eszközök pszichometriai validálása sok esetben hiányos vagy nem kellően

megalapozott. A kiberreziliencia különböző komponenseit, mint például a kiberbiztonsági tudatosság, a problémás internethasználat vagy az általános pszichológiai reziliencia, jellemzően önálló, egymástól elhatárolt, eltérő elméleti háttérre épülő és különböző célpopulációra validált skálákkal mérik. A kiberbiztonsági tudatosságra kidolgozott eszközök, mint a Bognár és Bottyán [103] által validált skála a megelőző és proaktív kiberbiztonsági viselkedés mérésére szolgál egyetemi hallgatókra szabottan, és célja a kiberbiztonsági kultúra kialakítása. Arpaci és Sevinc [42] által fejlesztett Cybersecurity Scale (CSA) és annak magyar nyelvű adaptációja [S-7], vagy a közösségi média felhasználókra fókuszáló változata [104] az egyének kiberbiztonsági, proaktív védekezési gyakorlatait mérik. Specifikus fókuszuk miatt (titoktartás, kontroll/birtoklás, integritás, hitelesség, elérhetőség és hasznosság) azonban kizárják a reziliencia pszichológiai és viselkedésbeli dimenzióit, így nem alkalmasak a kiberreziliencia szélesebb körű holisztikus értékelésére. Ezzel ellentétben a pszichológiai rezilienciát mérő, széles körben használt eszközök, mint a Connor-Davidson reziliencia kérdőív (CD-RISC) [105] vagy a fiatalok körében alkalmazott Child and Youth resilience mérőeszköz (CYRM-28) [106] az általános pszichoszociális megküzdési képességekre koncentrálnak, és nem specifikusak a digitális kontextusra. Ez a mérőeszköz-sokféleség, amely a különböző megközelítésekben, célcsoportokban és elméleti keretekben nyilvánul meg, megnehezíti egy egységes, kiberreziliencia-központú, többdimenziós modell kidolgozását és gyakorlati vizsgálatát.

Az utóbbi években azonban olyan kezdeményezések jelentek meg, amelyek a kiberreziliencia átfogó mérését célozzák. Qi és Yang [107] tanulmánya egy kínai serdülők számára kifejlesztett digitális reziliencia kérdőívet mutat be. Ez a skála négy elméletileg megalapozott faktort azonosít: a kockázatok ismeretét, a segítségkérést, a proaktív tanulást és a felépülést. Ugyanakkor ez a skála rávilágít a mérés kulturális és kontextuális beágyazottságának problémájára is. Egy Kínában, specifikus oktatási és társadalmi rendszerben validált mérőeszköz tételei és faktorszerkezete nem feltétlenül alkalmazható közvetlenül európai, jelen esetben magyar kontextusra. A fiatalok által használt nyelvezet, szleng és digitális kommunikációs formák szintén olyan helyi specifikumok, amelyek egy mérőeszköz érvényességét alapvetően meghatározzák.

Végül, a harmadik kihívás a pszichometriai validálás hiányossága, különösen a legfiatalabb, Alfa generációk esetében. A fent említett eszközök közül kevés létezik, amelyet kifejezetten a Z vagy Alfa generáció specifikus jellemzőire validáltak volna. A

CSA [104] ugyan közösségi média-felhasználók számára készült, de a célpopuláció széles demográfiai spektrumot ölel fel, nem tesz különbséget a generációk között. A CYRM-28 [106] a pszichológiai rezilienciát méri fiatalokon, de nem integrál kiber-specifikus dimenziókat. Továbbá a validálási problémák területén a legtöbb létező eszköz esetében hiányzik a megfelelő pszichometriai validálás, különösen az Alfa generáció vonatkozásában. Ezek a kihívások együttesen rámutatnak arra, hogy szükség van olyan új mérőeszközök fejlesztésére, amely pszichometriailag robusztus, többdimenziós skála, és a fiatalok személyes kiberrezilienciáját átfogóan, integrált módon, a Z és Alfa generációk sajátosságait figyelembe véve méri. Jelen kutatás ezt a hiányt kívánja pótolni egy magyar fiatal populációra szabott, kulturálisan érzékeny kiberreziliencia skála integrálásával, kifejlesztésével és validálásával.

1.3.4 Stressz, szorongás és kiberreziliencia generációs mintázatai

A reziliencia fejlesztésének relevanciája különösen szembetűnő a generációs sajátosságok tükrében. A kiberreziliencia-profilok feltárásához elengedhetetlen a célpopuláció, a Z és Alfa generáció digitális életterének megértése. A két generáció eltérő digitális szocializációs tapasztalatainak hatása a kiberrezilienciára jelenleg kevéssé ismert területnek számít, annak ellenére, hogy online jelenlétük intenzitása kiemelkedő [98], [99], [103], [S-7]. Egy 2024-es felmérés [108] alapján a 16-29 éves fiatalok 97%-a naponta használja az internetet az Európai Unióban, és ez az arány Magyarországon eléri a 99%-ot. Ez az intenzív jelenlét egy sokszínű platform-ökoszisztémában valósul meg, ahol a többségük aktívan használja az online közösségi media és videómegosztó csatornákat, YouTubeot (93%), a TikTokot (63%), a Snapchatet (60%), és az Instagramot (59%) [109]. A szakirodalom [110] ezt a folyamatos navigációt a fizikai és a digitális világ között a „*phygital*” fogalmával írja le, amely során a fiataloknak mindkét világhoz szükséges kompetenciákat kell fejleszteniük, miközben alkalmazkodnak az online tér sajátosságaihoz, mint az anonimitás, hozzáférhetőség és megfizethetőség. Ennek a folyamatnak a mélységét jelzi a „*digitális fenotípus*” koncepciója is, amely szerint az online viselkedés már az egyén mentális egészségének indikátoraként is értelmezhető, például a közösségi média bejegyzések mintázatai előre jelezhetik a depresszió kockázatát.

A két generáció közötti kulcsfontosságú különbség a digitális szocializációjuk jellegében rejlik. A Z generáció tagjai már gyermekkorukban találkoztak az internettel és digitális eszközökkel, ami jelentős hatással van információfeldolgozási szokásaikra, társas

kapcsolataikra és stresszkezelési stratégiáikra formálódásához [111], [112]. A túlzott digitális jelenlét szorongást, depressziót, magányt okozhat, különösen a társas támogatás hiányában [113]. A Z generáció tagjai fokozottan érzékenyek a közösségi média által közvetített társas nyomásra, ami gyakran szorongáshoz, alacsony önértékeléshez és testképzavarokhoz vezet.

Az Alfa generáció életében korai életkorban előtérbe kerülnek a közösségi média platformok, 40%-uknak már kétéves korukban volt táblagépe, míg négyéves korukra ez az arány 58%-ra emelkedett [114]. Számukra a digitális eszközök nem csupán kommunikációs csatornák, hanem a világgal való interakció, a tanulás és a játék alapvető közegei [115]. Ugyan a tudományos vizsgálatok még kezdeti fázisban vannak, de már most látható, hogy a korai digitális eszközhasználat, a multitasking és az információs túlterheltség kihívásokat jelenthet a pszichés fejlődés és a szocializáció szempontjából [116], [117].

A generációk közötti különbségek nemcsak a technológiai eszközhasználatban, hanem a megküzdési mechanizmusokban is megmutatkoznak. Míg a Z generáció tagjai gyakran keresnek társas támogatást és közösségi megerősítést [S-6], addig az Alfa generáció esetében a digitális térben való önkifejezés és az azonnali visszacsatolás iránti igény válik dominánssá. Ez a különbség a pedagógiai gyakorlatban is megjelenik, hiszen a tanulók rezilienciájának fejlesztése során figyelembe kell venni generációs sajátosságaikat, társas kapcsolati mintázataikat és technológiai szocializációjukat [118].

Mindkét generáció fejlődését alapvetően meghatározza, hogy születésüktől fogva digitális környezetbe szocializálódnak, tanulnak és formálják identitásukat. A „*digitális bennszülött*” nemzedékek számára a folyamatos online jelenlét kettős természetű, lehetőségeket teremt a könnyen elérhető, gyors tanulásra és a kapcsolatépítésre, ugyanakkor specifikus stresszforrásokat és mentális egészségügyi kockázatokat is generál, különösen a szorongásos rendellenességek területén [113], [119], [S-6].

A kutatási eredmények [120], [121], [S-6] egybehangzóan igazolják a fiatalok körében növekvő szorongásos tünetek gyakoriságát. Ezen jelenségek hátterében a digitális stressz komponensei, nevezetesen a társas összehasonlítás, az információtúlterhelés és a folyamatos online jelenlét szükségességének érzése azonosíthatók kulcstényezőkként. A digitális stressz szignifikáns összefüggést mutat a szorongásos tünetekkel, különösen a mások elismerésének kényszerszerű keresése, mint a like gyűjtés és a folyamatos

interakciókból fakadó kognitív és érzelmi kimerülés tekintetében. A közösségi médiában zajló társas összehasonlítás elsősorban a tökéletességet sugalló tartalmak és teljesítményközpontú bejegyzések fokozzák a szorongást, különösen a pszichológiailag sérülékenyebb egyéneknél. E nyomás hatására kialakuló hamis önkifejezés tovább torzítja az énképet. A nők magasabb szintű stresszről és szorongásról számolnak be, amely agyi aktivitási mintázatokban is tükröződik [122].

Ezekhez a mechanizmusokhoz specifikus viselkedésformák társulnak. A problematikus okostelefon használat egyértelműen előre jelzi a szorongást [123]. Hatását az adaptív megküzdési stratégiák, például a társas támogatás keresése enyhítheti a tüneteket, de nem szünteti meg teljesen, míg a maladaptív megküzdési formák, mint az ismétlődő, passzív gondolkodás, a legrosszabb forgatókönyv feltételezése és a kizárólag negatívumokra való összpontosítás tovább rontják az állapotot [124]. A digitális detox, vagyis a szándékos offline időszakok tartása csökkentik a kognitív terhelést és javítják a pszichológiai jóllétet, bár hatásuk egyén és kontextusfüggő [125]. A folyamatos online jelenlét, azaz a naprakészség kényszere szorosan kapcsolódik a szorongáshoz, depresszióhoz és magányossághoz. A digitális környezet hatása a használat módjától és az egyéni jellemzőktől függően csökkenthetik vagy növelhetik is a stresszt [126]. A szórakoztató és kapcsolatteremtő tartalmak pozitívan hatnak, míg a társas összehasonlításra épülők negatív következményekkel járnak. A túlzott online jelenlét bizonyítottan gyengíti a családi kötelékeket és csökkenti az interakciók minőségét [127]. Ugyanakkor a technológia fejlődése lehetőségeket is kínál, a virtuális valóság és a mesterséges intelligencia alapú chatbotok ígéretes eszközök lehetnek a szorongás csökkentésére és a pozitív énkép kialakítására, ugyanakkor helytelen használata akár romboló hatású is lehet [128], [129].

A Z és Alfa generációk számára a digitális tér az identitásalkotás és az önkifejezés elsődleges színtere. Avatárok, alternatív fiókok és tudatos manipulációs stratégiák segítségével kísérleteznek identitásukkal, miközben gyakran manipulatív módon próbálnak megfelelni a társas elvárásoknak vagy elkerülni a konfrontációt. A virtuális környezet számukra nem a valóság alternatívája, hanem annak kiterjesztése, ahol a virtuális és valós identitás határai elmosódnak. Ez a folyamat egyidejűleg egyfajta lehetőség és kockázat, hiszen az önkifejezés, kreativitás és elfogadás mellett megjelennek a testképzavarok, a technológiai függőség, valamint az etikai és adatvédelmi problémák is [130], [131]. Ezek a jellemzők közvetlenül befolyásolhatják a kiberreziliencia profilt.

A kognitív rugalmasság elősegíti a proaktív tanulást, ugyanakkor a fokozott érzékenység és a közösségi média intenzív használata mentális egészségügyi kockázatot jelent, amely csökkenti a stresszkezelő képességet. A szakirodalom dokumentálja a generációs különbséget, azonban empirikus vizsgálat hiányzik arról, hogy az eltérő szocializációs háttér hogyan alakítja a specifikus kiberreziliencia dimenziót. Ez a kutatási rés teszi lehetővé a generációs kiberreziliencia jellegzetesség empirikus feltárását.

Elméleti keret összegzése

Jelen fejezet átfogó képet nyújtott a kiberbiztonság 21. századi kihívásairól generációs nézőpontból. A kibertér, kiberbiztonság és kiberreziliencia fogalmi tisztázását követően bemutatásra kerültek a kiberbiztonsági tudatosság dimenziója, valamint a releváns mérési modellek és eszközök. A Z és Alfa generáció digitális szocializációjának vizsgálata rávilágított az online szokás generációspecifikus jellemzőjére, a digitális szocializációs különbségre, valamint a kognitív fejlődés és szocio-emocionális készség generációs aspektusára. Részletes elemzés történt a problémás internethasználat jelenségéről és a kapcsolódó kiberbiztonsági kockázatról, különös tekintettel a generációs rizikófaktorra. A reziliencia humán dimenziójának tárgyalása során bemutatásra került a fogalom pszichológiai alapja, a stressz és szorongás generációs megjelenése a digitális környezetben, valamint a digitális ellenállóképesség és kiberreziliencia elméleti kerete és mérési kihívásai. A fejezet a kiberreziliencia generációs aspektusának elemzésével zárult, megalapozva a további kutatási irányt és hipotéziseket.

A bemutatott elméleti háttér és szakirodalmi áttekintés alapján a következő fejezet a kutatás módszertani keretét tárgyalja. A módszertani fejezet részletesen ismerteti a mintaválasztás elvét, az alkalmazott adatgyűjtési technikát és elemzési eljárást, amelyek lehetővé teszik az elméleti megállapítások empirikus vizsgálatát és a kutatási kérdések megválaszolását.

2 KUTATÁSI MÓDSZERTAN

A jelen fejezet a kutatás módszertani keretét mutatja be részletesen. Az első részében bemutatom a kutatás általános tervezését, a mintavételi stratégiát és az adatgyűjtés módját. Ezt követően részletezem az alkalmazott eljárásokat és az etikai megfontolásokat, amelyek biztosították a kutatás tudományos integritását és a résztvevők védelmét. A minta demográfiai jellemzőinek ismertetése után kitérek a kutatásban alkalmazott mérőeszközökre, beleértve azok validálását és kulturális adaptációját is. A fejezet további részében az adatelemzési módszertant mutatom be, kitérve mind a kvantitatív, mind a kvalitatív adatok elemzésének eljárásaira. Végül bemutatom az adatintegráció, modellépítés és validáció módszertanát, amely a vegyes módszertani kutatás szintézisét szolgálja.

2.1 Mintavétel és adatgyűjtés

Az attitűdök komplex, társadalmi és pszichológiai jellege miatt a kutatás primer, vegyes módszertanú, szekvenciális kiegészítő stratégiát (QUAN → qual) alkalmaz [132].

2.1.1 Kvantitatív adatgyűjtés (1. fázis QUAN)

A kutatás első fázisa (QUAN) kvantitatív adatgyűjtéssel és statisztikai elemzéssel azonosítja a kiberbiztonsági tudatosság és a reziliencia szintjét, és a problémás internethasználat mértékét a Fejér vármegyei Z és Alfa generáció körében. A vizsgálat központi komponense a kvantitatív vizsgálat, mely leíró jellegű és deduktív logikára épül, tesztelve a hipotéziseket. A kutatás során alkalmazott hibrid mintavételi eljárás hozzáférésen alapuló volt, melynek során a kérdőív Fejér vármegye összes oktatási intézményébe kiküldésre került (kényelmi mintavétel), és néhány kiválasztott intézményt felkerestem célzottan (rétegzett mintavétel – a kiválasztási szempontok között szerepelt, hogy minél szélesebb képzési palettájú és szintű intézményi válasz rendelkezésre állása biztosított legyen). Összesen Fejér vármegye 45 intézménye vett részt a felmérésben. A válaszadás ezt követően önkéntes és anonim volt, tehát a kiválasztott osztályok diákjainak is megvolt a lehetősége, hogy kimaradjanak a válaszadásból. A hibrid mintavételi eljárás miatt a minta reprezentativitásának megítélése körültekintést igényel.

A minta heterogénnek tekinthető, mivel általános, közép- és felsőoktatási intézményekből egyaránt érkeztek adatok, eltérő arányban. A kutatás első szakaszában vegyes lebonyolítású, papír alapú és online kérdőíves felmérés készült. A kérdőív validálási szakaszában (*2022.09-2023.05*), az első pilot és re-test körben $N = 35$, majd a második

körben *N = 398* felsőoktatásban résztvevő hallgató (*79%* férfi, *21%* nő) vett részt az Óbudai Egyetem Alba Regia Karáról (*86%*), illetve a Corvinus Egyetem Székesfehérvári kampuszáról (*14%*), többségében (*82%*) Z generációhoz tartozók. A minta összetétele a képzési orientáció szerint *81%* reál tudományos (mérnöki *N = 173*, informatikai *N = 149*) és *19%* humán tudományos (gazdasági *N = 76*) területekről került ki, dominánsan BSc szintű, nappali képzésekből (*94%*). Az ezt követő nagyszámú felmérésben *N = 3473* Fejér vármegyei közoktatásban és szakképzésben résztvevő diák került bevonásra. Az X és Y generáció tagjait kizárásra kerültek a gyűjtött nagymintából, mivel nem képezte a célcsoportot (Z és Alfa), továbbá kizárásra kerültek a hiányzó értékeket tartalmazó válaszok, nem megfelelően, adatbeviteli hibákkal kitöltött kérdőívek is. Az elemzéshez szükséges adatok előkészítése során azonosításra és további törlésre kerültek azok a válaszok, melyek kiugró, vagy szélsőséges értéket tartalmazott. Az adattisztítási folyamat eredményeként *N = 198* válasz került eltávolításra a nagymintából. A végleges minta (*N = 3275*) összetétele alapján a Z generációhoz tartozó résztvevők száma *N = 2438* (*74.4 %*), míg az Alfa generációhoz tartozóké *N = 837* (*25.6 %*). A felmérésben nemek szerint a résztvevők *N = 1746* fiú (*53.3 %*), és *N = 1529* lány (*46.7%*) az általános iskola felső tagozatától, 5. osztálytól kezdődően a felsőoktatásig. A résztvevők száma a vizsgált mintában az általános iskolákat érintően *N = 1215* (*37 %*), a középfokú oktatási intézményt tekintve *N = 1726* (*53 %*), a felsőoktatásban tanulókat nézve *N = 334* (*10 %*).

A végleges kérdőív (1/E. melléklet) az adaptált kiberbiztonsági tudatosság kérdőív (CS-C-H), a Connor-Davidson reziliencia kérdőív (CR-RISC) (1/D. melléklet), és a problémás internethasználat (PIH) standardizált mérőeszközöket (1/C. melléklet), valamint demográfiai kérdéseket (1/B. melléklet) tartalmazott. A végleges kérdőívet a demográfiai kérdésekkel az 1. melléklet tartalmazza.

2.1.2 Kvalitatív adatgyűjtés (2. fázis qual)

A második fázis, kiegészítő komponens (qual) célja a kvantitatív eredmények mélyebb megértése és magyarázata. Ez a fázis feltáró jellegű és induktív logikára építve, kvalitatív adatgyűjtéssel és tematikus tartalomelemzéssel magyarázza meg az adatok mögött húzódó személyes tapasztalatokat. A két fázis szekvenciális ütemezésben valósult meg, ahol a kvalitatív mintavétel a kvantitatív eredményein alapul. Az adatok integrációja elsősorban narratívan magyarázza meg a kvantitatív eredményeket.

A kvalitatív, fókuszcsoportos beszélgetésekkel végzett feltáró jellegű kutatás elsődleges célja mélyebb betekintést nyerni a résztvevők online viselkedésébe, a potenciális kockázatokhoz való hozzáállásukba, valamint az érzelmi és kognitív tényezők szerepébe. Az interjúk asszociatív elemekkel integrált módon zajlottak, tematikus képek kiválasztásával vizsgáltam a résztvevők érzelmi reakcióit és szorongásos megnyilvánulásait. A beszélgetés moderátorként, általam volt vezetve, ügyelve a téma fókuszának megőrzésére. A beszélgetések félig strukturált módon zajlottak, ahol volt egy előre összeállított, 17 kérdéses lista (2/C. melléklet), de a résztvevők új gondolatokat is megoszthattak. A fókuszcsoportok mérete 5-7 fő között mozgott, csoportonként iskolatípus szerint homogén csoportokban. A célja, hogy feltárja a diákok hozzáállását a kiberbiztonsághoz. A beszélgetések mobiltelefonnal kerültek rögzítésre, majd az online Transkriptor program segítségével kerültek átírásra. Az átírás során a beszélt szöveg került rögzítésre, a nonverbális jelek nem.

A kvantitatív elemzés eredményeinek figyelembevétele mellett, célzott mintavételi stratégia került alkalmazásra a kvalitatív kutatási fázishoz, amelynek keretében *N = 89* fő került bevonásra a vizsgálatba. A mintaválasztás központi szempontja a reprezentativitás biztosítása volt, amely két dimenzió mentén került érvényesítésre, az iskolatípus egyenletes reprezentációja és a nem arányos képviselete. A generációs megoszlás szempontjából a minta kiegyensúlyozott, a résztvevők közül *N = 46* fő *(51.7%)* az Alfa generációhoz tartozik, míg *N = 43* fő *(48.3%)* a Z generációhoz sorolható. A nemek szerinti eloszlásban enyhe túlsúly mutatkozik a női résztvevők javára, mivel *N = 50* lány *(56.2%)* és *N = 39* fiú *(43.8%)* vett részt a vizsgálatban (*az Alfa generáción belül a nemek enyhe eltolódását a kvantitatív eredmények indokolták*). A minta az oktatás mindhárom szintjét magában foglalja, hiszen általános iskolai *(N = 7)*, középiskolai *(N = 4)* és felsőoktatási intézmények *(N = 4)* csoportok egyaránt képviseltetik magukat. A résztvevők szakmai orientációja heterogén, a reprezentált szakterületek között általános képzés, idegen nyelvi tagozatok (angol, német), valamint specifikus szakirányok szerepelnek. Az utóbbiak közé tartozik a földmérés, a gazdasági, az informatikai, a kereskedelmi, a környezetvédelmi, a menedzsment, a matematika, a művészeti és a villamosmérnöki képzés.

2.1.3 Adatgyűjtési eljárások és etikai megfontolások

A résztvevők kiválasztása célzott kényelmi mintavételi eljárással történt Fejér vármegye oktatási intézményeiben. Az adatgyűjtés 2022. szeptember és 2023. május 30. között

zajlott, standardizált online és papíralapú kérdőívek alkalmazásával. A kiskorú résztvevők esetében az intézmény gondoskodott a szülői/gondviselői beleegyezés beszerzéséről, a nagykorú diákok saját beleegyezésüket adták a részvételhez (minta beleegyező nyilatkozat a 2/B. mellékletben érhető el). A résztvevők tájékoztatást kaptak a kutatás céljáról, a részvétel önkéntességéről, valamint az anonimitás és az adatok bizalmas kezelésének biztosításáról (2/A. melléklet). A papír alapú kérdőívek kitöltése tantermi körülmények között, felügyelet mellett történt, átlagosan 20-30 percet vett igénybe. A válaszadási arány intézményenként eltért (résztvevő iskola $N = 45$, válaszadási arány iskolánként $min = 1,\ max = 444$), amely befolyásolhatja az eredmények általánosíthatóságát az iskolatípusokra vonatkozóan.

2.1.4 Demográfiai adatok, jellemzői és reprezentativitása

A vizsgálat célcsoportját a Z generáció (1995-2009 között születettek) és az Alfa generáció (2010-2025 között születettek az 5. évfolyamos képzéstől) képviselői alkották. Az X és Y generáció tagjait kizártam a gyűjtött nagymintából $(N = 3473)$, mivel nem képezte a célcsoportot, továbbá kizárásra kerültek a hiányosan, nem megfelelően kitöltött kérdőívek is. Az elemzéshez szükséges adatok előkészítése során azonosításra és törlésre kerültek azok a válaszok, melyek kiugró, vagy szélsőséges értéket tartalmazott. Az adattisztítási folyamat eredményeként $N = 198$ sor került eltávolításra a mintából. A végleges minta $(N = 3275)$ összetétele alapján a Z generációhoz tartozó résztvevők száma $N = 2438\ (74.4\ \%)$, míg az Alfa generációhoz tartozóké $N = 837\ (25.6\ \%)$. A felmérésben résztvevők $N = 1746$ fiú (53.3%), és $N = 1529$ lány (46.7%). A résztvevők száma a vizsgált mintában az általános iskolákat érintően $N = 1215\ (37\ \%)$, a középfokú oktatási intézményt tekintve $N = 1726\ (53\ \%)$, a felsőoktatásban tanulókat nézve $N = 334\ (10\ \%)$. A minta demográfiai kérdései az 1/A. mellékletben, a demográfiai jellemzői generációs bontásban a 1/B. mellékletben található részletesen bemutatva.

A minta Fejér vármegyei reprezentativitása χ^2-próbákkal került összevetésre a KSH 2022-es referenciaadataival [133], [134]. A nemek arányában nem mutatkozott szignifikáns eltérés az általános iskola felső tagozatában ($\chi^2(1,N = 1215) = 1.40,\ p = .237$), a középiskolában $(\chi^2(1,N = 1726) = 1.25,\ p = .263)$, valamint a teljes 10-29 éves korcsoportban $(\chi^2(1,N = 3275) = 1.90,\ p = .168)$. A generációs megoszlás $(\chi^2(1,N = 3275) = 3.80,\ p = .051)$, az Alfa generáción belüli nemi arány $(\chi^2(1,N = 837) = 0.17,\ p = .680)$ és a Z generáción belüli nemi eloszlás $(\chi^2(1,N = 2438) = 3.44,\ p = .064)$ szintén reprezentatívnak bizonyult. A felsőoktatásban

tanulók körében azonban szignifikáns eltérés tapasztalható *($\chi^2(1,N = 334) = 126.05$, $p < .001$)*, ahol a férfiak felülreprezentáltak, ezért ez az alcsoport nem tekinthető reprezentatívnak. Viszont a kényelmi mintavételi eljárás nem valószínűségi jellege miatt az eredmények általánosíthatóságát fenntartásokkal kell kezelni, még a demográfiai illeszkedés ellenére is.

2.2 Mérési eszközök ismertetése

A kvantitatív kutatás során online és papír alapú kérdőíves felmérés zajlott, amely négy fő részből állt. A kérdőív első része a résztvevők alapvető szocidemográfiai adatait rögzítette, ez kiterjedt a nemre, születési évre, intézmény nevére és típusára, a tanult szakirányra, specializációra, az állandó lakhelyre, a szülők legmagasabb iskolai végzettségére és az átlagos napi internethasználat idejére. A második részben a problémás internethasználat kérdőív (PHIK-6), harmadik részben a Connor-Davidson reziliencia skála (CD-RISC-10), végül a kiberbiztonsági tudatosság kérdőív (CS-C-H) magyar nyelvű adaptált változata került felhasználásra.

2.2.1 Problémás internethasználat kérdőív (PHIK-6)

A problémás internethasználat mérésére Demetrovics és tsa által kidolgozott, validált PIUQ-SF-6 rövidített magyar változata került felhasználásra, amely 6 tételből áll és 5-fokú Likert-skálán méri a problémás internethasználatot [135]. Az eredeti, felhasznált kérdőív az 1/C. mellékletben érhető el. A kérdőív három dimenzióban vizsgálja a problémás internethasználatot. Két tétel az obszesszió, az internettel kapcsolatos kényszeres gondolatokat, két tétel az elhanyagolás, más életterületek háttérbe szorulását, tanulási és munkahatékonyság csökkenését, társas kapcsolatok romlását és két tétel a kontrollzavar, az internethasználat feletti kontroll elvesztését, kényszeres viselkedést méri. A magasabb összesített pontszám a problémás internethasználat fokozott kockázatára utal. A skála megbízhatósága Cronbach $\alpha = 0.77$ [136].

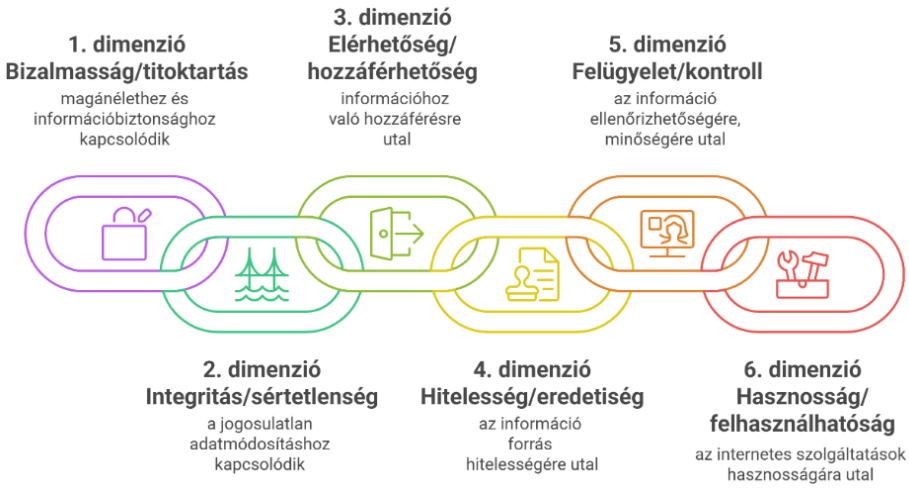
2.2.2 Connor-Davidson reziliencia skála (CD-RISC-10)

A reziliencia mérésére szolgáló egyik legelterjedtebb eszköz a 2003-ban kifejlesztett Connor–Davidson reziliencia skála (CD-RISC), amelyet eredetileg klinikai és nem klinikai populációk vizsgálatára használtak [137]. A skálának létezik egy 10-tételes változata (CD-RISC-10), mely különösen nagy minták gyors és megbízható vizsgálatára alkalmas [138]. A skála az egyén pszichés ellenállóképességét méri egy 5-fokozatú Likert-skálán, ahol a magasabb pontszám nagyobb rezilienciát jelez. Jelen felmérésben a

CD-RISC-10 magyar nyelvű adaptált, validált változata [105] került felhasználásra. A kérdőív az 1/D. mellékletben érhető el. A mérőeszköz 10 állítást tartalmaz, amelyek az egyén stresszel és nehézségekkel való megküzdésének képességét mérik. A résztvevőknek egy ötfokú Likert-skálán kellett jelölniük (0 – egyáltalán nem igaz; 1 – ritkán igaz; 2 – néha igaz; 3 – gyakran igaz; 4 – szinte mindig igaz), hogy az egyes állítások mennyire voltak rájuk jellemzőek az elmúlt hónapban. Az eredmény az egyes tételekre adott pontok összegzéséből képződik, és 0-tól 40-ig terjedhet, ahol a magasabb pontszám magasabb szintű rezilienciát jelez.

2.2.3 Cybersecurity Scale kérdőív (CS-C) bemutatása

A 25 kérdésből, 5 alskálából álló Cybersecurity Scale-t (CS-C[8]) Arpaci és mtsai alkották meg 2021-ben [42]. A CS-C kérdőív a felhasználók kiberbiztonsági gyakorlatát és felfogását méri, valamint megfelelő validitással és megbízhatósággal rendelkezik. A teljes skála Cronbach-alfa értéke .887, és a hat alskála belső konzisztenciája ($.735 < \alpha < .810$) megfelelő. A kérdőív alapjait a NIST Cybersecurity Framework [139] és a Parkerian Hexad modell [140] képezi. A NIST a kiberbiztonsági gyakorlatokra és kockázatokra összpontosít, míg a Parkerian Hexad modell olyan kritikus biztonsági jellemzőket azonosít, melyek befolyásolják a felhasználók felfogását és gyakorlatát. A kérdőív az alapvető biztonsági keretrendszer, CIA[9] triád alapelveit [139] követve, tehát hat dimenzión keresztül (2. ábra) vizsgálja a felhasználók kiberbiztonsággal kapcsolatos gyakorlatát, tudását és tudatosságát.



2. ábra A CS-C kiberbiztonsági skála dimenziói [forrás: saját szerkesztés]

[8] CS-C Cybersecurity Scale – Kiberbiztonsági skála
[9] CIA - Confidentiality, Integrity, Avalilability – Bizalmasság, Sértetlenség, Rendelkezésre állás

Természetesen ezen aspektusokon felül lehetnek egyéb kulcsfontosságú kiberbiztonsági jellemzők, mint az anonimitás, a magánélet védelme és a reziliencia készség, melyek hatással lehetnek a felhasználók kiberbiztonsági felfogására és gyakorlatára. A kérdésekre ötfokozatú, 1-5 válaszokat lehetett adni, ahol az 1 *"határozottan nem értek egyet"* és az 5 *"határozottan egyetértek"* skálán jelzik, hogy az egyes állítások milyen mértékben írják le az egyén tapasztalatait, hozzáállását és gyakorlatát. A magasabb pontszám magasabb szintű kiberbiztonsági tudatosságra utal [42].

2.2.4 Kiberbiztonságtudatosság kérdőív magyar adaptációja és validálása

A kiberbiztonsági tudatosság, CS-C kérdőív magyar nyelvű adaptációja során szisztematikus hatlépcsős eljárás került alkalmazásra, amely nemzetközi szabvány és irányelv alapján lett meghatározva [141]. A magyar nyelvre fordított, adaptált CS-C változatának elnevezése a továbbiakban, CS-C-H néven jelenik meg. A mérőeszköz teljes adaptálási és pszichometriai validálási folyamata, beleértve a feltáró és megerősítő faktoranalízist, valamint a vizsgált populáció eredményeinek összefoglalása, csoportok közötti különbségeinek elemzése egy korábbi publikáció [S-7] keretében került részletes bemutatásra. A disszertáció terjedelmi korlátja miatt jelen fejezetben ezen folyamat rövid áttekintése kerül bemutatásra.

A CS-C-H kérdőív Pilot és a re-teszt mérés megbízhatósági tesztjének értékelése magas szintű belső konzisztenciát jelez mindkét esetben, melyet a 3/B. melléklet táblázata szemléltet. A kapott $\alpha_{pilot} = .772$ és $\alpha_{re\text{-}test} = .836$, az eredeti kérdőív értékétől kis mértékben tér el, mely $\alpha = .887$. A vizsgálat kiterjedt az egyes dimenziók belső érvényességének vizsgálatára is. Az alskálák, dimenziók megfelelő belső konzisztenciát mutattak $(.621 < \alpha < .795)$. A Kaiser-Meyer-Olkin (KMO) adatok mintavételi megfelelőségének értéke 0.850 alapján az adathalmaz alkalmas a faktoranalízisre. A Bartlett próba szignifikánsan magas értéke ($\chi^2 = 3340.778, df = 300, p < .001$) további megerősítést nyújt a változók közötti szignifikáns korrelációkról. A CS-C-H kérdőív hat dimenzió mentén vizsgálja a kiberbiztonsági tudatosságot az eredeti kérdőívhez hasonlóan. A kérdőív konstrukciós érvényességének vizsgálatához főkomponens-analízist (PCA) alkalmaztam varimax rotációval. Az elemzés célja a 25 változóból álló halmaz dimenziócsökkentése olyan főkomponensekre, amelyek az eredeti változók varianciájának legnagyobb részét magyarázzák. Az elemzés alapján azonosításra került az eredeti hat fő komponens, amelyek közül mindegyikhez különböző kérdések vagy kérdéscsoportok kapcsolódnak. A feltáró elemzéssel kapott hatfaktoros struktúra alskálái

öt alskála esetén (bizalmasság, sértetlenség, elérhetőség, hitelesség, hasznosság) teljesen, egy alskála (felügyelet) esetén részben (három kérdés CSC05, CSC06, CSC09 kivételével) tükrözték az eredeti dimenziók tartalmát. Mivel az egyes komponensekhez rendelt tételek nagyrésze erősen korrelál az adott faktorral, csupán néhány tétel esetén alacsonyabb ez az érték, de ezek is megfelelő szinten vannak *(.458 < r < .815)*, ezért egy tétel sem került törlésre a nagymintás felmérést megelőzően.

Összességében a kapott alskálák reprezentálják a faktorokat és az azokhoz kapcsolódó kérdéscsoportokat, amelyek egyúttal tükrözik az eredeti kérdőív dimenzióit. Megállapítható, hogy a CS-C-H kiberbiztonsági tudatosság mérő kérdőív alkalmas a diákok kiberbiztonsági attitűdjeinek megbízható és értelmezhető mérésére a magyar oktatási intézményekben, és a további nagymintás mérőeszközeként szolgálhat. A teljes kérdőív szövege az 1/E. mellékletben található.

2.2.5 Fókuszcsoport beszélgetés képasszociatív technikával

A kvalitatív beszélgetések célja a Z és Alfa generációhoz tartozó hallgatók digitális viselkedésmintáinak, kiberbiztonsági attitűdjeinek és kockázatkezelési mechanizmusainak feltárása, valamint e tényezők mentális egészségre gyakorolt hatásainak elemzése nyílt végű kérdések alkalmazásával. Összesen 17 kérdés szerepelt az interjún, mely kérdések a 2/C. mellékletben érhetők el. A válaszok segítségével feltérképezésre került az online eltöltött idő és az online tevékenységek típusai, valamint a résztvevők által érzékelt online veszélyek és biztonságérzet az általuk használt platformokon. Betekintést nyújt a személyes adatok védelmére alkalmazott biztonsági intézkedéseket, a jelszókezelési gyakorlatokat, valamint a kiberbűnözéssel kapcsolatos tapasztalatokat illetően. A kérdések kitérnek az online viselkedést befolyásoló tényezőkre, például a biztonságos internetezésre törekvés elmaradásának okaira. Emellett vizsgálom az online tevékenységek által felmerülő alvászavarok, és az online tevékenységek okozta stressz mentális hatásait. Az asszociatív technikával alkalmazott, tematikusan válogatott képek segítségével feltárásra kerülnek a kibertérrel kapcsolatos legnagyobb aggodalmaik és a szorongást okozó élmények a résztvevők körében. Néhány mintakép az asszociációs kérdéshez a 2/D. mellékletben érhető el.

2.3 Adatelemzési módszertan

A kvantitatív és kvalitatív adatok kódolására, tisztítására, kategorizálása és feldolgozására az IBM SPSS Statistics 27, Microsoft Excel, NVivo, Voyant és Python

3.11.13 szoftverek kerültek alkalmazásra. A Python-alapú elemzésekhez pandas, NumPy, scikit-learn, factor_analyzer, sklearn, NLTK, semopy, seaborn valamint matplotlib könyvtárakat használtam. A mediációs és moderált mediációs elemzésekhez Andrew F. Hayes PROCESS v5 makrójának különböző modelljei kerültek alkalmazásra, ahol a Model 4 az egyszerű mediáció vizsgálatára szolgál, lehetővé téve a mediator (M) közvetítő szerepének felmérését az X → Y kapcsolatban, a Model 7 a mediáció X → M útvonalának moderáltságát teszteli, míg a Model 14 a mediáció M → Y útvonalát moderálja, míg a Model 10 mindkét útvonal moderáltságát vizsgálja.

2.3.1 Kvantitatív elemzési módszerek

A kutatási hipotézisek tesztelésére az adatokon a leíró statisztikák (átlag, szórás) mellett korrelációszámítás (Pearson és Spearman féle r), regresszióanalízis, reliabilitás vizsgálat (Cronbach-alfa, α), valamint feltáró és megerősítő faktorelemzés (EFA, CFA) többváltozós elemzési eljárások kerültek alkalmazásra. A közvetítő hatások vizsgálata mediációs útvonal-elemzéssel valósult meg. A csoportok közötti különbségek vizsgálatára többféle statisztikai eljárás került alkalmazásra a változók mérési szintjének és az összehasonlítandó csoportok számának függvényében. Két független csoport esetében t-próbák, míg ordinális vagy nem normál eloszlású folytonos változók vizsgálatakor Mann-Whitney U teszt került felhasználásra. Kettőnél több csoport összehasonlítására varianciaanalízis (ANOVA), illetve nem parametrikus esetben Kruskal-Wallis H teszt került kiválasztásra a folytonos változók elemzésére. Kategorikus változók csoportonkénti eloszlásának vizsgálatára khí-négyzet (χ^2) próba került felhasználásra. Az adatstruktúra feltárása klaszteranalízissel történt. Az optimális klaszterszám meghatározása könyökszabály alapján, a csoportosítás K-means (K-közép) algoritmussal került végrehajtásra. Minden statisztikai próba esetében $p < .05$ szignifikancia szint, a korrelációs együtthatók esetén $|r| \geq .30$ közepes hatásméret került meghatározásra [142]. A statisztikai elemzések során alkalmazott küszöbértékek a nemzetközi standardoknak megfelelően kerültek meghatározásra, ahol a Cronbach-alfa reliabilitási mutató esetében $\alpha > .60$ [143], [144], a Kaiser-Meyer-Olkin (KMO) mutató tekintetében $> .60$, míg a faktorsúlyok vonatkozásában $> .40$ értékek jelentették az elfogadhatóság alsó határát [143], [145].

2.3.2 Kvalitatív elemzési módszerek

A szöveges adatok előfeldolgozása során adattisztítás, tokenizálás, szótövezés, valamint a stopszavak eltávolítása került sor. Az átiratok a tartalomelemzés és a háromoszlopos

tematikus elemzés módszerével kerültek feldolgozásra [146]. Az átiratok jelentésegységeinek kialakítását követően, értelmező kódok kerültek meghatározásra, majd a kutatási kérdésekre adott válaszok összesítése történt meg. A tartalmak elemzése, kódolása, és a releváns témák, minták felfedése induktív megközelítéssel történt [147]. A vizsgálat részét képezte a kulcsszavak és kifejezések gyakoriságának, valamint a szavak közötti korrelációvizsgálat feltárása, a gyakran együtt előforduló kifejezések és azok összefüggései Voyant és az NVivo szoftver segítségével [148]. Az elemzés célja a kvantitatív mintázatok hátterében rejlő tapasztalatok, attitűdök és stratégiák mélyebb megértése.

2.3.3 Adatintegráció, kiberreziliencia modell felépítés és validáció

A tanulmány többlépcsős, szekvenciális magyarázó vegyes módszertani megközelítést alkalmaz, ahol a kvantitatív fázis célja a személyes kiberreziliencia skála (PCRS) integrálása, megalkotása a használt mérőeszközöket felhasználva, validálása és a kiberreziliencia profilok azonosítása. A kvalitatív fázis a kvantitatív eredmények, különösen a generációs és nemi különbségek mélyebb megértését szolgálta.

A PCRS item-készlet alapja a korábban bemutatott három validált mérőeszköz. A kiberbiztonsági tudatosság kérdőív magyar adaptációjából (CS-C-H), a Connor-Davidson reziliencia kérdőívből (CD-RISC) és a problémás internethasználat skálából (PIU) került kiválasztásra az integrált kiberreziliencia faktorszerkezet feltáró faktoranalízishez szükséges tételegyüttes. A három kérdőívből származó adatok integrálását követően a teljes minta véletlenszerű mintavétellel két független részhalmazra lett felosztva. A modellépítéshez a minta 70%-a tanítóhalmazként, míg 30%-a teszthalmazként lett elkülönítve a modell objektív értékelése céljából. Az első fázisban a PCRS pszichometriai vizsgálata feltáró faktoranalízissel (EFA) történt. Az elemzés előfeltételeinek ellenőrzéseként a Kaiser-Meyer-Olkin mutató *(> .60)* és a Bartlett-teszt szignifikanciája került tesztelésre. A végső tételek megtartási kritériuma > *.40*-es faktortöltés és jelentős kereszttöltések kizárása volt Promax rotáció mellett. Egy darab alacsonyabb töltésű tétel megtartására mellett döntöttem a hozzá kapcsolódó faktor tartalmi validitásának biztosítása érdekében. A faktorok belső megbízhatóságát Cronbach-alfa *(α > .60)* mutatta. A tanítóhalmazon feltáró faktorelemzés (EFA) került végrehajtásra a faktorstruktúra azonosítása érdekében. Az EFA eredményei és az elméleti keret alapján a strukturális egyenletmodell (SEM) specifikálása történt meg, amely során mind a mérési modell, mind a strukturális modell definiálásra került. A modell validálására másodrendű

megerősítő faktorelemzés (CFA) lett végrehajtva a 70%-os tanító és 30%-os teszt halmazon, standard illeszkedési mutatók (*CFI > .90, TLI > .90, RMSEA < .08, SRMR < .08*) alapján értékelve. A modell külső validációja a teszthalmazon lett elvégezve [143], [144], [145], [149]. A validált faktorok z-pontszámai alapján K-means klaszteranalízis azonosította a kiberreziliencia profilokat. A profilok generációs és nemi eloszlását khí-négyzet próba, az aldimenziók mentén mutatkozó különbségeket független mintás t-próbák és Mann-Whitney U teszt vizsgálta ($p < .05$) [142].

Módszertani keret összegzése

A jelen fejezetben részletesen bemutattam a kutatás módszertani keretét, amely vegyes módszertani megközelítésen alapul. A nagymintás kvantitatív adatfelvételt *(N = 3275)* kiegészítő fókuszcsoportos beszélgetések *(N = 89)* gazdagították, lehetővé téve az online szokások és jelenségek kvantitatív és kvalitatív aspektusainak integrált vizsgálatát. A mintavételi stratégia biztosította a Fejér Vármegye Z és Alfa generáció megfelelő reprezentációját, míg az etikai protokollok garantálták a résztvevők védelmét és az önkéntes részvételt. A mérőeszközök bemutatása során kiemelt figyelmet kapott a kiberbiztonsági tudatosságot mérő kérdőív (CS-C-H) adaptációja és validálása, amely lehetővé tette a kiberbiztonsági tudatosság megbízható mérését a vizsgált populációban. A reziliencia és a problémás internethasználat mérésére alkalmazott validált eszközök szintén megfelelő pszichometriai tulajdonságokat mutattak. Az adatelemzési módszertan mind a kvantitatív (leíró statisztikák, korrelációs, regresszós elemzések, mediációs és moderációs modellek), mind a kvalitatív (tematikus elemzés) komponensek esetében megalapozott és átlátható eljárásokat követett. Az adatintegráció és modellépítés módszertana biztosította, hogy a különböző adatforrásokból származó információk egységes keretrendszerbe történő integrálását.

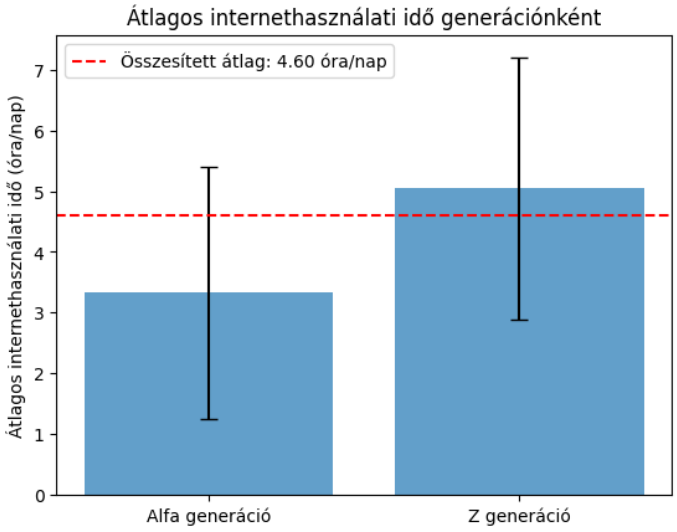
A következő fejezetben az itt bemutatott módszertani keretek alapján gyűjtött és elemzett kvantitatív adatok eredményei kerülnek bemutatásra, amelyek a kutatási kérdések megválaszolásának és a hipotézisek igazolásának első lépését képezik.

3 KVANTITATÍV EREDMÉNYEK

A jelen fejezet a kvantitatív kutatás keretében végzett empirikus vizsgálat eredményeit mutatja be részletesen. A kutatás során három validált mérőeszköz került alkalmazásra. A problémás internethasználat kérdőív, a reziliencia kérdőív, valamint a kiberbiztonsági tudatosság kérdőív, melyek segítségével az internet problémás használata, a pszichológiai ellenálló képesség és a kiberbiztonsági tudatosság közötti összefüggéseket a Z és Alfa generációs csoportokat érintően vizsgáltam. Először a három kérdőív alapstatisztikai jellemzőit és a skálák belső konzisztenciáját mutatom be, majd az egyes mérőeszközökkel nyert eredményeket ismertetem külön-külön, a generációs és nemi különbségek elemzésével együtt. Végül a moderációs elemzések rávilágítanak arra, hogy a reziliencia és a problémás internethasználat milyen módon befolyásolhatja a kiberbiztonsági tudatosság mértékét.

3.1 A kérdőívek leíró statisztikai jellemzői és megbízhatósága

A kutatásban összesen 3275 fő vett részt. A résztvevők generációs megoszlása szerint a minta jelentős többségét a Z generáció tagjai alkották *(N = 2438, 74.4%),* míg a fennmaradó részt az Alfa generáció képviselte *(N = 837, 25.6%).* A nemek arányát tekintve a mintában valamivel több férfi *(N = 1746, 53.3%)* vett részt, mint nő *(N = 1529, 46.7%).* A résztvevők átlagosan 4,6 órát töltöttek naponta internetezéssel (*M* = 4,60, *SD* = 2,27). A két generáció napi internethasználata szignifikánsan eltér *(t(3273) = - 20.02, p < .001)*, melyet a 3. ábra szemléltet.



3. ábra Átlagos napi internethasználati idő generációnként [forrás: saját szerkesztés]

A Z generáció tagjai szignifikánsan több időt töltöttek online, mint az Alfa generáció tagjai *(U = 579609.000, p < .001; r_s = .338, p < .01).* Az Alfa generáció tagjai *(N = 837)* átlagosan *3.33 ± 2.08* órát töltenek naponta internetezéssel, míg a Z generáció tagjai átlagosan *5.05 ± 2.16* órát töltenek naponta internetezéssel. Ez azt jelzi, hogy a képernyőidő generációnként eltérő mintázatot követ, még ha mindketten digitális környezetben szocializálódnak is. A napi átlagos internethasználat nemek közötti különbségének független mintás t-próba eredménye alapján, a férfiak átlagosan *4.56 órát (SD = 2.30, N = 1746),* míg a nők 4.66 órát *(SD = 2.24, N = 1529)* töltenek naponta online. A t-próba sem mutatott szignifikáns különbséget a nemek között, *t(3273) = - 1.277, p = 0.202.* Az eredmények alapján **a napi internethasználat mennyisége nem különbözik szignifikánsan a férfiak és nők között**. Az eredmények alapján viszont nem függetlenül elmondható, hogy aki többet internetezik naponta, annál nagyobb valószínűséggel alakul ki problémás internethasználat. Ez az összefüggés szignifikáns, közepes kapcsolattal írható le *(r_p = 0.321, p < 0.001)*, mely alapján **a napi internethasználat idejének növekedésével párhuzamosan emelkedik a problémás használat kockázata is**.

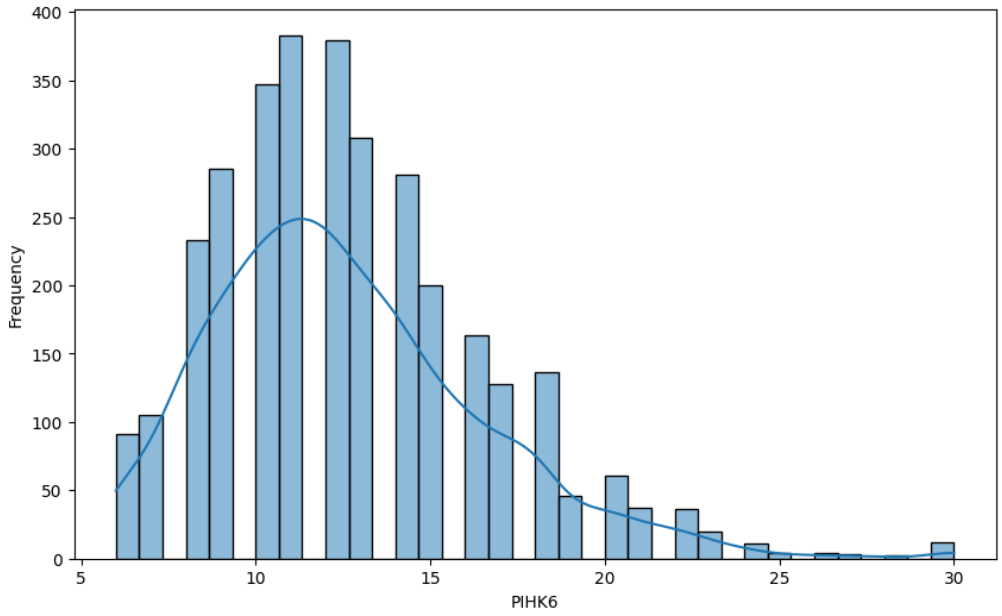
A Z generációban a napi internethasználat számos demográfiai változóval mutatott gyenge, de szignifikáns összefüggést. A nők több időt töltenek online, mint a férfiak. Az iskolatípus, a szakirány, a tudományterület és a szülői iskolai végzettség szignifikánsan befolyásolta az internethasználatot, míg a lakóhely nem. A felsőoktatásban tanulók interneteznek a legtöbbet *(M = 5.27, SD = 2.02).* Tudományterületek közül az informatika és gazdaságtudomány hallgatói töltik a leghosszabb, átlagosan *5.44 ± 2.14* órát online. A szülői végzettség tekintetében az általános iskolai végzettségű szülők gyermekei kimagaslóan magasan, átlagosan *5.44 ± 2.14* órát használják az internetet, a felsőfokú végzettségű szülők gyermekei pedig a legrövidebb ideig *(M = 4.85, SD = 2.14)*.

3.1.1 Problémás internethasználat kérdőív alapstatisztikái

A PIH skála belső konzisztenciájának vizsgálatára Cronbach-alfa együtthatók kerültek kiszámításra *(N = 3275).* A teljes skála megbízhatósága elfogadhatónak tekinthető *(α = .635),* azonban a kontrollzavar *(α = .285)* és az elhanyagolás *(α = .320)* alskálák esetében alacsony konzisztencia mutatkozott, míg az obszesszió alskála megbízhatósága elfogadható α = .683. A PIH skála belső struktúrájának korrelációs elemzése vegyes eredményeket mutat. Az egyes alskálák tételei között gyenge *(„kontroll” r = .17*,

„elhanyagolás” r = .19) vagy közepes *(„obszesszió” r = .52)* a kapcsolat. Ugyanakkor az egyes tételek erősen korreláltak saját alskálájukkal *(r = .74-.79),* az alskálák pedig a teljes pontszámmal *(r = .68-.79).* Bár a tételek közötti korreláció változó, a skála elméleti struktúrája, azaz az aldimenziók hozzájárulása az eredmények alapján a teljes koncepcióhoz megalapozottnak mondható. (A részletes korrelációs eredmények a 3/A. mellékletben találhatók.)

A résztvevők átlagos PIH-összesített pontszáma *M = 12.58*, *SD = 3.91,* a *medián* pedig *12*. A pontszámok 6 és 30 között helyezkedtek el, a válaszadók középső fele 10 és 15 pont közötti értéket ért el. A pontszámok eloszlása a 4. ábrán tekinthető meg.



4. ábra A PIH-összesített pontszámok gyakorisági eloszlása (N = 3275) [forrás: saját szerkesztés]

A 4.ábrán az eloszlás enyhe balra tolódást mutat, vagyis a legtöbb résztvevő az alacsonyabb és közepes tartományban helyezkedik el, miközben egy kisebb csoport jóval magasabb értékeket ért el. Ezt alátámasztja, hogy az átlag meghaladja a mediánt, mivel a magasabb értékek felfelé emelik azt. A viszonylag magas szórás jelentős egyéni különbségeket jelez a problémás internethasználat szintjében.

A **kontrollzavar dimenzió** átlagértéke *M = 4.26 (SD = 1.62)* mely mérsékelt kontrollvesztésre utal az internethasználatot illetően. Az első tétel *(„Milyen gyakran érzed úgy, hogy csökkentened kellene az internetezéssel töltött időt?”)* átlagértéke *2.68 ± 1.11,* mely szerint a résztvevők gyakran érzik szükségét az internethasználat csökkentésének. A második tétel *(„Milyen gyakran próbálod titkolni, hogy mennyi időt töltöttél internetezéssel?”)* átlagértéke *1.58 ± 1.01*, tehát azzal, hogy titkolják, vagy

titkolniuk kellene, hogy az idejüket internetezéssel töltik, kevésbé jellemzi a válaszadókat.

Az obszesszió dimenziói az internethasználathoz kapcsolódó megszállottságot és érzelmi függőséget vizsgálja. Az **obszesszió dimenzió** átlagértéke *3.38 ± 1.77,* ami mérsékelt szintű internethasználati megszállottságra utal. Az első tétel *(„Milyen gyakran érzed nyugtalannak, feszültnek magad, ha nem internetezhettél annyit, amennyit szerettél volna?”*) átlagértéke *1.90 ± 1.07,* míg a második tétel *(„Milyen gyakran fordul elő, hogy depressziósnak, szomorúnak, idegesnek érzed magad, amikor nem internetezel, és ez az érzés elmúlik, amikor újra internetezni kezdesz?”)* átlagértéke *1.48 ± 0,96.*

Az elhanyagolás dimenziói az internethasználat által okozott elhanyagolási magatartást értékeli. Az **elhanyagolás dimenzió** átlagértéke *4.94 ± 1.86* mely szerint a résztvevők gyakran tapasztalnak elhanyagolási tüneteket a túlzott internethasználat miatt. A két tétel *(„Milyen gyakran internetezel olyankor, amikor inkább aludnod kellene?” és „Milyen gyakran panaszkodnak a környezetedben lévők arra, hogy túl sokat internetezel?”)* átlagértékei *2.80 ± 1.26*) és *2.14 ± 1.15*.

Az eredmények alapján megállapítható, hogy a vizsgált mintára a **mérsékelt problémás internethasználat jellemző**, a kontrollzavar és elhanyagolás dimenzióiban. Az obszesszió dimenziói kevésbé mutatnak súlyos problémákat, ami arra utal, hogy bár az internethasználat befolyásolja a résztvevők életét, **az érzelmi megszállottság és függőség mértéke viszonylag alacsony**.

3.1.2 Reziliencia skála alapstatisztikái

A skála belső megbízhatósága a jelenlegi mintán *(N = 3275)* megfelelő, a Cronbach-alfa érték $\alpha = .82$, mely közelíti az eredeti $\alpha = .85$ értéket. Az item-analízis eredményei alátámasztják a skála belső konzisztenciáját, értékei *.328 és .621* között szóródnak, mely megegyezik az eredeti és a validált [131] forrásokkal. A legalacsonyabb korrelációs értéket *(„A megérzéseim alapján kell cselekednem”,* $r_s = .328$), a legmagasabbat pedig a *„Nagyon céltudatos vagyok”* tétel mutatta *(*$r_s = .621$*).* A teljes skála átlagpontszáma *M = 26.05 (SD = 6.96),* mely nagyon hasonló a Campbell-Sills és Stein [146] *N = 1622* populáción mért értékével *(M = 27.21, SD = 5.84).* Ezen eredmények alapján a CD-RISC-10 skála megbízható mérőeszköznek tekinthető a vizsgált populációban.

A generációs alcsoportokat tekintve a Z generáció tagjai enyhén magasabb átlagos reziliencia pontszámmal (*M = 26.36, SD = 6.85*) rendelkeztek, mint az Alfa generáció tagjai (*M = 25.14, SD = 7.17*).

3.1.3 Kiberbiztonságtudatosság kérdőív (CS-C-H) alapstatisztikái

A kiberbiztonságtudatosság kérdőív elemzése alapján a válaszadók általánosan magas szintű tudatosságról számoltak be, a teljes pontszám átlaga magas volt (*M = 96.57, SD = 14.70*) a maximálisan elérhető 125 ponthoz képest. A teljes skála Cronbach-alfa értéke *.836*, és a hat alskála belső konzisztenciája *(.621 < α < .795)*.

A legerősebb területeknek a hitelesség (*20.96 ± 4.09*), a felügyelet (*20.72 ± 3.97)* és a bizalmasság (*16.86 ± 3.30*) alskálák bizonyultak. Az egyedi tételek elemzése azt mutatja, hogy **a válaszadók óvatosak a jelszavak megosztásával, az adataik láthatóságának korlátozásával és az ismeretlen forrásból származó e-mailekkel szemben** (*4.35<M<4.51*). Ezzel szemben a legalacsonyabb átlagpontszámot a sértetlenség alskálánál értéke el a válaszadók *(12.60 ± 3.86)*. A kapott eredmény ellentmondásos attitűdöt tükröz. A válaszadók egyértelműen **elutasították, hogy az adatmegosztás kockázatmentes** (*M = 2.37*), ami pozitív, hiszen tudatos hozzáállásra utal. Ugyanakkor **bíznak a kibertérben való adattárolásban**, bíznak abban, hogy az adataik biztonságban vannak az online térben (*M = 3.19*) és nem veszhetnek el (*M = 3.69*), ami potenciális sebezhetőségre utal. Hasonlóképpen, a proaktív védelmi eszközök használatát mérő hozzáférhetőség alskála (*14.15±4.35*) és a hasznosság alskála (*11.28±2.73*) pontszámai is alacsonyak voltak. Ezen kategórián belül, különösen **a rendszeres vírusellenőrzésre** (*M = 3.35*) és **a letöltött fájlok vizsgálatára** (*M = 3.48*) vonatkozó tételek kaptak **alacsonyabb értékelést**, ami arra utal, hogy **a passzív óvatosság, a bizalmatlanság erősebb, mint az aktív, rutinszerű védelmi cselekvések.**

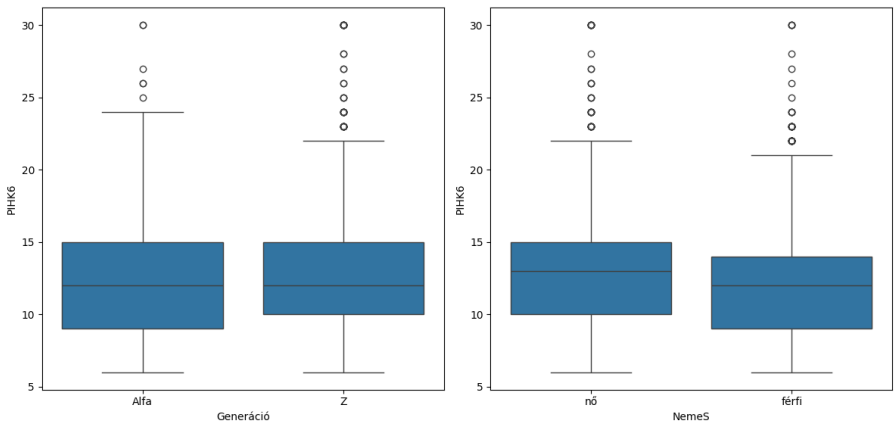
3.2 Problémás internethasználat kérdőív eredményei

A Spearman-féle rangkorrelációs együttható értéke alapján a különböző demográfiai változók, generáció *($r_s = 0.043$, $p < 0.05$),* neme *($r_s = 0.133$, $p < 0.01$),* szakirány ($r_s = -0.066$, $p<0.05$), tudományterület *($r_s = -0.045$, $p<0.05$),* átlagos napi internethasználati idő *($r_s = 0.323$, $p < 0.01$)* és a PIH összesített pontszám között több szignifikáns, eltérő mértékű és irányú korreláció van, mely szerint ezek a változók befolyásolhatják a problémás internethasználat kialakulását.

3.2.1 Problémás internethasználat generációs eltérései

A generációs hovatartozás és a PIH dimenziók között eltérő mértékű és irányú kapcsolat figyelhető meg. Az **elhanyagolás** alskála esetén gyenge, szignifikáns pozitív a korreláció *(r = 0.123, p < 0.01),* míg a **kontrollzavar** *(r = -0.042, p < 0.05)* és a **PIH összesített pontszám** *(r = 0.037, p < 0.05)* esetében gyenge, statisztikailag szignifikáns korrelációk vannak. Az **obszesszió** alskála dimenzió esetében nincs szignifikáns kapcsolat a generáció változóval. Az eredmények alapján a generációs különbségek hatással vannak a problémás internethasználat, mentális egészség különböző aspektusaira, de ezek a hatások dimenziónként eltérő fokúak és irányúak.

Az **Alfa generáció enyhén magasabb kontrollzavar** átlagértékkel *M = 4.38 (SD = 1.62)* és az obszesszió értékkel *M = 3.41 (SD = 1.78)* rendelkezik, mint a Z generáció *M = 4.22 (SD = 1.617)* és *M = 3.37 (SD = 1.762).* Az átlagok közötti különbség kicsi, de az eltérés szignifikáns mindkét esetben *(F(1,3273) = 5.790, p = 0.016; F(1,3273) = 0.291, p = 0.59).* Az **elhanyagolás skála átlagértéke enyhén magasabb a Z generációban** *(M = 5.07, SD = 1.82),* mint az Alfa generáció csoportjában *(M = 4.54, SD = 1.90),* a különbség szignifikáns a generációk között *F(1,3273) = 50.529, p < 0.001).* A Z generáció tagjai sűrűbben tapasztalják, hogy a gyakori internethasználat miatt elhanyagolják a feladataik elvégzését. A **Z generáció átlagos összpontszáma enyhén magasabb** *M = 12.66 (SD = 3.87),* mint az Alfa generációé *M = 12.33 (SD = 4.01),* szignifikáns különbséggel a generációk között *(F(1,3273) = 4.470, p = 0.035).* A 5. ábra alapján a Z generáció tagjainak PIH pontszámai enyhén magasabbak, mint az Alfa generáció tagjaié. Mindkét csoportban megfigyelhető a pontszámok pozitív ferdesége, amit a medián felett elhelyezkedő számos kiugró érték is jelez.



5. ábra Problémás internethasználat mértéke generációnként és nemenként [forrás: saját szerkesztés]

3.2.2 A problémás internethasználat nemi aspektusai

Szignifikáns, gyenge pozitív korreláció van a résztvevők neme és PIH eredménye között *(r = 0.136, p < 0.01)*, valamint az egyes aldimenziókban is, a kontrollzavar esetén *(r = 0.154, p < 0.01)*, obszesszió dimenzió *(r = 0.070, p < 0.01),* és az elhanyagolás dimenzióval *(r = 0.085, p < 0.01).*

A kontrollzavar dimenzió esetében a nemek közötti különbség statisztikailag szignifikáns *(F = 79.919, p < 0.001).* Az eredmények alapján a nők átlagosan magasabb pontszámot értek el *(M = 4.53, SD = 1.65),* mint a férfiak *(M = 4.03, SD = 1.56),* mely szerint **a nők nagyobb kontrollzavart tapasztalnak az internethasználat során**, mint a férfiak.

Az **obszesszió dimenzióban** szintén szignifikáns különbséget tapasztaltunk a nemek között *(F = 15.930, p < 0.001).* Az eredmények alapján **a nők magasabb átlagpontszámot értek el** *(M = 3.51, SD = 1.85)* a férfiaknál *(M = 3.27, SD = 1.68).*

Az elhanyagolás dimenzióban *(F = 23.996, p < 0.001)* a nők átlagpontszáma *M = 5.11 (SD = 1.91),* míg a férfiaké *M = 4.79 (SD = 1.80),* tehát **a nők nagyobb mértékben tapasztalják az internethasználat elhanyagoló hatásait, következményeit.**

A független mintás t-próba erősen szignifikáns eredményt adott *t(3273) = -7.85, p < .001.* A nők átlagpontszáma *(M = 13.15, SD = 4.01)* magasabb, mint a férfiaké *(M = 12.08, SD = 3.73)*, jelezve, hogy **a nőkre jellemzőbb a problémás internethasználat.**

Összességében a problémás internethasználat mértékét mind a nem, mind a generáció befolyásolja, azonban a nemek közötti különbség jóval markánsabbnak bizonyult a vizsgált mintában, ahogy ezt az 5. ábra mutatja.

3.2.3 A problémás internethasználat prediktorainak vizsgálata

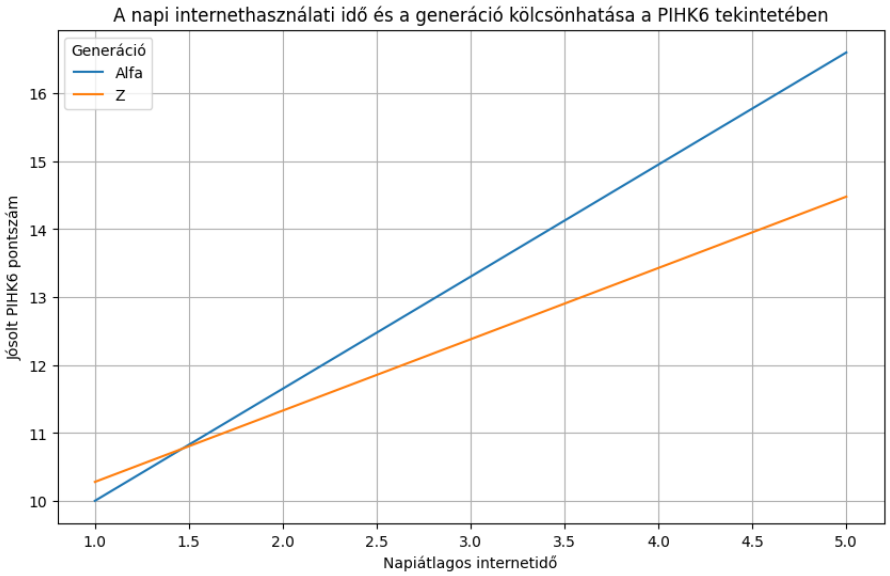
A problémás internethasználat prediktorainak vizsgálatára három lineáris regressziós modell került illesztésre. A napi átlagos internethasználati idő szignifikáns és pozitív prediktorként azonosítható *(R^2 = .103, F(1,3273) = 375.4, p < .001, b = 1.11).* A modell a variancia 10.3 százalékát magyarázza, ami a vizsgált változók közül a legerősebb hatásnak tekinthető. A nem szintén szignifikáns prediktorként jelenik meg *(R^2 = .018, F(1,3273) = 61.58, p < .001, b = 1.07)*, de csupán a variancia 1.8 százalékát magyarázza. A nők által átlagosan *1.07* ponttal értek el magasabb eredményt a problémás internethasználat skálán, mint a férfiak. A generációs hovatartozás statisztikailag

szignifikáns szintén szignifikáns volt *(R^2 = .001, F(1, 3273) = 4.47, p = .035, b = 0.33),* azonban a variancia alacsony értéke (0.1%) miatt gyakorlati jelentősége elhanyagolhatónak tekinthető. **Az eredmények alapján a napi internethasználati idő a problémás internethasználat legerősebb prediktora,** míg a *nem* mérsékelt, a *generáció* pedig elhanyagolható mértékben járul hozzá a pontszámok alakulásához.

A problémás internethasználat prediktorainak vizsgálatára többszörös lineáris regressziós modell is illesztésre került a generációs hovatartozás, a nem és a napi átlagos internethasználat bevonásával. A teljes modell szignifikáns, *F(3,3271) = 154.5, p < .001,* és a variancia 12.3 százalékát magyarázta (*korrigált R^2 = .123*). Mindhárom prediktor szignifikáns egyedi hatást mutatott. A napi átlagos internethasználati idő volt a legerősebb pozitív prediktor ebben az esetben is *(b = 1.18, p < .001),* jelezve, hogy a magasabb online idő magasabb problémás internethasználati pontszámmal jár együtt. A *nem* szintén szignifikáns pozitív hatást gyakorolt *(b = 0.99, p < .001).* A generációs hovatartozás szignifikáns negatív prediktor volt (b = -0.65, p < .001), ami azt jelenti, hogy **az Alfa generáció alacsonyabb problémás internethasználati pontszámot mutat a Z generációhoz képest, miután a többi változó hatása kontrollálásra került.**

A napi internethasználati idő hatásának generáció és nem specifikus vizsgálatához moderációs elemzés készült. Az elemzés célja annak tesztelése volt, hogy a generációs és nemi hovatartozás moderálja-e a napi átlagos internethasználat és a problémás internethasználat közötti kapcsolatot. A regressziós modell szignifikáns volt, *F(3,3271) = 139.2, p < .001*, *korrigált R^2 = .112* a generációs moderáló hatásának vizsgálatában. Az eredmények szignifikáns interakciós hatást mutattak a napi internethasználat és a generáció között *(b = -0.60, p < .001),* tehát a napi internethasználati idő a problémás internethasználatra gyakorolt hatásának erőssége szignifikánsan különbözik a két generáció között. A kapott eredményeket a 6. ábra szemlélteti.

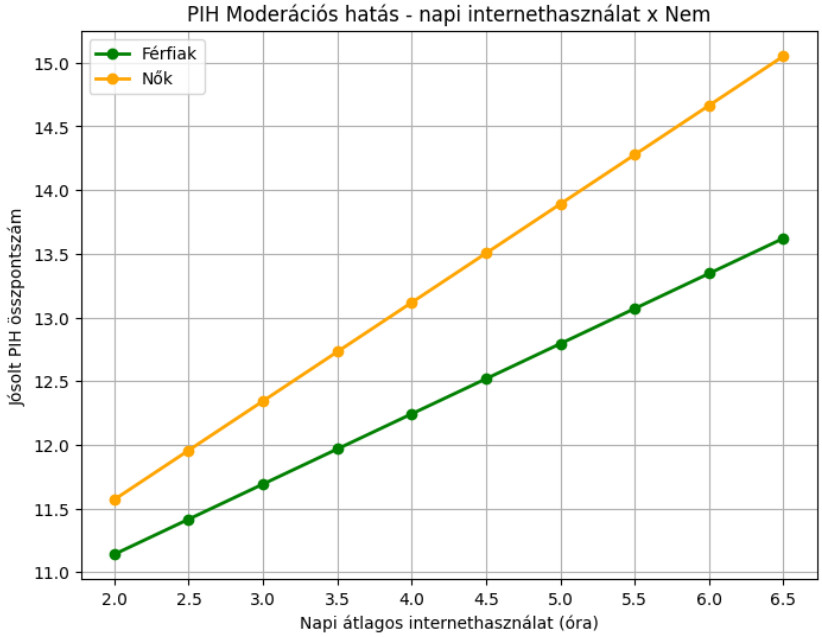
Az Alfa generáció esetében minden további egységnyi internethasználat növekedés 2.25 egységgel emeli a problémás internethasználat pontszámát, míg a Z generációnál ez a növekmény csupán 1.65 egység. Bár mindkét generációban **a több internethasználat magasabb kockázattal jár, a kapcsolat meredeksége mérsékeltebb a Z generációnál**.



6. ábra Az átlagos napi internethasználati idő és a generáció kölcsönhatása a PIH tekintetében [forrás: saját szerkesztés]

Ez arra utal, hogy a problémás internethasználat és a képernyőidő kapcsolatát a generációs kontextus érdemben befolyásolja.

A nemi hovatartozás moderáló hatását vizsgáló regressziós modell szignifikáns volt, $F(3,3271) = 153.78$, $p < .001$, korrigált $R^2 = .124$. A 7. ábra a napi átlagos internethasználat és a problémás internethasználat közötti kapcsolatot mutatja nemenként.



7. ábra A napi átlagos internethasználati idő és a nem kölcsönhatása a PIH tekintetében [forrás: saját szerkesztés]

Az interakciós elemzés szerint a kapcsolat szignifikánsan eltér a férfiak és a nők között *(b = 0.222, p < .001).* **A nőknél** a meredekség nagyobb, azaz **minden további egységnyi internethasználat erősebben növeli a problémás internethasználati pontszámot** (~0.67 pont), míg a férfiaknál a növekedés mérsékeltebb (~0.45 pont).

Összességében az eredmények arra utalnak, hogy **a problémás internethasználat kialakulásában és súlyosságában** a vizsgált populációban **az online töltött idő mennyisége, a nemi identitás és a generációs hovatartozás együttesen játszik szerepet**. A Z generáció kissé magasabb összesített PIH értékekkel rendelkezik az Alfa generációhoz képest. A nők lényegesen magasabb összesített pontszámot értek el, és a kontrollzavar, az obszesszió és az elhanyagolás területén is, mint a férfiak. A prediktív modellek alapján a napi internethasználati idő bizonyult a problémás internethasználat legerősebb prediktorának, amely a variancia jelentős részét magyarázza. A többszörös regressziós analízis kimutatta, hogy mindhárom változó független előrejelző szerepet tölt be. A moderációs elemzés alapján, mind a generációs, mind a nemi hovatartozás módosítja az internethasználat és a PIH közötti kapcsolatot. **Az Alfa generáció tagjai esetében az internethasználat növekedése erősebben emeli a problémás internethasználat mértékét**, mint a Z generáció tagjainál. Hasonlóan **a nőknél az internethasználat és a PIH közötti összefüggés intenzívebb**, mint a férfiaknál.

3.3 Reziliencia skála eredményei

A reziliencia teszt eredményeinek elemzése segít megérteni a résztvevők mentális rugalmasságát és stresszkezelési képességeit. Az eredmények alapján lehetőség van a reziliencia szintek összehasonlítására a demográfiai változók tükrében. Ebben a fejezetben a reziliencia összesített pontszámainak (RISC) eloszlásának vizsgálati eredményei kerülnek bemutatásra generációs és nemi aspektusból. A Shapiro–Wilk-teszt eredményei mind a generációs (Alfa generáció: *W(837) = .979, p < .001*; Z generáció: *W(2438) = .985, p < .001),* mind a nemi (férfi: *W(1746) = .980, p < .001*; nő: *W(1529) = .988, p < .001*) alcsoportokban szignifikánsan eltértek a normális eloszlástól. A normalitás feltételének sérülése miatt a csoportok összehasonlítására Mann–Whitney U-próba került felhasználásra.

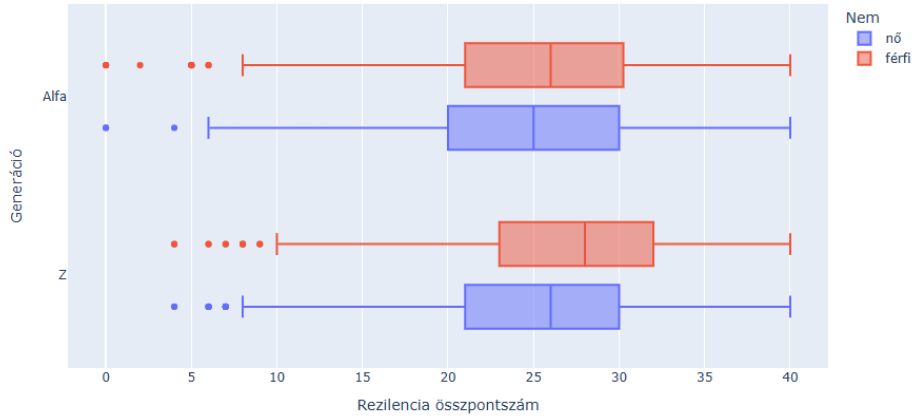
3.3.1 A reziliencia és a demográfiai háttér kapcsolata

A Kruskal-Wallis próba eredményei alapján az **állandó lakhely típusa alapján nem volt szignifikáns különbség** a reziliencia pontszámokban ($\chi^2(3) = 6.947,\ p = .074$). Ezzel szemben **a szülők legmagasabb iskolai végzettsége szignifikáns hatást gyakorolt** a rezilienciára ($\chi^2(3) = 20.135,\ p < .001$), tehát **minél magasabb a szülők iskolai végzettsége, annál magasabb a diákok reziliencia pontszáma**. A legmagasabb reziliencia szintet a diplomás szülők gyermekei (*Mean Rank = 1700.38*), míg a legalacsonyabbat az általános iskolai végzettségű szülők gyermekei mutatták (*Mean Rank = 1364.15*). Hasonlóan szignifikáns különbségek rajzolódtak ki az intézmény típusa ($\chi^2(2) = 31.677,\ p < .001$) és a tanulmányi szakirány ($\chi^2(2) = 26.559,\ p < .001$) mentén is. **A felsőoktatásban és középiskolában tanulók magasabb reziliencia szinttel rendelkeznek**, mint az általános iskolások. A szakirányok közül **a reál beállítottságú diákok mutatják a legmagasabb** (*Mean Rank = 1740.13*), míg az általános tantervű képzésben résztvevők a legalacsonyabb rezilienciát (*Mean Rank = 1541.26*).

A reziliencia és a napi internethasználat közötti kapcsolat vizsgálata Spearman-féle rangkorrelációval szignifikáns, gyenge negatív összefüggést mutatott ($r_s = -.144,\ p < .001$), amely szerint **a több online töltött idő alacsonyabb reziliencia összesített pontszámmal társul**.

3.3.2 Generációs és nemi különbségek a reziliencia területén

A Mann–Whitney U-próba eredményei statisztikailag szignifikáns különbséget mutattak a két generáció között ($U = 923181.50,\ z = -4.119,\ p < .001$). A rangsorok vizsgálata alapján, **a Z generáció tagjai magasabb összesített reziliencia pontszámmal** rendelkeznek (*Mean Rank = 1677.84*), mint az Alfa generáció tagjai (*Mean Rank = 1521.96*). A nemek összehasonlítására lefuttatott Mann–Whitney U-próba szintén szignifikáns különbséget tárt fel ($U = 1148668.50,\ z = -6.902,\ p < .001$). **A fiúk szignifikánsan magasabb összesített reziliencia pontszámmal rendelkeznek** (*Mean Rank = 1744.61*), mint a lányok (*Mean Rank = 1516.25*). A nemek és generációk szerinti különbségek a 8. ábra mutatja be.



8. ábra A reziliencia pontszámok eloszlása generáció és nemek szerint [forrás: saját szerkesztés]

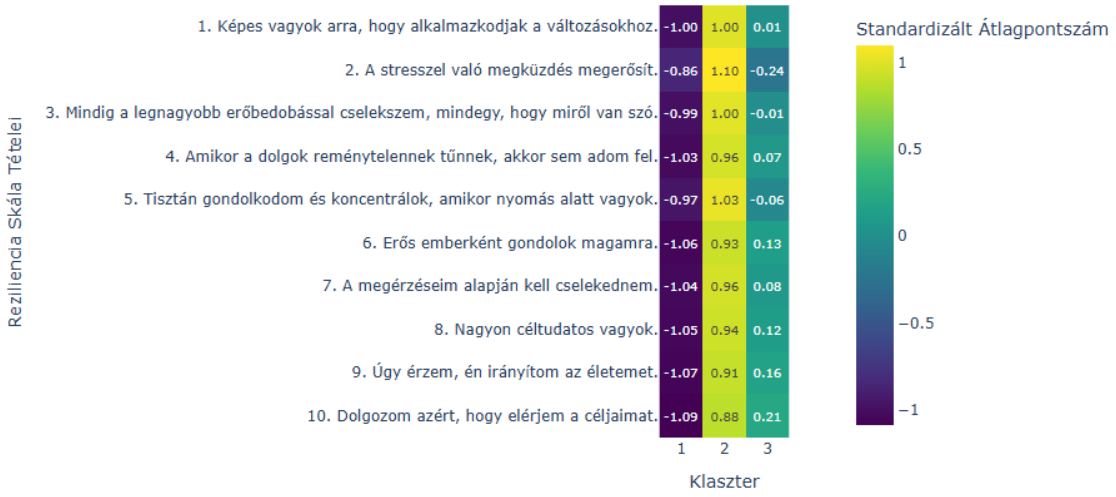
A diagramon jól látható, hogy a fiúk mediánértékei mindkét generációban magasabbak, mint a lányoké. Továbbá a Z generáció dobozdiagramjai, mindkét nem esetében enyhén jobbra tolódnak az Alfa generációhoz képest, jelezve a Z generáció magasabb összesített reziliencia pontszámait.

3.3.3 Reziliencia profilok klaszteranalízise demográfiai bontásban

A reziliencia profilok azonosítására kétlépcsős klaszteranalízist került alkalmazásra. Hierarchikus klaszteranalízis (Ward-módszer, négyzetesített euklideszi távolság) alapján a dendrogram és a könyökszabály a háromklaszteres megoldást jelölte optimálisnak. A K-középpontú klaszteranalízis 39 iteráció után konvergens megoldást eredményezett.

Az elemzés három jól elkülöníthető profilt azonosított, melynek vizuális ábrázolására a 9. ábra szolgál:

1. **Alacsony reziliencia („*Törékenyek*”)** – a minta 23,6%-a ($N = 772$). Item-pontszámaik 1–2 között mozogtak, különösen alacsony értékekkel a stresszkezelés ($M = 1$), önértékelés ($M = 1$) és kontrollérzés ($M = 1$) területén.
2. **Magas reziliencia („*Megállíthatatlanok*”)** – a minta 34,9%-a ($N = 1144$). A profilt magas pontszámok jellemzik (jellemzően $M = 3$), a célokért való küzdelem terén maximális értékkel ($M = 4$). Magabiztos, proaktív, hatékony megküzdési profil.
3. **Átlagos reziliencia** – a minta 41,5%-a ($N = 1359$). Ez a csoport egy mérsékelt, átlagos szintű (item-pontszámok 2–3 között) rezilienciával rendelkező populációt képvisel, akik bizonyos helyzetekben magabiztosak, míg másokban bizonytalanabbak lehetnek.



9. ábra A reziliencia profilok ábrázolása hőtérképpel, ahol az 1. klaszter – a „Törékenyek", a 2. klaszter – a „Megállíthatatlanok" és a 3. klaszter az átlagos rezilienciával rendelkező profilokat jelölik. [forrás: saját szerkesztés]

A khí-négyzet-próba statisztikailag szignifikáns, bár gyenge összefüggést mutatott a klaszter-hovatartozás és a generáció között ($\chi^2(2) = 16.415, p < .001$; *Cramer's V* = .071). Az **Alfa generáció tagjai voltak felülreprezentáltak az „Törékenyek", alacsony reziliencia klaszterben** (Alfa generáció 27.1%, Z generáció 22.4%). Ezzel párhuzamosan a **Z generáció tagjai nagyobb arányban kerültek a „Megállíthatatlanok", magas reziliencia klaszterbe** (36.8%), mint az Alfa generáció tagjai (29.5%). A klasztertagság és a nem között szintén szignifikáns, és az előzőnél erősebb kapcsolatot mutatkozott ($\chi^2(2) = 55.949, p < .001$; *Cramer's V* = .131). Az eredmények alapján **a lányok szignifikánsan felülreprezentáltak „Törékenyek" klaszterben** (lányok 29.0%, fiúk 18.8%). Ezzel összhangban **a fiúk nagyobb arányban tartoztak a „Megállíthatatlanok" klaszterbe** (39.3%), mint a lányok (30.0%).

Összefoglalva a magasabb online internetidő alacsonyabb rezilienciaszinttel jár együtt, illetve a generációs különbségek vizsgálata rámutatott, hogy az Alfa generáció tagjai alacsonyabb rezilienciaszintet mutatnak és nagyobb arányban kerülnek a sérülékeny csoportba, mint a Z generáció képviselői. A nemi hovatartozás vizsgálata alapján a fiúk magasabb rezilienciát mutatnak, míg a lányok felülreprezentáltak a „Törékeny" klaszterben. A szülői háttér vizsgálata megerősítette a szocioökonómiai státusz jelentőségét, mely szerint a magasabb szülői iskolai végzettség magasabb rezilienciaszinttel párosul. Ezek az összefüggések rávilágítanak arra, hogy a lelki ellenálló képesség nemcsak egyéni, hanem társadalmi-demográfiai tényezők által is formált jelenség.

3.4 A kiberbiztonsági tudatosság kérdőív eredményei

A kiberbiztonsági tudatosság összpontszáma és aldimenziói, valamint a demográfiai változók közötti korrelációs elemzés több szignifikáns, gyenge összefüggést tárt fel. A *generációs hovatartozás* a bizalmasság, a felügyelet/birtoklás, a sértetlenség és a hasznosság alskálákkal mutatott szignifikáns kapcsolatot, $r_s = -0.079 - 0.072$ között mozogtak ($p < .001$). A *nem* a bizalmasság, a hitelesség és a hozzáférhetőség dimenziókkal korrelált szignifikánsan, $r_s = 0.061 - 0.071$ tartományban ($p < .001$). Az átlagos napi internethasználati idő a legtöbb alskálával összefüggést mutatott, a legerősebb kapcsolatot a bizalmasság dimenzióval mutatta, $r_s = -0.163,\ p < .001$. Az intézménytípus elsősorban a felügyelet alskálával korrelált, $r_s = 0.098,\ p < .001$. A tanult szakirány a felügyelet/birtoklás, a sértetlenség és a hasznosság dimenziókkal mutatott szignifikáns összefüggést, $r_s = -0.071$ és 0.080 között ($p < .001$). A lakóhely kizárólag a sértetlenség alskálával korrelált gyengén, $r_s = 0.040,\ p<.05$.

3.4.1 A kiberbiztonsági tudatosság és demográfiai változók

Az eredmények alapján azok a fiatalok, akik naponta több időt töltenek online, kevésbé óvatosak személyes adataik védelmében. A magasabb internethasználati idő szinte minden óvatosságra és proaktív védelemre utaló kérdéssel gyenge, de szignifikáns negatív kapcsolatot mutat. Ez különösen igaz az elérhetőségek megosztása ($r_s = -0.152,\ p < .001$), az ismeretlen személyektől érkező e-mailek megbízhatósága ($r_s = -0.104,\ p < .001$), és a letöltött fájlok vírusírtóval való ellenőrzése ($r_s = -0.104,\ p < .001$) területein, valamint az összesített CSCH pontszám és az internethasználati idő között is szignifikáns, negatív kapcsolat áll fenn ($r_s = -0.080,\ p < .001$), jelezve, hogy **a több online töltött idő általánosan alacsonyabb kiberbiztonsági tudatossággal jár együtt**. A hosszabb online jelenlét egy bizonyos mértékű kockázati érzéketlenséghez vezethet.

Az egyutas varianciaanalízis **szignifikáns különbségeket mutatott a napi átlagos internethasználati csoportok között a teljes kiberbiztonsági tudatosságban**, $F(4, 3270) = 5.23$, $p < .001$. A Tukey HSD post-hoc teszt szerint a napi 7+ órát internetező csoport szignifikánsan alacsonyabb tudatossági pontszámmal rendelkezett ($M = 93.92$) a kevesebbet használó csoportokhoz képest ($M = 96.28–97.54$). A hasznosság alskálán fordított mintázat jelentkezett ($p < .001$), a napi 0-1 órát internetezők mutatták a legalacsonyabb pontszámot ($M = 10.52$), szignifikánsan elmaradva a többi csoporttól. Az eredmény talán nem meglepő, mivel a kevésbé aktív internethasználók ritkábban

használják a kibertér szolgáltatásait információkezelésre, problémamegoldásra és közösségi média alkalmazásokra.

Az egyes tanulmányi területek vizsgálata alapján a természettudományi és műszaki szakirányokon tanuló diákok tudatosabb online viselkedést mutattak. Ezek a diákok gyakrabban használnak technikai védelmi funkciókat, mint a telefonos megerősítés *($r_s = 0.103,\ p < .001$)*, hatékonyabban szűrik az adathalász kísérleteket *($r_s = 0.111,\ p < .001$)*, és gyakrabban használják ki a digitális platformok által nyújtott problémamegoldás lehetőségeit *($r_s = .099,\ p < .001$)*. Ugyanakkor reálisabban értékelték adataik sebezhetőségét, kevésbé bíznak az online információk hitelességégen *($r_s = - 0.135,\ p < ,001$).*

Az egyutas ANOVA szignifikáns különbségeket mutatott a szülők iskolai végzettsége alapján képzett csoportok között a teljes kiberbiztonsági tudatosságban, *$F(3,3271) = 4.97,\ p = .002$*. A post-hoc Tukey HSD teszt igazolta ezt a pozitív kapcsolatot, ahol az **általános iskolai végzettségű szülőkkel rendelkező válaszadók szignifikánsan alacsonyabb kiberbiztonsági tudatosság pontszámot értek el** (*$M = 93.02$*) a magasabb iskolai végzettséggel rendelkező szülők gyermekeihez képest. A hitelesség alskálán a magasabb szülői végzettség fokozottabb óvatosságot eredményez az ismeretlen e-mailek, biztonsági tanúsítvány nélküli weboldalak és adathalász támadások kezelésében. A hozzáférhetőség dimenzióban szintén pozitív összefüggés mutatkozott, tehát a diplomás szülők gyermekei gyakrabban alkalmaznak proaktív védelmi intézkedéseket, mint vírusirtó programok és tűzfal. A bizalmasság alskálán is a diplomás szülőkkel rendelkezők mutatták a legmagasabb pontszámot (*$M = 17.09$*), amely szignifikánsan meghaladta a többi csoport értékeit. Ez óvatosságra utal a személyes adatok megosztásában és a privátszféra védelmével kapcsolatban.

3.4.2 Kiberbiztonsági tudatosság generációs különbségei

Az átlagos internetidő és a kiberbiztonság tudatosságra kimutatható negatív kapcsolat az **Alfa generáció** esetében a leginkább hangsúlyos. Az **internethasználat idejének növekedésével szinte minden óvatossági mutatóval erősebb negatív korreláció** figyelhető meg. Különösen a **személyes adatok védelmével** (*$r_s = -0.233,\ p < .001$*), a **jelszavak erősségével** (*$r_s = -0.126,\ p < .001$*) és az **ismeretlen források tudatos kerülésével** (*$r_s = -0.108,\ p = .002$)* kapcsolatban. Emellett, egyedülálló módon ennél a generációnál a több internethasználat szignifikáns pozitív kapcsolatot mutatott azzal a

téves meggyőződéssel, hogy **a kibertérben az adatok tárolása biztonságos** *(r_s = 0.089, p = .010)*. Az összesített **kiberbiztonsági tudatosság pontszámmal való negatív korreláció itt a legerősebb** *(r_s = -0.104, p = .003)*.

A különböző generációs csoportok eltérő megközelítést mutattak a technológiai biztonság adaptációja terén. A **Z generáció képviselői nagyobb arányban alkalmaztak telefonos hitelesítést** fiókjaik védelme érdekében *(r_s = 0.109, p < .001),* ami fejlett technológiai tudatosságukra enged következtetni. Ezzel ellentétben az Alfa generáció tagjai kevésbé reálisan ítélték meg az online adattárolás kockázatait, nagyobb mértékben bíznak abban, hogy a kibertérben tárolt információikhoz illetéktelenek nem férhetnek hozzá *(r_s = - 0.159, p < .001)*.

3.4.3 Nemi eltérések a kiberbiztonsági tudatosság terén

A nemi különbségek vizsgálata a független mintás t-próba eredményei a kiberbiztonsági tudatosság szintjével kapcsolatban nem mutatott szignifikáns különbséget a férfiak és nők között, de az alskálákat vizsgálva a nők szignifikánsan magasabb pontszámot értek el a bizalmasság (M = 17.07; $t(3273)$ = -3.46, p < .001) és a hitelesség (M = 21.28; $t(3271,48)$ = -4.21, p < .001) alskálákon. Ezzel szemben a férfiak a proaktív védelmet mérő hozzáférhetőség alskálán értek el szignifikánsan magasabb pontszámot (M = 14.39; $t(3273)$ = 3.39, p < .001). Ezen eredményeket erősíti a nemek szerinti korrelációs elemzés. A női válaszadók óvatosabban kezelik az ismeretlen eredetű e-maileket *(r_s = 0.104, p < .001).* A férfi résztvevők ezzel szemben következetesebbek az eszközeik tűzfalvédelmének fenntartásában *(r_s = -0.162, p < .001).*

3.4.4 A kiberbiztonsági tudatosság regressziós elemzése

A kiberbiztonsági tudatosság előrejelzésére lineáris regressziós elemzés történt, amelyben prediktorként a generáció, nem, napi internethasználat és szülői iskolázottság változó szerepelt. A modell szignifikáns *F(4, 3270) = 5.69, p < .001*, azonban alacsony magyarázó erővel *(R^2 = .007)* rendelkezik. Egyedül a napi átlagos internethasználat szignifikáns negatív prediktora a kiberbiztonsági tudatosságnak összesített pontszámának *(β = -.076, p < .001),* jelezve, hogy **a több online töltött idő alacsonyabb kiberbiztonsági tudatossággal jár együtt**.

Az egyes alskálákat tekintve, a személyes adatok és privátszféra védelmét mérő bizalmasság alskála lineáris regressziós modellje szignifikáns, *F(3, 3271) = 23.62, p < .001, R^2 = .021*, ahol a női nem magasabb *(β = .065, p < .001),* míg a fokozott

internethasználat alacsonyabb adatvédelmi tudatosságot jelzett előre (β = -0.127, p < .001). Az online források és kommunikáció megbízhatóságának értékelését mérő hitelesség alskála lineáris regressziós modellje szignifikáns, *F(3, 3271) = 9.72, p < .001, R² = .009,* ahol a női nem magasabb *(β = 0.076, p < .001),* míg a fokozott internethasználat alacsonyabb kritikai gondolkodást jelzett előre az ismeretlen e-mail, bizonytalan weboldal és potenciális fenyegetés kezelésében *(β = -0.050, p = .004).* A proaktív technikai védelmi eszközök, mint vírusirtó, tűzfal használatát mérő hozzáférhetőség alskála lineáris regressziós modellje szignifikáns, *F(3,3271) = 12.81, p < .001, R² = .012*, ahol a férfi nem *(β = -0.056, p < .001)* és a kevesebb internethasználat *(β = -0.087, p < .001)* magasabb technikai biztonsági tudatosságot jelzett előre. A kibertér szolgáltatásainak, a közösségi médiának, felhőalkalmazások aktív használatát mérő hasznosság alskála lineáris regressziós modellje szintén szignifikáns, *F(3, 3271) = 8.38, p < .001, R² = .008*, ahol a fokozott internethasználat jelzett előre magasabb online szolgáltatás használatot *(β = .083, p < .001)*.

A napi internethasználat és az online óvatosság közötti kapcsolat vizsgálata ordinális regressziós elemzéssel történt. Az eredmények szerint az online napi átlagos idő szignifikáns prediktora az óvatos magatartásnak a személyes elérhetőségek megosztásával kapcsolatosan. A modell illeszkedésének vizsgálata kimutatta, hogy az internethasználati időt tartalmazó modell szignifikánsan jobban magyarázta az adatokat az alapmodellhez képest, *χ²(1) = 75.51, p < .001.* A paraméterek becslése során **a napi átlagos online töltött idő negatív irányú szignifikáns kapcsolatot mutatott az óvatos viselkedéssel** *(β = -0.126, Wald χ²(1) = 77.27, p < .001).* Az esélyhányados értéke *(OR = 0.88)* alapján minden további óra, amelyet a fiatalok naponta az interneten töltenek, körülbelül 12%-kal csökkenti annak valószínűségét, hogy magasabb szintű óvatosságot tanúsítanak személyes adataik megosztása során. Ez az eredmény alátámasztja azt a feltételezést, hogy **a hosszabb online jelenlét csökkenti a kockázatérzékelést és az elővigyázatosságot a digitális környezetben**.

Az ordinális regresszióelemzés elemzése során az Alfa generáció *(β = -0.461, Wald χ²(1) = 38.80, p < .001*) szignifikáns negatív kapcsolatot mutatott a telefonos megerősítés használatával a Z generációhoz viszonyítva. Az esélyhányados *(OR = 0.63)* alapján **a Z generáció tagjai körülbelül 1,6-szor nagyobb valószínűséggel alkalmazzák rendszeresen a telefonos hitelesítést biztonsági célokra** *(95%-os CI [1.37; 1.83]*). Az eredmények alátámasztják, hogy a generációs hovatartozás szignifikáns prediktora a

proaktív kiberbiztonsági magatartásnak, ahol **a Z generáció fejlettebb technológiai tudatosságot és elővigyázatosságot mutat az Alfa generációhoz képest**.

A multinomiális logisztikus regressziós elemzés szerint az Alfa generáció szignifikánsan magasabb bizalmat mutat az online adatbiztonság iránt, mint a Z generáció. Az Alfa generáció kisebb valószínűséggel kételkedik az online adatbiztonságban, mint a Z generáció, $OR = 0.49,\ p < .001,$ ami azt jelenti, hogy a Z generáció tagja körülbelül kétszer nagyobb valószínűséggel kételkedik az online adatbiztonságban. A likert skálán elérhető többi egyetértési szint esetében is hasonló mintázat mutatkozik, $OR = 0.33$ és 0.55 *között,* $p < .001$. Az eredmény arra utal, hogy az Alfa generáció optimistább attitűddel rendelkezik az online adatvédelemmel kapcsolatban, míg **a Z generáció kritikusabb megítélést és reálisabb kockázatészlelést mutat a digitális biztonság terén**.

Az ordinális regressziós elemzés során a férfiak $(\beta = -0.431,\ Wald\ \chi^2(1) = 35.01,\ p < .001)$ szignifikáns negatív kapcsolatot mutattak az ***ismeretlen e-mailekkel szembeni bizalmatlansággal*** a nőkhöz viszonyítva. Az esélyhányados $(OR = 0.65)$ alapján a nők körülbelül 1.54-szer nagyobb valószínűséggel tanúsítanak óvatos magatartást az ismeretlen eredetű e-mailekkel kapcsolatban $(95\%\text{-os CI } [1.28;\ 1.84])$. Az eredmények alátámasztják, hogy a nem szignifikáns magyarázó változója az online óvatosságnak, ahol **a nők fejlettebb kockázatészlelést és elővigyázatos magatartást mutatnak a férfiakhoz képest az ismeretlen kommunikációs csatornákkal szemben**.

Az ordinális regressziós elemzés során a férfiak $(\beta = .591,\ Wald\ \chi^2(1) = 85.32,\ p < .001)$ szignifikáns pozitív kapcsolatot mutattak ***a tűzfal folyamatos használatával*** a nőkhöz viszonyítva. Az esélyhányados $(OR = 1.81)$ eredménye alapján a férfiak 1.81-szer nagyobb valószínűséggel tartják folyamatosan bekapcsolva a tűzfalat biztonsági elővigyázatosságból $(95\%\text{-os CI } [1.59;\ 2.05])$. Az eredmények alátámasztják, hogy a nem szignifikáns prediktora a proaktív kiberbiztonsági magatartásnak, ahol **a férfiak a technikai védekezés terén mutatnak nagyobb tudatosságot a nőkhöz képest**.

3.5 Moderációs és mediációs elemzések

Az alábbi moderációs és mediációs elemzések azt vizsgálják, hogy a problémás internethasználat, a reziliencia és a kiberbiztonsági tudatosság milyen direkt és indirekt hatásmechanizmusok mentén kapcsolódnak egymáshoz, és ezeket a kapcsolatokat hogyan befolyásolják a demográfiai tényezők.

3.5.1 Problémás internethasználat és kiberbiztonsági tudatosság kapcsolata

A problémás internethasználat és a kiberbiztonsági tudatosság közötti közvetlen kapcsolat vizsgálata során a problémás internethasználat közvetlen hatása a kiberbiztonsági tudatosság szintjére szignifikánsan negatív volt *(b = -0.167, p < 0.01)*. Ez az eredmény alátámasztja, hogy a magasabb problémás internethasználati szint alacsonyabb kiberbiztonsági tudatossággal jár együtt a Z és Alfa generáció körében. A problémás internethasználat nem csupán az internethasználat időbeli túlzott használatát jelenti, hanem a digitális térben megjelenő alacsonyabb tudatossággal és egyben kevésbé felelősségteljes magatartással jár együtt.

3.5.2 A reziliencia mediáló szerepe

A reziliencia mediációs elemzés eredményei alapján a modell szignifikáns direkt hatást mutatott *(b = −0.163, SE = 0.061, p = .008)*, valamint szignifikáns mediáló hatást *(b = −0.327, Boot SE = 0.034, 95% CI [−0.395, −0.263])*. A magasabb problémás internethasználat érték szignifikánsan alacsonyabb reziliencia pontszámmal járt együtt *(b = −0.384, SE = 0.030, p < .001),* míg a reziliencia pozitívan jelezte előre a kiberbiztonsági tudatosságot *(b = 0.851, SE = 0.034, p < .001*), megerősítve a mediációs útvonal jelentőségét.

A problémás internethasználat → reziliencia → kiberbiztonsági tudatosság útvonal szignifikáns indirekt hatást mutatott *(b = −0.329, 95% CI [−0.398, −0.263]).* Ez az eredmény arra utal, hogy a problémás internethasználat csökkenti a rezilienciát, ami következményként alacsonyabb kiberbiztonsági tudatossághoz vezet. A mediáció részleges, mivel a direkt és az indirekt hatás egyaránt szignifikáns maradt. Tehát **a reziliencia kulcsszerepet játszik abban, hogy az egyén mennyire képes tudatosan és felelősségteljesen navigálni a digitális térben.** Az alacsonyabb pszichológiai ellenálló képesség gyengíti a kiberbiztonsági kompetenciát, ami magyarázhatja, miért válnak a problémás internethasználók sebezhetőbbé az online veszélyekkel szemben.

A moderációs vizsgálatok (Model 7 és Model 14 esetében) nem találtak szignifikáns generációs moderációt, az indirekt hatás mindkét generációs csoportban szignifikáns volt, de nagyságuk nem különbözött egymástól szignifikánsan. Ez arra enged következtetni, hogy a reziliencia mediáló mechanizmusa hasonló módon működik mindkét generációs csoportban. Ez az eredmény meglepő lehet, tekintve a két generáció eltérő digitális

szocializációját, ugyanakkor alátámasztja, hogy a reziliencia mint pszichológiai védőfaktor univerzális szerepet tölt be, függetlenül a generációs különbségektől.

3.5.3 A napi internethasználati idő moderáló szerepe

A napi átlagos internethasználati idő moderáló hatását vizsgálva a reziliencia és a kiberbiztonsági tudatosság közötti kapcsolatban a moderált mediáció indexe nem bizonyult szignifikánsnak *(index = 0,011; 95% CI [-0,019; 0,039])*. A feltételes indirekt hatások a napi átlagos internethasználati idő különböző értékeinél stabilan fennálltak, azonban az indirekt hatás mértéke nem változott szignifikánsan az internethasználati idő függvényében. A kapott eredmény alapján megállapítható, hogy az internethasználat puszta mennyisége önmagában nem befolyásolja érdemben a reziliencia és a kiberbiztonsági tudatosság közötti kapcsolat erősségét. Más szóval, **nem az számít, hogy valaki mennyi időt tölt online, hanem az, hogy milyen minőségű a használat és milyen pszichológiai erőforrásokkal rendelkezik a felhasználó.**

3.5.4 A nem moderáló szerepe a mediációs modellben

A *nem* moderáló szerepét két modell (PROCESS Model 7 és Model 14) segítségével vizsgáltam. Az elemzés eredményei alapján a nem szignifikánsan moderálta a reziliencia és a kiberbiztonsági tudatosság közötti kapcsolatot *(b = −0.190, SE = 0.068, p = .005).* Mindkét nem esetében a direkt hatás pozitív volt, azonban erősebb összefüggés mutatkozott a férfi válaszadóknál *(b = 0.960, 95% CI [0.866, 1.054])*, mint a női válaszadóknál *(b = 0.770, 95% CI [0.675, 0.866])*.

Az indirekt hatás mindkét nem esetében szignifikáns volt, de nagyobb mértékű a férfiaknál *(b = −0.369)*, mint a nőknél *(b = −0.296)*. Az indirekt hatások különbsége szignifikánsnak bizonyult *(index = 0.073, 95% CI [0.010, 0.138])*, ami megerősíti a moderált mediáció jelenlétét ezen az útvonalon.

Ezzel szemben a *nemi hovatartozás* nem moderálta szignifikánsan a problémás internethasználat és a reziliencia közötti kapcsolatot *(b = 0.065, SE = 0.061, p = .286),* a problémás internethasználat rezilienciára gyakorolt negatív hatása mindkét nem esetében hasonló mértékű volt. Összességében tehát a **nem csak a reziliencia → kiberbiztonsági tudatosság útvonalon fejtett ki moderáló hatást, ahol a reziliencia védő szerepe erősebb volt a férfi válaszadóknál.** Ez a mintázat felveti, hogy a kiberbiztonsági kompetenciák fejlesztésében a reziliencia erősítése különösen hatékony lehet a férfi

válaszadók számára, míg a nőknél más tényezők is szerepet játszhatnak a kiberbiztonsági tudatosság alakulásában.

Kvantitatív eredmények összegzése

Jelen fejezet a problémás internethasználat, a reziliencia és a kiberbiztonsági tudatosság empirikus vizsgálatának eredményeit mutatta be a Z és Alfa generáció körében. Az eredmények megerősítették, hogy **a három jelenség között szoros és összetett kapcsolatrendszer áll fenn**. A leíró statisztikai elemzések és a megbízhatósági mutatók alátámasztották a mérőeszközök alkalmasságát, míg a korrelációs és regressziós elemzések feltárták a változók közötti összefüggéseket.

Generációs összehasonlítás alapján az Alfa generációra jellemző a magasabb kontrollzavar, míg a Z generáció esetében az elhanyagolás és a problémás internethasználat magasabb szintje figyelhető meg. A nemek közötti különbségek vizsgálata ellentmondásos eredményeket mutat. Míg korábbi kutatások a férfiaknál magasabb problémás internethasználati szintet találtak [81], [82], ezen belül a férfiak az elhanyagolás, míg a nők a kontrollzavar dimenzióban érnek el magasabb pontszámot [135]. Jelen vizsgálatban **a Z generációs nők nagyobb valószínűséggel tartoznak a problémás vagy súlyos internethasználati kategóriába, különösen a kontrollzavar és elhanyagolás dimenziót érintően**. A vizsgált női populáció így különösen a viselkedésszabályozási nehézségek és tevékenységek elhanyagolása terén mutat magasabb problémás internethasználati szintet. Korábbi eredményekkel [81] összhangban a **napi 5 óránál hosszabb online jelenlét szignifikánsan növeli a problémás internethasználat, különösen az elhanyagolás kialakulásának kockázatát, mely az Alfa generáció esetében hangsúlyosabb**. Ez összhangban áll a szakirodalommal, amely a túlzott online jelenlét és az alvásproblémák közötti negatív kapcsolatot igazolja serdülőknél [150], [151].

Az eredmények alapján a **Z generáció szignifikánsan magasabb reziliencia-pontszámokkal rendelkezik.** A szakirodalomban ezt a generációt mentálisan törékenynek írja le az idősebb generációkhoz képest [77]. Az online térben szerzett tapasztalatok révén különféle megküzdési stratégiákat alkalmaznak, ami az Alfa generációhoz viszonyítva magasabb rezilienciában mutatkozik meg. **A fiúk magasabb reziliencia pontszámot értek el**. Összhangban a szakirodalommal, ahol a serdülő lányok körében magasabb szorongás és depresszió jellemző [152], ami alacsonyabb

rezilienciával jár együtt [153]. Ennek oka lehet a szocializációs különbségek, eltérő megküzdési stílusok és társadalmi elvárások.

A válaszadók **magas kiberbiztonsági tudatosságról számoltak be különösen jelszókezelés, adatvédelem és forrásellenőrzés terén.** Tudatában vannak az adatmegosztás kockázatainak, azonban a **proaktív védelmi intézkedések (vírusellenőrzés, fájlvizsgálat) alacsonyabb értékeket** mutattak, jelezve a **passzív stratégiák dominanciáját**. Ez összhangban áll azzal, hogy a fiatalok önbizalma gyakran meghaladja tényleges tudásukat [154], [155].

Az internethasználat intenzitása negatívan korrelál a kiberbiztonsági tudatossággal, **a legaktívabb felhasználók (7+ óra/nap) alacsonyabb biztonsági tudatossággal rendelkeztek** [156], [157]. A nők a bizalmasság és hitelesség dimenziókban értek el magasabb értékeket, míg a férfiak proaktívabb technikai védekezéssel jellemezhetők. A szülői iskolázottság pozitív hatása megerősíti a családi szocializáció szerepét a digitális kompetenciák fejlesztésében [158]. Az eredmények alapján a Z generáció tagjai fejlettebb technológiai tudatossággal és elővigyázatossággal, valamint reálisabb kockázatészleléssel rendelkeznek. Ezzel szemben az Alfa generáció esetében a szignifikánsan magasabb online jelenlét minden vizsgált dimenzióban gyengébb kiberbiztonsági mutatókkal társul.

A mediációs vizsgálatok egyértelműen kimutatták, hogy **a reziliencia kulcsszerepet játszik a problémás internethasználat és a kiberbiztonsági tudatosság kapcsolatában, illetve a PIH negatív hatással van a CSC-H-ra**. A generációs és nemi összehasonlítások tekintetében, a generációs hovatartozás nem bizonyult szignifikáns moderátornak, míg a *nem* jelentős különbségeket eredményezett a reziliencia védő mechanizmusának erősségében, ahol a férfiak erősebb moderáló hatást mutattak. Az internethasználati idő mennyisége ezzel szemben nem moderálta a vizsgált kapcsolatokat, ami az internethasználat minőségi aspektusának fontosságára hívja fel a figyelmet.

A kvantitatív eredmények által feltárt összefüggések mélyebb megértéséhez a következő fejezetben a kvalitatív vizsgálat eredményeit mutatom be, amelyek az egyéni tapasztalatok és narratívák szintjén gazdagítják a képet.

4 KVALITATÍV EREDMÉNYEK

A jelen fejezet a kutatás kvalitatív komponensének eredményeit mutatja be, amely a kvantitatív elemzésekben feltárt összefüggések mélyebb, kontextuális megértését szolgálja. A fókuszcsoportos beszélgetések lehetővé tették, hogy a Z és Alfa generáció tagjainak saját hangjával, személyes narratíváikon keresztül közelítsem meg a problémás internethasználat, a reziliencia és a kiberbiztonsági tudatosság jelenségeit. A kvalitatív adatok elemzése tematikus elemzési megközelítéssel történt, amely során a résztvevők narratíváiból felszínre kerülő főbb jelentéstartalmak, mintázatok és témakörök azonosítására kerültek. A fejezet bemutatja a tematikus elemzés során azonosított főbb kategóriákat és azok tartalmi jellemzőit, kitérve a generációk közötti attitűdbeli különbségekre és a *nem* specifikus perspektíváira egyaránt.

4.1 Fókuszcsoportos beszélgetések elemzése

Az induktív tematikus tartalomelemzés során azonosított főbb témakörök és mintázatok generációs és nemi bontásban kerülnek bemutatásra, ahol a százalékos értékek az adott alcsoport elemszámához viszonyított relatív gyakorisággal fejezik ki az egyes kategóriák előfordulását. Mivel a válaszadók több szempontot is megnevezhettek válaszaikban, az alcsoportokon belüli százalékos értékek összege meghaladhatja a 100 százalékot. A Z generációs ($N = 43$) és Alfa generációs ($N = 46$) résztvevők válaszainak összehasonlítása lehetővé teszi a generációk közötti különbségek és hasonlóságok feltárását, míg a nemi bontás (Z generáció $N = 22$ férfi, $N = 21$ nő, Alfa generáció $N = 17$ férfi, $N = 29$ *nő*) további segítséget nyújt az eredmények értelmezéséhez. A kapott kódokat a teljes 17 tételt tartalmazó elemzésre vonatkozóan a 4/A. melléklet táblázata tartalmazza részletes bontásban, kérdésenként, tématerületenként, kódonként generációs és nemi bontásban. A kódokból és kérdések jellegéből felépített tematikus térképet a 4/B. melléklet szemlélteti.

A továbbiakban a kutatás három fő dimenziója a kiberreziliencia konceptuális modelljéhez igazodva, a tudást (Q03, Q12), a viselkedést (Q01, Q05, Q06, Q07) és a pszichológiai hatásokat öleli fel (Q13-Q17), ehhez a közvetlenül kapcsolódó 11 kiválasztott kérdés részletes eredményei kerülnek bemutatásra. A kiberbiztonsági attitűd az ismert online kockázatok feltérképezése (Q03) az alapvető tudásszintet méri, az alkalmazott biztonsági intézkedések (Q05) a proaktív védekezési gyakorlatot, a jelszókezelési stratégiák (Q07) pedig a kritikus biztonsági magatartást vizsgálják, míg a fenyegetés-felismerési képesség (Q12) a tudásalapú kockázatészlelést reprezentálja. A

tudás és viselkedés közötti rés feltárására a biztonságtudatos viselkedés elmaradásának okait (Q06) elemző kérdés szolgál, amely mind elméleti, mind gyakorlati szempontból központi jelentőségű. A problémás internethasználatot az internet-függőség jelzői (Q13) közül az elvonási tünetek, a kompulzív használat indikátoraként az alvás hanyagolása (Q14), valamint a mennyiségi mutatóként a napi használati idő (Q01) jellemzi. A reziliencia, a technikai stresszre adott reakciókon (Q15) keresztül az érzelmi szabályozási képességet, az online kritikára vagy sértésre adott válaszok (Q16) révén a pszichológiai rugalmasságot, valamint a főbb aggodalmak és megküzdési stratégiák (Q17) feltárásával a reziliencia-kapacitást vizsgálja.

4.2 Tudás, kiberbiztonsági tudatosság és tudás-viselkedés rés

4.2.1 Online kockázatok ismerete (Q3)

A válaszadók **online veszélyforrásokkal** kapcsolatos ismeretei közepes szintet mutatnak, amelyek között a leggyakrabban **azonosított kategóriák a pénzügyi csalás** (26%), az **adathalászat** (22%) és a **fiókfeltörések** (33%) voltak. Generációs és nemi bontásban elemezve a Z generációs férfi résztvevők körében a pénzügyi csalások (45%) és az adathalászat (32%) említési aránya emelkedett ki, míg az Alfa generációs fiúk esetében a hackeléssel összefüggésbe hozható fiókfeltörések (41%), valamint a rosszindulatú szoftverek és vírusok kategória (29%) bizonyult a leginkább felismert veszélyforrásnak. A tartalomelemzés során összesen **12 különböző veszélytípus került beazonosításra**, amely a válaszadók heterogén tudásszintjére és veszélyészlelési spektrumának szélességére utal.

A válaszadók említései között az online zaklatás (*N = 6*) és az online bántalmazás (*N = 4*) kategóriák jelentek meg a leggyakrabban, míg a zsarolás (*N = 4*) és a pedofil jelenlét (*N = 3*) mint potenciális veszélyforrások szintén említésre kerültek. A szóhasználat lexikai diverzitását jelző mutatók közül a szókincsdenzitás 0.301-es értéke, valamint a 13.661-es olvashatósági index és a mondatonkénti átlagosan 18.1 szó mérsékelt nyelvi komplexitásra utal. Az online kockázatok, potenciális ismert veszélyforrások szófelhőjét a 10. ábra szemlélteti.

10. ábra A leggyakoribb potenciális online veszélyhelyzetek szófelhője [forrás: saját szerkesztés]

A szótő-gyakorisági elemzés alapján a legdominánsabb fogalmi mezőket a vírus *(N = 22)* és a fiókfeltörés (*N = 22*) technikai veszélykategóriák, a pénzügyi vonatkozások (*N = 20*), valamint a zaklatás (*N = 15*) és a banki műveletek (*N = 13*) képviselték.

A kognitív asszociációs hálózat feltárására irányuló korrelációs elemzés több szignifikáns összefüggést azonosított. Erős pozitív kapcsolat mutatkozott a vírus és a hackelés fogalmai között (*r = 0.916; p < 0.001*), valamint a vírus és a külföldi szereplők közötti asszociációban (*r = 0.916, p < 0.001*). Az online bántalmazás és zaklatás kategóriák szoros fogalmi kapcsolatot mutattak (*r = 0.807, p < 0.005*), ahogyan az ismerős személyek és a zaklatás közötti asszociáció is (*r = 0.807, p < 0.005*). A pénzügyi veszélytípusok terén a telefonhívások és a pénzügyi motívum között közepes erősségű korreláció volt megfigyelhető (*r = 0.723, p = 0.018*). *„Lehet, hogy ingyenes dolgot csinálsz vagy akkor vagy feltörnek és pénzt húznak le”#17 Alfa fiú*

Szoros asszociáció figyelhető meg a linkekhez kapcsolódó veszélyészlelés (*r = 0.864, p < 0.001*), valamint az adatlopás és fiókfeltörés között (*r = 0.887, p < 0.001*). *„Hát ugye a hackerektől való veszély, feltörnek valamit”#37 lány Alfa*, *„az Instagram küld neked egy linket…a link pedig, amivel neki is feltörték a fiókját”#44 lány Z.* Egyedüli negatív korrelációként az emberi tényező és a fiókfeltörés közötti kapcsolat jelent meg *(r = - 0.790, p=0.006)*, amely arra utalhat, hogy a válaszadók a feltörést inkább technikai, mintsem szociális aspektusként értelmezik.

4.2.2 Fenyegetés-felismerési képesség (Q12)

A hamis weboldalak és adathalász e-mailek felismerésére irányuló kérdéskörben a válaszadók különböző stratégiákat alkalmaznak, amelyek hatékonyságában és gyakorisági előfordulásában jelentős eltérések mutatkoznak. A kutatási eredmények alapján a leggyakrabban alkalmazott felismerési módszer a vizuális és tartalmi jellemzők azonosítása, amelyet a válaszadók 54%-a jelölt meg (*kiemelkedő a Z generáció 67%-os eredménye, ezen belül is a nők 71%-os értéke*). Ebbe a kategóriába tartoznak a nyelvtani hibák, helyesírási pontatlanságok, valamint a professzionális megjelenéstől eltérő designelemek felismerése.

A második leggyakoribb stratégiaként a gyanús URL-ek és adathalász, illetve hamis e-mail címek azonosítása jelent meg, amelyet a válaszadók 44%-a alkalmaz, ahol az Alfa generáció férfi tagjai képviselik a legnagyobb arányt (65%). Ez a megközelítés már technikai szempontból pontosabb észlelést igényel, mivel a küldő címének vagy a weblap URL felépítésének kritikus értékelését feltételezi. Ezzel szemben a technikai védelmi jelzésekre való támaszkodás, mint például a HTTPS protokoll hiányának észlelése vagy a vírusirtó program által generált figyelmeztetések figyelembevétele, már lényegesen alacsonyabb arányban, csupán a válaszadók 15%-ánál jelenik meg, különösen gyenge arányban az Alfa generáción belül a nőknél (3%), aktív felismerési stratégiaként. Ez arra utal, hogy a technikai biztonsági jelzések tudatosítása és értelmezése még mindig nem képezi szerves részét a felhasználói kompetenciák többségének.

Különösen aggasztó azonban, hogy a válaszadók 11%-a, Alfa generáción belül a nők 21%-a, egyértelműen jelezte bizonytalanságát, és őszintén bevallotta, hogy nem képes felismerni az online fenyegetéseket. Ez az adat, a korábban bemutatott, egyébként is korlátozott felismerési képességekkel összevetve, jelentős hiányosságokra mutat rá a digitális kompetenciák terén. A válaszadók több mint egytizede (Alfa generációs nők ötöde) tehát nemcsak részlegesen, hanem **teljes mértékben kiszolgáltatott helyzetben van az online fenyegetésekkel szemben, ami komoly sebezhetőséget jelent** a digitális térben való biztonságos navigálás szempontjából.

4.3 Viselkedés, biztonsági gyakorlatok és magatartásminták

4.3.1 Internethasználati idő (Q1)

A kutatási eredmények alapján a válaszadók 54%-a magas használati kategóriába (6+ óra) sorolható hétvégén, míg hétköznap a használat jellemzően a közepes intenzitású

kategóriába (3-6 óra) esik, amely a válaszadók 47%-ára jellemző. Generációs szempontból vizsgálva a Z generáció mutatja a legmagasabb használati értékeket hétköznap és hétvégén is. A válaszadók 58%-a tartozik a magas kategóriába hétköznap, míg hétvégén ez az arány 72%-ra emelkedik. *„Hát szerintem egy napi 8-10 órát simán fent vagyok a neten.” #49 Z fiú* A nemi különbségek tovább árnyalják ezt a képet, mivel a fiúk körében ez az intenzitás még hangsúlyosabb, ahol a hétköznapi magas használat 77%-ot, a hétvégi pedig 82%-ot ér el.

Az eszközhasználat tekintetében a telefon tölti be az elsődleges szerepet. A telefon és a hétvégente kifejezések között szignifikáns pozitív, erős korreláció van ($r = 0.835$, $p = 0.002$), amely a hétköznapi használat esetében is fennáll, bár valamivel gyengébb ($r = 0.709$, $p = 0.022$). Ezek az értékek megerősítik, hogy a mobiltelefon mint elsődleges eszköz központi szerepet tölt be az internethasználati gyakorlatban. A szociális dimenzió jelentőségét a barátaimmal és otthon kifejezések közötti erős pozitív szignifikáns kapcsolat ($r = 0.829$, $p = 0.003$) hangsúlyozza. Ez az összefüggés az **online szocializáció kiemelkedő szerepére** mutat rá, amely a Z és Alfa generáció életében meghatározó. Az adatok elemzése alapján elmondható, hogy az internethasználat jelentős része a társas kapcsolatok fenntartásához és az online közösségi térben való jelenléthez kapcsolódik.

A mintában erőteljes tendencia mutatkozik a hétvégi, mobiltelefon-központú, tudatos és intenzív internethasználat felé. A Z generáció képviseli a legmagasabb használati időt, különösen a fiúk körében, míg a mobiltelefon nemcsak mint eszköz, hanem mint a szociális interakciók elsődleges csatornája is kulcsfontosságú szerepet tölt be. Ezek az eredmények megerősítik, hogy **az internethasználat mennyiségi és minőségi jellemzői szorosan összefonódnak a generációs sajátosságokkal, a nemi különbségekkel, valamint a szocializációs mintázatokkal.**

4.3.2 Jelszókezelés, mint kritikus biztonsági gyakorlat (Q7)

A **jelszókezelési gyakorlatokra vonatkozó eredmények a digitális biztonság terén jelentős hiányosságokat tárnak fel.** A válaszadók jelszóhasználati szokásai a jelszó felépítése és a memorizálási szokások mentén kerültek elemzésre.

A jelszóerősség tekintetében a férfi válaszadók 35%-a egyszerű, könnyen megjegyezhető jelszavakat alkalmaz, ami az Alfa generációs férfi (41%) és a Z generációs férfi (45%) egyaránt magas arányt mutat. Erős, vegyes karaktereket tartalmazó jelszót csupán a válaszadók 31%-a használ, amely arány a Z generációs férfiaknál a legmagasabb (41%),

legalacsonyabb az Alfa generációs fiúk esetében (24%). Aggasztó, hogy a személyes adatokhoz kötődő jelszavak használata 30%-os, amely különösen a nők körében emelkedik ki mindkét generáció esetén (Alfa generáció 38%, Z generáció 43%). *„Nem bonyolult egyik sem, igazából az állataimnak a neve.” #19 Alfa lány*

A jelszóváltoztatási gyakorlat terén a válaszadók 55%-a jelzi, hogy különböző jelszavakat alkalmaz fiókjaihoz (*Z generációs nőknél a legmagasabb 81%*), addig 37% vallotta be, hogy ugyanazt a jelszót használja minden fiókjához (*Alfa generációs nőknél 52%*). *„Hát nekem is egy jelszavam van mindenhova. Hát egy jelszó és azt megjegyzem, mert mindenhol ugyanaz.” #28 Alfa fiú*

A memorizálási stratégiák tekintetében a fejben történő megjegyzés dominál (53%), amely különösen a férfiak körében hangsúlyos (Alfa generáció férfi 65%, Z generáció férfi 82%). A papíralapú tárolás 31%-os előfordulással a második leggyakoribb módszer, amely az Alfa generációban nemeként kiegyensúlyozott (34-35%), de a Z generációs nők körében kimagasló 43%, a férfiakhoz képest (14%). Különösen alacsony a technológiai megoldások, mint a jelszókezelők, jelszógenerátorok alkalmazása, amely összesen 11%-ot tesz ki, bár a Z generációban ez magasabb (19%), viszont az Alfa generáción belül a fiúk 0%-ban jelölték. Az Alfa generációs válaszadók 6%-a szülői/felnőtt segítségre támaszkodik a jelszókezelésben. *„Apukámnak minden jelszó felvan írva noteszébe és az enyémek is oda vannak beírva. Ő őrzi nekem.” #12 Alfa fiú*

Az eredmények összességében arra mutatnak rá, hogy **a biztonságos jelszókezelési gyakorlatok, az erős, változatos jelszavak használata és a jelszókezelő alkalmazások alkalmazása még mindig nem terjedtek el széles körben, különösen az Alfa generáció körében**, ami jelentős biztonsági kockázatot jelent.

4.3.3 Alkalmazott biztonsági intézkedések (Q5)

Az alkalmazott védekezési módok eredményei alapján hatalmas a különbség a generációk tekintetében, a kétfaktoros hitelesítés (2FA) használatában a Z generáció 79%-a (férfiak 86%) alkalmazza, addig az Alfa generációban ez mindössze 9%. A vírusirtó használat fordított képet mutat, ahol az Alfa generáció 50%-a (férfiak 65%) használ védelmet, szemben a Z generáció 14%-ával (nők 19%, férfiak csupán 9%).

A biometrikus azonosítás a Z generációra jellemzőbb (21%), különösen a férfiaknál (27%). Az adatkorlátozás és privát beállítások terén az Alfa generáció aktívabb (28%), főként a nők (34%), míg a Z generációban ez alacsonyabb, 16%-os arányban van jelen

(férfiak csupán 5%). A gyanús tartalmak kerülése szintén az Alfa generációra jellemzőbb (30%, férfiak 41%). Érdekes eredmény, hogy a szülő kontroll, korlátozás nagyobb arányban az Alfa generáción belül a lányoknál jelenik meg, ahol 17% -os értéket mutat, míg a fiúk esetében ez 0%. A válaszok vizuális megjelenítését az 11. ábra mutatja be.

11. ábra Az alkalmazott biztonsági intézkedések szófelhője [forrás: saját szerkesztés]

Az eredmények erős pozitív korrelációkat tárnak fel a biztonsági intézkedések alkalmazása és az eszközhasználat között. A kétlépcsős hitelesítés használata erős, szignifikáns pozitív összefüggést mutat mind az általános alkalmazással *($r = 0.932$, $p < 0.001$)*, mind a telefonos eszközhasználattal *($r = 0.921$, $p < 0.001$),* ami arra utal, hogy a 2FA elsődlegesen telefon használatakor, ami a leginkább használt eszköz valósul meg.

A privát beállítások használata szignifikáns kapcsolatot mutat a biztonságos jelzővel *($r = 0.772$, $p < 0.01$)*, valamint erős összefüggést az Instagramon való jelenléttel *($r = 0.883$, $p < 0.001$)* és gyengébb, de még mindig szignifikáns kapcsolatot a Facebookon való használattal *($r = 0.707$, $p = 0{,}022$)*. Ez azt jelzi, hogy a közösségi média platformokon a privát profilbeállítások tudatos biztonsági stratégiát képviselnek.

A biometrikus azonosítás laptop környezetben való használata közepes erősségű pozitív korrelációt mutat az ujjlenyomat-használattal *($r = 0.726$, $p = 0.017$),* ami az ujjlenyomat-technológia fokozatos terjedését jelzi a számítógépes eszközökön is.

Az ismert, de nem használt módszerek eredményei alapján, a VPN ismerete elsősorban a Z generációs férfiaknál jelenik meg (14%), de alkalmazása mindkét generációban alacsony (6%). A jelszókezelők ismerete, de használatának mellőzése minimális (3%), főként az Alfa férfiakra (6%) jellemző.

A válaszadók 18%-a nem tud konkrét védekezési módot megnevezni vagy egyáltalán nem használ védelmet, amely arány generációtól és nemtől függetlenül magas (Alfa generáció 20%, Z generáció 16%).

4.3.4 Tudás és viselkedés közötti rés (Q6)

Az adatok egyértelműen rámutatnak a tudás és a tényleges biztonságtudatos viselkedés közötti eltérésre. A válaszadók egynegyede (25%) állította, hogy soha nem tér el a biztonsági szabályoktól (*kivéve a Z generációs férfiak 0%*), a többség azonosította is azokat a helyzeteket, amikor a tudása ellenére mégsem cselekszik biztonságosan. A válaszadók többsége ugyan tisztában van a biztonságos internethasználat alapelveivel, azonban a szabályok tényleges betartása és a mindennapokban alkalmazott gyakorlat között jelentős eltérés mutatkozik.

Ennek legfőbb okai a figyelmen kívül hagyás kategória (27%), az adatvédelmi tájékoztatók elolvasás nélküli elfogadása, a kényelem és lustaság (15%), valamint a kíváncsiság (15%) voltak. A biztonsági előírások figyelmen kívül hagyása különösen a Z generációs férfiaknál hangsúlyos, ahol az arány eléri a 36%-ot. *„Például ha el kell fogadni minden sütit ahhoz, hogy el lehessen olvasni valamit, vagy különben fizetni kell. Szóval én inkább elfogadom a sütiket.” #84 Z fiú* Emellett a pénzügyi előnyök (11%) és a közösségi nyomás (7%) is hozzájárul a szabályok megsértéséhez. *„A Snapchatet használom, de abban nem bízok, de ennek ellenére használom a barátok miatt, mert őket ott érem el” #33 Alfa lány*

A szabályszegések leggyakoribb tevékenységi területei az illegális tartalmak fogyasztása (17%) és az online játékokhoz kapcsolódó tevékenységek (15%). *„Általában le szoktam szedni egy oldalról…le is töltöm őket, a filmek érdekelnek, szóval ott abszolút nem foglalkozom a biztonsággal.” #38 Alfa lány*

Az online vásárlás során tanúsított biztonsági ellenőrzés hiánya elsősorban a Z generációs női válaszadóknál jelentkezik nagyobb arányban (33%), míg az online játékokhoz köthető biztonsági kockázatvállalás inkább a férfi válaszadókra jellemző, különösen az Alfa generációban (24%). **A puszta tudás egyértelműen nem elegendő a biztonságos online viselkedés garantálásához, hiszen a motivációs és pszichológiai tényezők kulcsszerepet játszanak a viselkedési hézag kialakulásában.**

Összességében a „Tudás” dimenzió eredményei azt mutatják, hogy **a felhasználók alapvető szinten tisztában vannak az online kockázatokkal, különösen azokkal,**

amelyek közvetlen károkat okozhatnak. Ugyanakkor a komplexebb fenyegetések ismeretében, felismerésében hiányosságaik vannak. Generációs különbségeket tekintve, a Z generáció szabályszegése inkább a kényelem miatt, kíváncsiságból ered és figyelmetlenségi okból történik. A női válaszadók jellemzőbb inkább a közösségi nyomás és a kíváncsiság motiválta kockázatvállalás, míg a férfiak esetében a kényelem és a tudatos kockázatvállalás dominál. Tehát a digitális biztonsági ismeretek önmagukban nem elégségesek a biztonságos online magatartás kialakításához. Azaz **meglévő tudás nem garantálja a proaktív biztonsági viselkedést**, ami jelentős „*knowledge – behaviour gap*" (tudás – viselkedés rést) eredményez, elsősorban a kényelem, a kíváncsiság, közösségi nyomás és a figyelmetlenség miatt.

4.4 Pszichológiai hatások, problémás internethasználat és reziliencia

4.4.1 Internetfüggőség jelzők, mint elvonási tünetek (Q13)

Az internetmegvonásra adott válaszok túlnyomórészt negatív érzelmi reakciókat, függőségi jeleket mutatnak a vizsgált populációban. A résztvevők közel fele (48–51%) azonnali frusztrációról, idegességről számol be, ami az érzelmi függés jelenlétére utal, túlmutatva egy egyszerű kényelmetlenség érzésen. *„Úristen. Ne. Hát én kiugrok a vonat elé…ez a legnagyobb rémálmom." #1 Alfa lány* Fizikai elvonási tünetek, mint remegés, pánik érzése ritkább, de kimutathatók (9-12%), különösen hangsúlyos a Z generáción belül a nőknél (19%). *„egy hétig? Remegek... Te jó ég! Alapesetben én szerintem megőrülnék, tehát én nem bírnám ki, mert tényleg annyira a mindennapjaim része sajnos." #53 Z lány* A kimaradástól való félelem (FOMO) főként a Z generáción belül a férfiaknál erős (36%), míg a kommunikáció esetleges hiánya a Z generáción belül a nőkre jellemző nagyobb mértékben (57%%). *„Hát az arcomra kiült ez az érzés. Hát a világ végét érezném leginkább, nem jutok hozzá minden információhoz, meg nem nézhetem meg az Instagramomat." #64 Z lány* A rutinok zavara szintén magas arányban jelent meg, főleg nőknél Z generáción belül (62%), ami a mindennapi feladatokhoz köthető akadályoztatás esetén került említésre. *„Hát nyilván az ijesztő lenne, hogy mondjuk egy térképet nem tudsz használni, tehát a megszokott dolgaidat meg kéne változtatni…" #44 Z lány „Hát én biztosan azt érezném, hogy meg van kötve a kezem, hogy az online ügyintézés és a kapcsolattartás területén" #56 Z lány*

Pozitív érzelmi reakciók az internetmegvonásra kisebb mértékben jelentkeztek. A felszabadulás és digitális detox érzése inkább Z generáción belül a férfiaknál (27%) fordult elő, míg a kiesett online tevékenységek offline tevékenységekkel való

helyettesítése főként az Alfa generáción belül a férfiakra (35%) jellemző nagyobb arányban. *„Jól van, kicsit sem lennék úgy búslakodva. Mert igazából tudok a családommal játszani.” #3 Alfa lány* Az alkalmazkodó attitűd ugyan kisebb mértékben (11-16%) a reziliens válaszok irányába mutatva, azt jelzi, hogy egyes csoportok képesek tudatosan kezelni az internet esetleges hiányát.

Az **internetmegvonás leginkább a Z generáció esetén vált ki erős negatív érzelmi reakciókat és függőségi jeleket**, főként **a nők csoportjában**, akiknél gyakoribb a frusztráció, pánik, a fokozódó kommunikációs hiányérzet és a mindennapi rutinok elvégzésében érzett kellemetlen érzés, zavar. A Z generációs **férfiaknál** inkább a **kimaradástól való félelem (FOMO) és a felszabadulás kettőssége** jelenik meg. Az Alfa generáció tagjai enyhébb érzelmi függést mutatnak, a férfiaknál jellemzőbb az offline tevékenységek bevonása a szabadidős tevékenységek körébe. Összességében **a nők érzelmileg érzékenyebben, a férfiak adaptívabban viszonyulnak az internet hiányához**.

4.4.2 Alvásidő feláldozása, mint kompulzív használat (Q14)

Az alváshiány, az alvásidő feláldozása az online tevékenységek miatt széles körű és rendszeres probléma a résztvevők körében (Alfa generáció 52%, Z generáció 70%). Különösen nagy arányban van jelen a Z generáción belül a nőknél (76%). *„akkor nem alszok, hanem csak megnézek pár videót, de abból nem pár videó lesz, hanem rengeteg. Tehát nagyon nagyon be tud szippantani.” #43 Z lány* A tudatos önkontroll szinte csak a Z generáción belül a férfiaknál jelent meg a válaszok elemzése során (18%), ami a vizsgált populációban alacsony önszabályozási képességre utal.

Az éjszakai domináns tevékenység a passzív tartalomfogyasztás (55%), youtube videók, TikTok, instagram pörgetésben nyilvánul meg, ami könnyű „időcsapdát” jelent. Mindegyik generációt közel egyformán érinti, az Alfa generáción belül inkább a fiúkat (65%), a Z generáción belül inkább a lányokat (62%). *„Hát nekem még rendszeresen van úgy, mert így egyszerűen nem tudom abbahagyni. Csak így pörgetek. És már csak azt veszem észre, hogy ilyen fél egy-egy és akkor csak így rá kell szólnom magamra, hogy tegyem már le, és akkor tudom csak letenni, de egyébként talán nem tudatosan még nem éhezek meg, vagy valami nem zökkent ki valami, akkor nagyon sokáig ott tudok ülni. Beszippant ez az egész. Vagy TikTok vagy Instagram.” #47 Z fiú* Az online játékok (25%) és barátokkal való csevegés (26%) hasonló arányban jelenik meg, inkább a Z generációra

jellemzően. *„Hát én a gép előtt nem veszem észre magamat és csak játszok és játszok mert van kivel és megint van kivel és még egy utolsó kör jobb esetben fél 2-kor ki tudok szállni, de igazából nem szokott belőle megállás lenni.” #61 Z fiú* A játékok a fiúkra (45%), a közösségi élet, chat alkalmazások a lányokra (33%) jellemzőbb. *„Az általában úgy szokott lenni, hogy valakinek írok, hogy nem tudok aludni és általában ő sem, és akkor így nagyon sokáig elbeszélgetjük az időt.” #45 Z lány*

Az okokra, motivációra az érdeklődés, kíváncsiság (17%) és az alvászavar, unalom (15%) az automatikus, reflexszerű használatot jelölték a válaszadók. A szülői kontroll kijátszása vagy hiánya, mint faktor csak az Alfa generáció esetén van jelen (17%), az életkorukból kifolyólag. **Összességében az éjszakai internethasználat mondható, hogy szokássá vált, főként a Z generációs lányoknál, akiknél a közösségi jelenlét, míg a fiúknál a játék és tartalomfogyasztás a legjellemzőbb éjszakai tevékenység.**

4.4.3 Online stresszre adott reakció, mint érzelmi szabályozás (Q15, Q16)

A technikai jellegű problémák, internet sebessége, online tevékenység közben az eszköz lefagyása, szoftverhibák összességében erős negatív érzelmi reakciókat váltanak ki a válaszadók körében (74%). Főként frusztrációt, stresszt, idegességet írnak le (64%), különösen nagy arányban az Alfa generáción belül a lányok (72%). A fiúk, mindkét generációban gyakrabban reagálnak dühös tombolással, ordibálással vagy akár tárgyak rongálásával (Alfa generáció fiú 35%, Z generáció fiú 45%). *„Játékban vesztettem egymás után 5 menetet és földhöz vágtam a telefont.” #32 Alfa lány „Hát játék közbe szoktam felhúzni magamat a mai napig. Hát amúgy kiabálok, de már összetörtem két monitort is.” #74 Z fiú „Hát volt már erre példa, akkor elég ideges voltam. Ilyenkor tombolok, török, zúzok, nehezen kezelem a dühömet.” #78 Z fiú*

Tudatos stresszkezelés csak alacsony mértékben, a Z generáción belül a lányoknál figyelhető meg nagyobb arányban (19%), mint konstruktív megoldáskeresési módszer, önszabályozás. A negatív online visszajelzések érzelmileg, lelkileg erősen érintik a válaszadókat, különösen a lányokat, akiknél gyakoribb a szomorúság, kínos és rossz érzés (Alfa generáció lány 38%, Z generáció lány 43%). *„Hát engem irritál és én mindent túlgondolok, egész este azon agyalok, hogy ki fogja látni ezeket.” #38 Alfa lány*

„Szörnyű érzés, horror érzés. Hogyha egy olyan embertől kapok rossz kommentet vagy megjegyzést vagy bántást, aki így mondjuk nekem fontos vagy hallgatok a véleményére, vagy érdekel a véleménye, akkor attól nagyon rosszul tud esni.” #39 Alfa lány

A fiúk inkább figyelmen kívül hagyják (Alfa generáció fiú 29%, Z generáció fiú 45%). Az Alfa generációra jellemzőbb, hogy akár még konfrontálódnak is, verbálisan visszatámadnak, veszekedéssel reagálnak (fiú 59%). Reziliens, építő jellegű megküzdési stratégia, a kritika elfogadása, valóságtartalom átgondolása ritka, de a Z generáción belül a fiúknál viszonylag magasabb arányban van jelen (32%).

„Ha kritika ér, akkor jöjjön a kritika. Elgondolkozok valahol belül, hogy mennyire jogos vagy mennyire nem, és ha jogos és valóban van mögötte ésszerű tartalom vagy ésszerű érv vagy akármi, amin el lehet gondolkozni, akkor elgondolkozok rajta." #63 Z fiú

A korrelációs eredmények alapján, a zavar és negatív érzés közötti erős, szignifikáns kapcsolat *($r = 0.845$, $p < 0.05$)* arra utal, hogy a zavarba ejtő online helyzetek, a sértő kommentek vagy jogosulatlanul megosztott tartalmak hozzájárulnak az intenzív negatív érzelmi reakciókhoz. A komment és negatív érzés közötti közepesen erős pozitív korreláció *($r = 0.686$, $p = 0.029$)* alapján a negatív visszajelzések, kritikák, illetve online kommentek közvetlenül hozzájárulnak a negatív érzelmi állapot kialakulásához. Ez megerősíti, hogy az online érzelmi sebezhetőség és az önértékelés, mentális jóllét között erős a kapcsolatot.

Az osztálytárs és érdekel kifejezések közötti erős, szignifikáns korreláció *($r = 0.847$, $p = 0.002$)* szerint az online interakciók érzelmi jelentősége fokozott mértékben van jelen, ha az érintett személy a személyes szociális környezetből, az iskolai közösségből, közvetlen közeli baráti körből származik. A társas közeghez való tartozás és az online visszajelzések érzelmi befolyása szorosan összefügg, különösen abban a fejlődési időszakban, amikor az identitás és önértékelés formálódása még intenzíven zajlik.

Összességében a fiatalok érzelmi reakciói intenzívek és impulzívak, de a pszichológiai rugalmasság jelei, főként az önkontroll és tudatos megküzdés formájában azért kezdenek kialakulni.

4.4.4 Online reziliencia, aggodalmak és megküzdési stratégiák (Q17)

A fókuszcsoportos eredményei különböző típusú aggodalmakat és stresszforrásokat azonosítottak a kibertérrel kapcsolatban. Az **online fenyegetések** közül a legnagyobb arányban (79%) az **online zaklatás, bántalmazással, hamis tartalmakkal és a valóság torzulásával kapcsolatos félelmek jelentek** meg, mely különösen az Alfa generáción belül a lányok körében jelentős (86%). A fiatalabb generációba tartozók érzékenyebben reagálnak az online zaklatás és manipulációs tartalmak által keltett fenyegetettségre. *„Sok*

fiú már 14-15 évesen azért hát furcsa dolgokra gondolnak és ők folyton fotózzák a lányoknak a fenekét az iskolába és hát nálam ez kiveri a biztosítékot, nekem nagyon visszataszító, ha egy fiú ezt csinálja." #1 Alfa lány „Az interneten könnyen tudsz bántani másokat és ugye az nem jó dolog. Könnyebben lehet az interneten bántani mást, mint mondjuk a való életben és sokkal gyakoribb is." #10 Alfa lány

Ezzel szemben az **állandó lekövetéssel, megfigyeléssel** és a kamerás, mikrofonos adatgyűjtéssel kapcsolatos aggodalmak a technológiailag tudatosabb Z generációban, ezen belül is különösen a férfiaknál jelent meg nagyobb arányban (41%), szemben a női válaszadókkal (14%). A férfiak inkább technológiai szinten érzékelik a kockázatokat, míg a nők a személyes és szociális fenyegetéseket tartják veszélyesebbnek. *„Én ezzel kapcsolatban azt érzem, hogy állandóan megfigyelve érzem magam, kamerák vannak mindenhova elhelyezve, ettől félek nagyon." #57 Z fiú*

Az **adatbiztonsággal, adatlopással, bankkártyaadatokkal való visszaélésekkel** kapcsolatos aggodalmak a teljes mintában megjelenik (62%), a Z generáción belül a nők körében magasabb arányban (81%). *„Hát itt van ugye ez a jelszó és a fájl ugye, hogy ellopják az adatainkat. Ez is azért szerintem elég frusztráló, hogy bármikor megtörténhet végül is. Nem is kell kifejezett indok rá még egy linkre se kell rákattintani." #53 Z lány* Az Alfa generációnál valamivel kisebb arányban, de ez magyarázható azzal, hogy a fiatalabb Alfa generáció tagjai még nem minden esetben használják az online fizetési szolgáltatásokat.

A mesterséges intelligencia gyors ütemű fejlődése, az **AI és deepfake technológiák fejlődésével kapcsolatos félelmek** kis mértékben jelentek meg (4%), elsősorban a női résztvevőknél (Alfa generáció 7%, Z generáció 10%). A férfi válaszadók esetében egyáltalán nem volt jelen (0%) ez a félelem egyik generációban sem. A társas kapcsolatok és önszabályozás szintjén a leggyakoribb aggodalom a **függőség, túlzott használat és elszigetelődés, kapcsolatok hiánya** volt, amely a teljes minta 51%-át érinti. A nagyobb arányt (64%) a Z generáción belül a férfi válaszadók képviselték, ami a közösségi médiahasználat túlzott használatára, a fiatalabb generáció védelmére és az online kapcsolati kimerülésre utal. *„A telefonomon mindig hangosra állítva, hogy csippan egyet ha jön egy üzenet és mindig meg kell néznem igazából, hogy mi az, mert semmiről nem akarok tényleg lemaradni, muszáj megnéznem." #70 Z lány „Hát én ide rögtön ezt a*

lemaradásról való félelmet mondanám. Ez bennem is megvan. Szerintem ez még amúgy sok másik embernél is ott van." #84 Z fiú

A mentális jólléttel, szorongással és önképpel, önbizalomhiánnyal kapcsolatos aggodalmak főként a Z generációt érintik, nemenként közel azonos arányban (férfi 45%, nő 43%). *„Online igazából egy hamis életet mutatunk az emberek felé. Tehát ha valaki nem figyelmes és nem szemfüles, akkor könnyen bele tud futni abba a hibába, hogy mondjuk önértékelési zavarokkal fog küzdeni, mert azt hiszi, hogy ő rossz ő nem elég jó a társadalomnak. Én is érezem így magam." #63 Z fiú*

A játékhoz köthető érzelmi stressz, szorongás inkább a férfiakra jellemző (Alfa generáció 18%, Z generáció 27%). A félelemre, stresszre adott érzelmi reakciók között a **tehetetlenség, frusztráció és idegesség** dominál (56%), kimagaslóan a Z generációnál (férfi 73%, nő 81%).

Ennél **erősebb érzelmi reakció a pánik, ijedtség és szorongás** a nők körében gyakoribb (Alfa generáció 28%, Z generáció 24%), ami az érzelmi megterhelés és a mentális sebezhetőség magasabb szintjét jelzi az online térhez köthető tevékenységek végzésével kapcsolatban. *„Online bántalmazás okoz szorongást, a csalók, személyazonosságlopások." #8 Alfa lány „Teljesen kivagyok tőle, hogy bármit csinálsz mondjuk a gépeden és előtte ülsz akkor azt felhasználhatják ellened, hogyha levideóznak. Engem is szoktak bántani akár itt a suliban is." #15 Alfa lány „Nekem ez nagyon nagy szorongás okoz a hamis infók. És hogy ugye szerintem a mai világban egy több olyan van, hogy nem tudod eldönteni, hogy mi az igazi és mi a kamu, és hogy így vacillálsz, hogy akkor most kire hallgassak és hogy kire ne. És ez így nagyon nehéz, hogy nem tudom, hogy mi az igazi. Meg, hogy egyre többen függők és hogy ez annyi mindent elvesz így az életből, előbb utóbb internetfüggők leszünk." #27 Alfa lány*

Kvalitatív eredmények összegzése

A fókuszcsoportos beszélgetések a kvantitatív eredmények értelmezését segítették elő, betekintést nyújtva hogyan élik meg a fiatalok az online térben való jelenlétüket, milyen stratégiákat alkalmaznak a digitális kihívások kezelésére, és hogyan értelmezik saját sebezhetőségüket és ellenálló képességüket a kibertérben.

A vizsgálat alapján a fiatal felhasználók online kockázatokkal kapcsolatos tudása, elsősorban **pénzügyi és technikai fenyegetések felismerésére** terjed. Az **internethasználat magas intenzitású, a mobiltelefon elsődleges eszköz** a szociális

interakciók fenntartásában nagy szerepet játszik. A **jelszókezelési és biztonsági gyakorlatokban jelentős hiányosságok mutatkoznak**. A tudás és viselkedés közötti szakadék nagy, amelyet a **kényelem, kíváncsiság és közösségi nyomás** vált ki nagyrészt. Az internetmegvonás gondolata **intenzív negatív érzelmi reakciókat** vált ki. A vizsgált populációra jellemző az alvás feláldozása és a túlzott internethasználati problémák.

A **legnagyobb online aggodalmat a zaklatás, bántalmazás és az adatokkal való visszaélés** jelenti. Generációs és nemi különbségek azonosíthatók a kockázatészlelésben, biztonsági gyakorlatokban és pszichológiai reakciókban. Az eredmények megerősítik, hogy a digitális kompetencia nem jelent automatikusan biztonságos viselkedést, és a digitális tudatosság fejlesztése sokrétű, összetett megközelítést igényel, amely integrálja a tudás, viselkedés és pszichológiai jóllét dimenzióit.

A következő fejezetben a kiberreziliencia faktorainak integrált modellje kerül bemutatásra. Ez az integráció megalapozza a személyes kiberreziliencia skála megalkotását, validálását, valamint a generációs mintázatok és kiberreziliencia profilok azonosítását.

5 A KIBERREZILIENCIA FAKTORAINAK INTEGRÁLT MODELLJE ÉS GENERÁCIÓS MINTÁZATAI

A fejezetben bemutatásra kerül a kutatás módszertani kerete, amely többlépcsős, szekvenciális magyarázó vegyes módszertani megközelítést alkalmaz. A kvantitatív fázis célja a személyes kiberreziliencia skála (PCRS) megalkotása, validálása és a kiberreziliencia profilok azonosítása. A kvalitatív fázis a kvantitatív eredmények, különösen a generációs és nemi különbségek mélyebb megértését szolgálja.

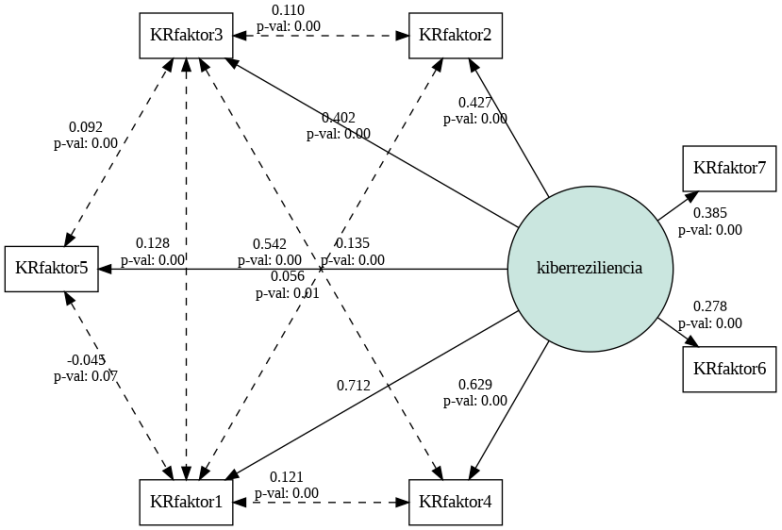
5.1 A személyes kiberreziliencia skála (PCRS) faktorszerkezete

A PCRS skálafejlesztése egy többlépcsős tisztítási folyamaton keresztül valósult meg, amelynek célja egy pszichometriailag robusztus és elméletileg értelmezhető faktorszerkezet kialakítása volt. A kezdeti 41 tételből álló item-készlet belső megbízhatósága kiválónak bizonyult (*Cronbach α = .877*). A megbízhatóság további növelése érdekében az item-analízis első lépéseként két, a skála koherenciájához gyengén illeszkedő tétel került eltávolításra (PIH_01_rev, CSCH12), amellyel a Cronbach-alfa értéke *.883*-ra javult. A fennmaradó 39 tételen elvégzett feltáró faktoranalízis (EFA) egy nyolcfaktoros struktúrát valószínűsített, amely a teljes variancia *51.875%*-át magyarázta. A faktortöltések és a kereszttöltések alapos vizsgálata után törlésre kerültek azok a tételek, amelyek egyik faktoron sem érték el a *>.40*-es minimális faktortöltési küszöböt (RISC01, RISC02, RISC07, RISC10 értékeik *.284 és .390* között mozogtak). Másodszor, eltávolításra került a PIH_06_rev tétel is, amely jelentős kereszttöltést mutatott a 3. és 8 faktorra *(.365, -.380)*, így nem volt egyértelműen hozzárendelhető egyetlen dimenzióhoz sem. Az elemzés következő lépésében a 34 tételes modell faktorstruktúrájának stabilitása került vizsgálatra. Mivel az 1. és 3. faktorok között egy erős korreláció mutatkozott *(r = .531),* ezért a két dimenzió elméleti és empirikus szoros összefüggése miatt egy kényszerített, hétfaktoros megoldás került tesztelésre a 34 tétellel. A modell illeszkedésének további javítása érdekében eltávolításra került további két tétel (CSCH09, PIH_05_rev). A fennmaradó 32 tételre vonatkozóan a Kaiser-Meyer-Olkin (KMO) mutató értéke kiváló, *.896* volt. A Bartlett-féle teszt szintén szignifikánsnak bizonyult ($\chi^2(496) = 29093.680,\ p < .001$), jelezve a változók közötti korrelációk meglétét. A végleges, 32 tételes, hétfaktoros modell a teljes variancia *56.99%*-át magyarázza. A skála teljes belső megbízhatósága kiválónak bizonyult (*Cronbach*

α = .871). A PCRS végleges faktorstruktúrája, az egyes tételek rövidített szövegével, faktorsúlyaival és az alskálák belső megbízhatósági mutatóival a 3/C. melléklet táblázatában került összefoglalásra. Az azonosított 7 faktor elméletileg jól elkülöníthető, és a kiberreziliencia különböző dimenzióit ragadja meg, a proaktív védekezési stratégiáktól a pszichológiai megküzdésen át a digitális jóllétig. A PCRS faktorszerkezete robusztusnak tekinthető, mivel a legtöbb item erősen (*> .50*) töltődik a saját faktorára, és az alskálák többsége jó belső konzisztenciát mutat (*α > .70*). Az alacsonyabb tételszámú faktorok (5, 6, 7) megbízhatósági értékei elfogadhatóak (*α > .60*), de jelzik a skála jövőbeli finomításának lehetséges irányait, esetleg a faktorok új tételekkel való bővítését a megbízhatóság növelése érdekében.

5.2 A PCRS modell faktorszerkezetének megerősítése és validációja

A feltáró faktorelemzése által azonosított 7 faktoros struktúra belső validitásának és általánosíthatóságának tesztelésére másodrendű megerősítő faktoranalízist (CFA) került alkalmazásra. A torzítás elkerülése és a modell robusztusságának ellenőrzése érdekében a teljes mintát véletlenszerűen egy 70%-os feltáró, tanító almintára és egy 30%-os megerősítő, teszt almintára osztottam. A modell egy központi, másodrendű látens faktort, „*kiberreziliencia*” faktort specifikált, amely a 7 elsőrendű faktort foglalja magában, de emellett lehetővé tette specifikus, közvetlen útvonalak modellezését is az elsőrendű faktorok között. A 12. ábra a végleges strukturális modell eredményeit mutatja be a tanító adathalmazon.



12. ábra A Személyes Kiberreziliencia Skála (PCRS) strukturális modellje a tanító adathalmazon, standardizált útvonal-együtthatókkal [forrás: saját szerkesztés]
Megjegyzés: A folytonos nyilak a központi kiberreziliencia faktor hatásait, a szaggatott nyilak az elsőrendű faktorok közötti közvetlen kapcsolatokat jelölik.

A modell illeszkedési mutatói elfogadhatóak, alátámasztva a feltételezett struktúra érvényességét (*CFI = .905, TLI = .895, RMSEA = .043, SRMR = .049*). A központi *kiberreziliencia* faktor, mint egy általános védőfaktor, szignifikánsan és pozitívan jósolta mind a hét aldimenziót. A legerősebb hatást a proaktív adatvédelem faktorra (KRfaktor1; *β = .712*) és a kiberfenyegetés észlelés faktorra (KRfaktor4; *β = .629*) gyakorolta. Gyengébb, de szintén szignifikáns hatás mutatkozott az offline jóllét faktorra (KRfaktor6; *β = .278*), jelezve, hogy az általános reziliencia a kontrollált internethasználattal is összefügg. Az általános faktoron túl a modell több, specifikus kapcsolatot tárt fel az elsőrendű faktorok között. A mentális erő faktor (KRfaktor2) közvetlenül és pozitívan hat az aktív technikai védelemre (KRfaktor3; *β = .110*), a pszichológiai erőforrások elősegítik a konkrét technikai védelmi viselkedések alkalmazását. Hasonlóképpen, a kiberfenyegetés észlelése (KRfaktor4) pozitívan befolyásolja a proaktív adatvédelmet (KRfaktor1; *β = .121*), jelezve, hogy a kockázatok felismerése konkrét adatvédelmi cselekedetekhez vezet.

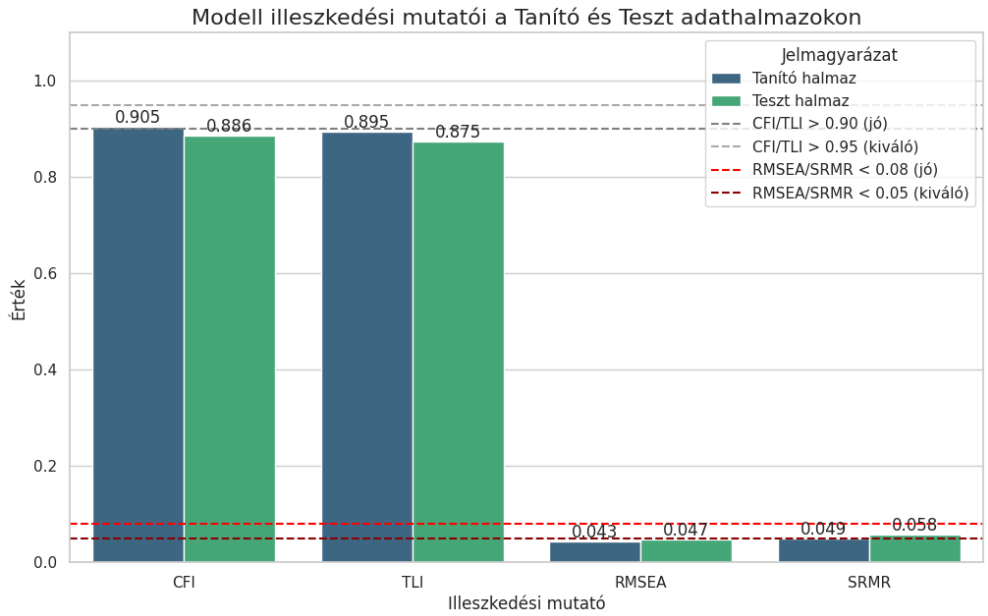
A modell illeszkedési mutatói a tanító adathalmazon a modell elfogadható illeszkedését jelezték (1. táblázat). A chi-négyzet próba szignifikáns *($\chi^2(450) = 2373.07$, $p < .001$),* és a Comparative Fit Index *(CFI = .905)* elérte, míg a Tucker-Lewis Index *(TLI = .895)* megközelítette a .90-es elfogadási küszöböt. A modell hibáját mérő mutatók kiválóak, a *RMSEA = .043 [90% CI: .041, .045]* és a *SRMR = .049* is a jó illeszkedésre utaló határértékek alatt maradtak.

1. táblázat A modell illeszkedési mutatóinak összehasonlítása

Illeszkedési mutató	Tanító halmaz értéke	Teszt halmaz értéke
Chi-négyzet (χ^2)	2373.07	1419.39
Szabadságfok (df)	450	450
p-érték (p)	< .001	< .001
CFI	.905	.886
TLI	.895	.875
RMSEA [90% CI]	.043 [.041, .045]	.047 [.044, .050]
SRMR	.049	.058

Megjegyzés: CFI = Comparative Fit Index; TLI = Tucker–Lewis Index; RMSEA = Root Mean Square Error of Approximation; CI = Konfidenciaintervallum; SRMR = Standardized Root Mean Square Residual. A modelllilleszkedés elfogadott küszöbértékei: CFI és TLI > .90, RMSEA < .08, SRMR < .08

A modell általánosíthatóságának ellenőrzésére a tanító adatokon becsült modell a teszt adathalmazon került validálásra. A 13. ábra szemlélteti az illeszkedési mutatókat.



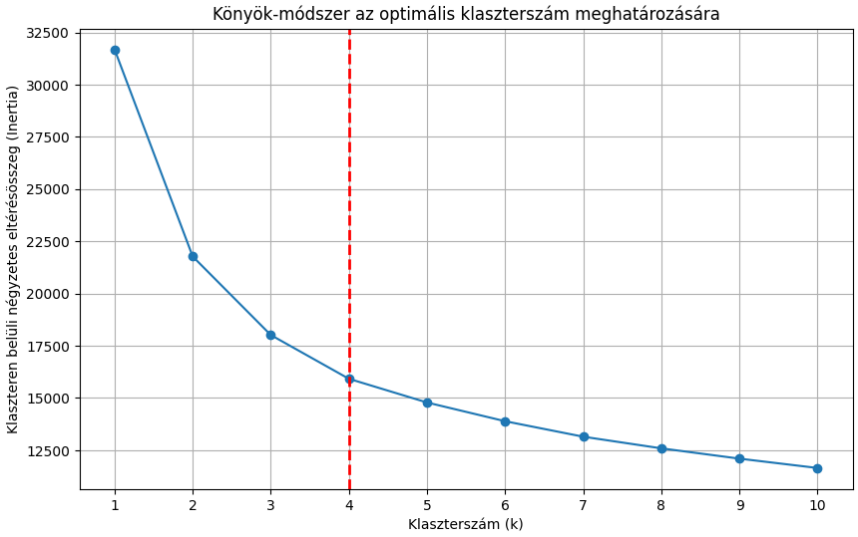
13. ábra A másodrendű kiberreziliencia modell fő illeszkedési mutatóinak összehasonlítása a tanító és a teszt adathalmazokon [forrás: saját szerkesztés]

A CFI (.886) és a TLI (.875) értékei a .90-es küszöb alá csökkentek. Ugyanakkor, ahogy a 13. ábra is kiemeli, a hibamutatók továbbra is az elfogadható tartományon belül vannak *(RMSEA = .047 [90% CI: .044, .050]; SRMR = .058)*, ami arra utal, hogy a modell illeszkedése összességében kielégítőnek tekinthető.

Összefoglalva, a modell a tanító adathalmazon elfogadható illeszkedést mutatott. A keresztvalidáció során feltárt csekély illeszkedésromlás egy enyhe túlilleszkedésre utalhat, azonban a hibamutatók stabilan alacsony szintje azt jelzi, hogy **a modell alapvető struktúrája robusztus és általánosítható.** Az eredmények a PCRS skála hétfaktoros, másodrendű struktúrájának óvatos, de alapvetően megalapozott érvényességét támasztják alá.

5.3 Kiberreziliencia profilok azonosítása

A PCRS segítségével azonosított hét faktor alapján K-középpontú klaszterelemzés került alkalmazásra a kiberreziliencia profil meghatározása céljából. Az elemzésben a hét faktor standardizált Z-pontszáma képezte a bemeneti változót, amely biztosította, hogy minden dimenzió azonos súllyal járuljon hozzá a csoportképzéshez. Az optimális klaszterszám kiválasztásához könyök-módszer került felhasználásra (14. ábra).

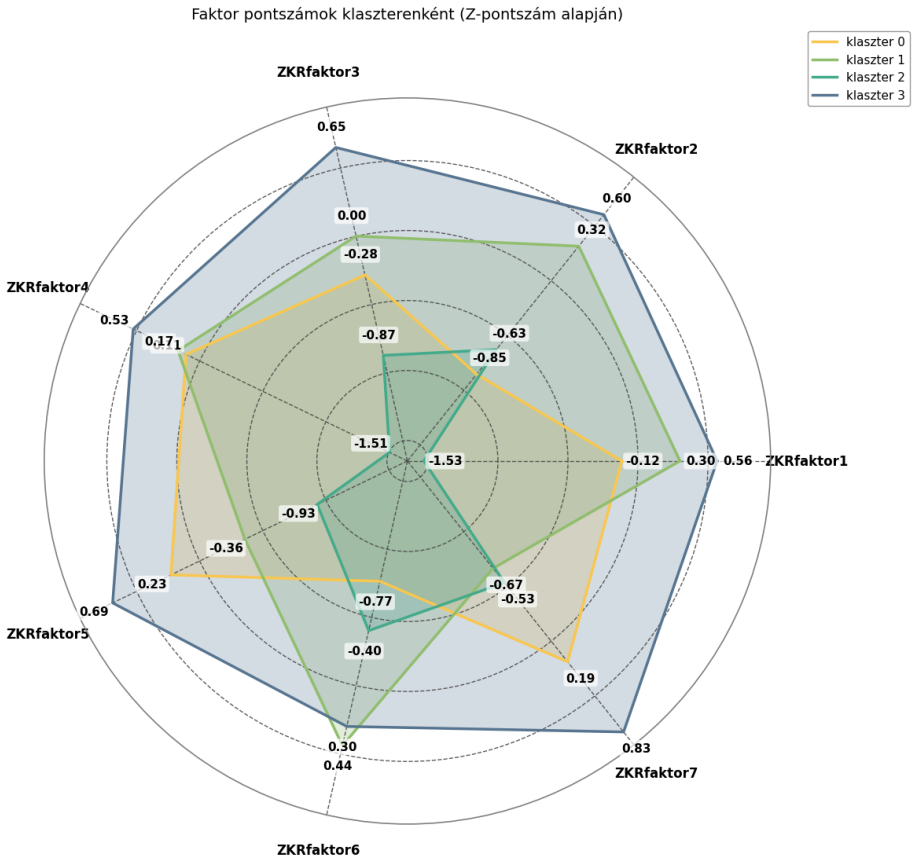


14. ábra Az optimális klaszterszám meghatározása a könyök-módszer segítségével [forrás: saját szerkesztés]

A görbén egyértelmű töréspontok figyelhetők meg *k=2*, k=3 és *k=4* értéknél. Míg a legnagyobb esés a klaszterek számának egyről kettőre növelésével érhető el, a *k=4* pont után a variancia csökkenése jelentősen lelassul, ami azt jelzi, hogy további klaszterek hozzáadása már nem eredményez számottevő javulást a csoportok belső homogenitásában. Az elméleti megfontolások és a fiatalok online viselkedésének feltételezett komplexitása alapján a négyklaszteres megoldás bizonyult a leginkább értelmezhetőnek és informatívnak. Ennek megfelelően a további elemzések során a négyklaszteres modell került alkalmazásra a kiberreziliencia-profilok részletes jellemzésére. A klaszteranalízis eredményeként négy, egymástól elkülönülő kiberreziliencia profil került azonosításra. Az 15. ábra vizualizálja a négy klaszter átlagos Z-pontszámait a hét kiberreziliencia-faktor mentén, míg a 2. táblázat a pontos értékeket foglalja össze.

2. táblázat A négy kiberreziliencia-klaszter faktoronkénti átlagos Z-pontszámai

Klaszter	faktor1	faktor2	faktor3	faktor4	faktor5	faktor6	faktor7
0	*-0.116*	*-0.854*	*-0.283*	0.108	0.228	*-0.765*	0.188
1	0.300	0.316	0.001	0.171	*-0.358*	0.439	*-0.666*
2	*-1.529*	*-0.629*	*-0.873*	*-1.505*	*-0.932*	*-0.404*	*-0.535*
3	0.565	0.604	0.651	0.527	0.690	0.299	0.829



15. ábra A négy kiberreziliencia-profil összehasonlítása a hét faktor mentén az átlagos Z-pontszámok alapján [forrás: saját szerkesztés]

A profilok a kiberreziliencia erősségei és sebezhetőségei alapján a következőképpen jellemezhetők:

0. klaszter - Passzív, mentálisan sérülékeny problémamegoldók *(N = 712, 21.7%)*: Ez a csoport ellentmondásos, mivel a gyakorlati, problémamegoldó képességeik (kiberfenyegetés észlelés *Z = 0.108*, online problémamegoldás *Z = 0.228*) átlagosak, ezt beárnyékolja a rendkívül alacsony mentális erő és önkontroll (*Z = - 0.854*) és offline jóllét (*Z = -0.765*). Ők azok a felhasználók, akik talán felismerik a konkrét veszélyeket, de hiányoznak a pszichológiai erőforrásaik a stresszel való hatékony megküzdéshez, de ők azok, akik bizonyos fokú gyakorlati tudatosságot mutatnak az online kockázatok kezelése terén.

1. klaszter - Óvatos navigálók *(N = 1036, 31.6%):* Ez a csoport egy kiegyensúlyozott, de a digitális rendszerek iránt alacsony bizalommal rendelkező profilt mutat. Átlag feletti pontszámokat értek el a proaktív védelem (*Z = 0.300*) és a mentális erő (*Z = 0.316*) és offline jóllét (*Z = 0.439*) dimenzióiban, ami stabil belső és viselkedésbeli erőforrásokra

utal. Ugyanakkor a bizalom az online adattárolásban (*Z = -0.666*) kifejezetten alacsony, ami defenzív online stratégiákat valószínűsít.

2. klaszter - Magas kockázatú, sérülékenyek *(N = 521, 15.9%)*: Ez a csoport képviseli a legsebezhetőbb profilt, amely alacsony kiberrezilienciát mutat szinte minden vizsgált dimenzióban. Különösen súlyos hiányosságaik vannak a proaktív adat- és hozzáférésvédelem (*Z = -1.529*) és a kiberfenyegetés észlelés (*Z = -1.505*) terén, ami a technikai, pszichológiai és viselkedésbeli védőfaktorok együttes hiányára utal.

3. klaszter - Magas rezilienciájú, proaktív és tudatosak *(N = 1006, 30.7%)*: Ez a csoport a legmagasabb szintű, komplex kiberreziliencia-profillal rendelkezik. Minden faktoron átlag feletti teljesítményt nyújtanak, kiemelkedően magas értékekkel a proaktív védelem (*Z = 0.565*), mentális erő és önkontroll (*Z = 0.604*), kiberfenyegetés észlelés (*Z = 0.527*), offline jóllét (*Z = 0.299*) és online bizalom (*Z = 0.829*). Ez a csoport komplex és erős kiberreziliencia-profil, akik egyszerre rendelkeznek technikai, pszichológiai és viselkedési védőfaktorokkal.

5.4 Generációs és nemi összehasonlítás a kiberreziliencia aspektusából

A kiberreziliencia profilok demográfiai hátterének vizsgálata szignifikáns különbségeket tárt fel mind a generációk, mind a nemek között. A Khi-négyzet próba alapján a profilok eloszlása szignifikánsan eltért a generációk között *($\chi^2(3) = 11.07$, $p = .011$)*, és még markánsabban a nemek között *($\chi^2(3) = 57.64$, $p < .001$)*. **A nők szignifikánsan nagyobb arányban tartoztak a *„passzív, mentálisan sérülékeny problémamegoldók”* (0. klaszter) csoportjába, míg a férfiak felülreprezentáltak voltak a *„magas rezilienciájú, proaktív és tudatosak”* (3. klaszter) csoportjában.**

A kiberreziliencia hét aldimenziójának részletesebb, kétutas varianciaanalízissel (ANOVA) végzett vizsgálata alapján a férfiak szignifikánsan magasabb pontszámot értek el a mentális erő és önkontroll *($F(1,3271) = 49.47$, $p < .001$)*, az aktív technikai védelem *($F(1, 3271) = 10.30$, $p = .001$)* és az offline jóllét *($F(1,3271) = 11.89$, $p < .001$)* terén. Ezzel szemben a nők szignifikánsan magasabb pontszámot értek el a kiberfenyegetés észlelés *($F(1,3271) = 14.36$, $p < .001$)* dimenzióban. Az eredmények alapján elmondható, hogy a férfiak inkább a belső erőforrásaikra és a technikai ismereteikre építenek, míg a nők a külső veszélyek felismerésében erősebbek.

A generáció főhatása szintén több területen is szignifikáns volt. **A Z generáció tagjai magasabb szintű mentális erőt (*p = .005*), offline jóllétet (*p = .007*) és online problémamegoldást *(p < .001)* mutattak.** Ezzel szemben az Alfa generációra volt jellemző a szignifikánsan magasabb online adattárolás bizalma *(p < .001),* ami a digitális rendszerek iránti nagyobb fokú, esetlegesen naivabb bizalmukra utalhat. A két demográfiai változó közötti interakciós hatás egyedül a mentális erő faktor esetében közelítette meg a szignifikancia határát *(p = .063),* jelezve azt a tendenciát, hogy a nemek közötti különbség ezen a téren az idősebb, Z generáció körében hangsúlyosabb.

A kutatási eredmények két alapvetően különböző kiberreziliencia stratégiát tárnak fel a generációk között. A Z generáció hibrid védelmi modellt alkalmaz, amely kiegyensúlyozott mentális állóképességre és tudatos digitális-analóg kettősségre épül, lehetővé téve számukra a rugalmas alkalmazkodást és a digitális fenyegetésekkel szembeni reaktív-adaptív válaszokat, bár körükben jelentős nemi különbségek mutatkoznak a mentális erő tekintetében. Ezzel szemben az Alfa generáció technológiacentrikus paradigmát képvisel, amelyet erős, helyenként naiv bizalom jellemez a digitális ökoszisztémában, és amely ellentmondásos módon sebezhetőséget eredményezhet a túlzott technológiai függőség révén. Míg a Z generáció a rugalmasságban és a különféle megküzdési mechanizmusban keresi a biztonságot, addig az Alfa generáció preventív-technológiai stratégiát követ, túlzott bizalommal a digitális védelmekben és gyengébb offline problémamegoldó kompetenciával, ami digitális incidensek esetén töréspontot eredményez a védelmi rendszerükben és korlátozott helyreállítási képességhez vezet.

5.5 A kiberreziliencia-profilok és különbségek kvalitatív magyarázata

A kvantitatív profilok mélyebb megértése érdekében a fókuszcsoportos interjúk tematikus elemzése került elvégzésre. Az elemzés célja az volt, hogy azok a megélt tapasztalatok, attitűdök és stratégiák feltárásra kerüljenek, amelyek magyarázatot adnak az egyes klaszterek jellegzetes mintázataira.

A **0. klaszter** a kvalitatív adatok alapján **a tudás és cselekvés közötti szakadék, a magas érzelmi reaktivitás és a kontrollvesztés** jegyeit mutatja. A csoport tagjai gyakran **tudatosan írják felül a biztonsági intézkedéseket a kényelem vagy egy azonnali jutalom érdekében.** *“Igazából, ha egy olyat akarok letölteni, amit ugye nem enged*

letölteni, mert van rajta ilyen vírusvédelem, akkor kemény 10 percre kikapcsolom a vírusvédelmet és letöltöm." *#17 Alfa fiú* vagy *"Általában amikor néha nem szoktam figyelni a biztonságra, amikor lusta vagyok." #50 Z fiú* Ezt a profilt a **magas érzelmi reaktivitás** is jellemzi, ami a mentális erő faktoron mért alacsony pontszámukat magyarázza. **A negatív online interakciók mélyen érintik őket, gyakran pánikot vagy erős frusztrációt kiváltva**. *"Hát engem eléggé rosszul érintene egy ilyen dolog... Hát így ilyenkor néha így elkezdek pánikolni." #33 Alfa lány - negatív kommentekre reagálva* vagy *"Játékban vesztettem egymás után 5 menetet és földhöz vágtam a telefont." 32 Alfa lány* Végül, a csoport offline jóllét faktoron mért alacsony pontszáma szoros összefüggésben áll a **digitális viselkedésük feletti csökkent kontroll**al. A válaszokból a lemaradástól való félelem (FOMO), az internet nélküli élet szorongató víziója és a kontrollvesztés rendszeres élménye rajzolódik ki. *„Hát nekem rendszeresen van úgy. Mert így egyszerűen nem tudom abbahagyni. Csak így pörgetek. Beszippant ez az egész." #47 Z fiú - az alvás helyetti internetezésről* és *„Úristen. Ne. Hát én kiugrok a vonat elé... ez a legnagyobb rémálmom." #1 Alfa lány - az internet pár napig történő elérhetetlenségének lehetőségéről.* Ez a profil egy olyan felhasználói csoportot ír le, amelynek **elméleti tudását aláássa az alacsony stressztűrő képessége és a csökkent önszabályozása**.

A legnagyobb elemszámú, **1. klaszter** egy **kiegyensúlyozott, de a digitális rendszerek iránt alapvetően bizalmatlan** profilt mutat. Rezilienciájuk a **személyes felelősségvállalásból, a tudatos szabálykövetésből és a magas szintű érzelmi kontroll**ból táplálkozik. **A biztonság** számukra nem egy adott, hanem egy megteremtendő állapot, amelynek **kulcsa a személyes kontroll**, például a privát fiókok használata. *„Abból a szempontból biztonságban érzem magam, hogy minden olyan oldalon, ahol fent vagyok [...] privát fiókom van." #19 Alfa lány* vagy *„Igazából én nem érzem magam veszélyben, minden oldalam privát, úgyhogy igazából én kevésbé érzem azt, hogy veszélynek lennének kitéve." #66 Z lány* Ez a csoport a proaktív adatvédelem faktoron elért magas pontszámának megfelelően konkrét, szabálykövető védekezési stratégiákat alkalmaz. **Ismerik és használják a modern biztonsági eszközöket, és a fenyegetésekre automatikus, tudatos reakciókkal válaszolnak**. *„Nálam a kétlépcsős azonosítás az online felületeken, telefonon jelszó és ujjlenyomat alap." #58 Z fiú* vagy *„Egyből tiltom és nem kattintok rá, tehát ignorálom." #49 Z fiú - gyanús linkekre reagálva* és *„Hát szerintem a betűstílus meg hogyha valamit nagyon akarnak, hogy töltsd*

le meg hogy sürgetnek vele." #18 Alfa fiú - a hamis weboldalak felismeréséről. A csoport mentális erő faktoron mért magas pontszámát a negatív online interakciókra adott higgadt, racionális válaszok magyarázzák. **Ahelyett, hogy érzelmileg túlzottan reagálnának, képesek a helyzetet objektíven értékelni és érzelmi távolságot tartani.** Az online kritikát a másik fél véleményeként, nem pedig a saját értéküket megkérdőjelező támadásként kezelni. *„Hátha idegentől kapom akkor nem én nem foglalkozom vele." #3 Alfa lány* és *„Ha valami negatívat mondanának, akkor őszintén nem szokott érdekelni másoknak a negatív véleménye. Mármint, hogy oké van véleményük rólam, de ez az övék. Én ezen nem fogok megsértődni." #21 Alfa lány* Ez a csoport egy tudatos, felkészült csoport, amelynek rezilienciája a digitális környezettel szembeni egészséges szkepticizmuson és az erős belső, pszichológiai és viselkedésbeli kontrollon alapul.

A **2. klaszter**, mint a leginkább sérülékeny profil, a kvalitatív adatok alapján **a konkrét tudás hiánya és az ebből fakadó passzív, kockázatvállaló viselkedés** miatt mutat alacsony kiberrezilienciát. A proaktív védelem és a kiberfenyegetés észlelés faktorokon mért alacsony pontszámokat alátámasztja a **védelmi stratégiák hiányos ismerete**, ami a hamis weboldalak felismerésére adott válaszokban is megmutatkozik. *„Hát én nem vagyok jó ezeknek a felismerésében. Se az e-mail se az ilyen weboldalaknak. Ennyi." #42 Z fiú* Ez a tudáshiány a gyenge jelszóválasztási szokásaikban is tetten érhető, a sérülékenység egyik legfőbb forrásaként. *„Általában mindenhova ugyanazt a jelszót adom meg, és akkor így egy jelszót kell megjegyeznem." #19 Alfa lány* vagy *„Hát én nagyon hanyag vagyok ilyen szempontból mert nekem egy jelszavam van mindenhova, szóval arra rájönnek akkor nekem végem... Mióta van Facebookom, kb 10 éve kábé ugyanaz a jelszavam." #47 Z fiú* A **tudás hiánya egy passzív, kockázatvállaló magatartással párosul, ahol a negatív következményeket, még az anyagi veszteséget is, egyfajta beletörődéssel, a digitális lét természetes velejárójaként kezelik,** ami megakadályozza a tapasztalatokból való tanulást. *„Igen, én általában rákattintok a linkekre amit kapok." #47 Z fiú* és *„Feltörték nagyon sokszor mindenem, de nem zavar. Van, amelyikről költöttek is el pénzt. Az egyik kártyáról buktam nyolcezret, a másikról kb 20 ezret." #17 Alfa fiú* Ennél a csoportnál **a tudás hiánya és a veszteségek normalizálása folyamatosan fenntartja a sérülékenységet**.

A **3. klaszter**, amely a statisztikai elemzés alapján a **legmagasabb szintű, komplex kiberreziliencia-profillal rendelkezik**, a kvalitatív adatokban egy **proaktív, tanulás-orientált és érzelmileg kiegyensúlyozott felhasználói csoportként** jelenik meg. A

csoport tagjai nemcsak ismerik, de magabiztosan és következetesen alkalmazzák a modern védelmi stratégiákat. Számukra **a biztonság** nem teher, hanem egy természetes, **rutinszerű szokás, és képesek a fenyegetéseket kifinomult jelek alapján azonosítani**. *„Én mindig erős jelszót használok. Sok karakterből áll... Még kétlépcsős azonosítást is használok vagy azonosító kulcsot, illetve VPN-t." #84 Z fiú* A csoport tagjai ahelyett, hogy a passzív áldozat szerepébe kerülnének, vagy impulzívan reagálnának, a tapasztalatokat a személyes fejlődés és a tudatos érzelmi szabályozás lehetőségének tekintik. *„Fiatal koromban nagyon sokat csúfoltak és bántottak. Tehát engem ugyanúgy érint az online és a személyes bántalmazás is. Ezt szerencsére már tudom kezelni most, hogyha valaki egy rossz szót mondana rólam, akkor igazából elengedem, nem veszem magamra, aztán megyek tovább. Azóta ezt tudom kezelni." #59 Z fiú* vagy *„Már leszoktam erről most már inkább próbálom nyugodtan kezelni a problémákat, például, hogyha mondjuk, ha nem sikerül valamit először beállítani, vagy nem sikerül a wifire csatlakozni egyből, akkor veszek egy mély levegőt, és akkor nekiállok még egyszer próbálkozni. Megtanultam az indulataimat kezelni." #57 Z fiú* Az internet számukra egy eszköz, nem pedig az életük központja. Az internet nélküli lét lehetőségét nem szorongással, hanem a való világban rejlő alternatívák (család, olvasás, pihenés) lehetőségeként élik meg. *„Én most egy fura választ fogok mondani a mai világban én örülnék neki. Azért, mert akkor legalább nem hívogatnak és több időm lenne azokra a dolgokra, amit egyébként megcsinálnék..." #5 Alfa lány* és *„Engem annyira nem zavarna, rendszeresen volt az, hogy én nem telefonoztam több napon át, mert nem volt rá szükségem." #76 Z lány* Ez a csoport sikeresen alkalmazza a technikai tudást, a pszichológiai erőforrásokat és a tudatos viselkedési stratégiákat. **Képesek a digitális teret magabiztosan és biztonságosan használni, miközben megőrzik a kontrollt az online jelenlétük felett és megvédik a mentális jóllétüket**.

A kiberreziliencia modell összegzése

A kapott eredmények megerősítik és empirikusan alátámasztják a szakirodalomban körvonalazódó elméleti keretet, miszerint **a kiberreziliencia nem egyetlen, homogén képesség, hanem egy többdimenziós, komplex jelenség** [98][99]. A Személyes kiberreziliencia skála (PCRS) hét, egymástól elkülönülő, mégis összefüggő faktora, a proaktív viselkedéstől a pszichológiai megküzdésen át a technikai tudásig, hűen tükrözi ezt a sokrétűséget. A **négy, statisztikai és kvalitatív módszerekkel alátámasztott kiberreziliencia-profil** túlmutat az egyszerű *„reziliens – nem reziliens"* megközelítésen,

és egy sokkal árnyaltabb rendszert kínál. Míg a *„magasan reziliensek”* és a *„magas kockázatúak”* profiljai a spektrum két végét képviselik, addig a két köztes csoport, különösen a *„passzív, mentálisan sérülékeny problémamegoldók”* profilja hívja fel a figyelmet a legfontosabb elméleti tanulságra. E csoport létezése rávilágít **a tudás és a cselekvés közötti kritikus szakadék**ra, azaz a *„knowing-doing gap”* jelenségére a digitális térben [S-7], [S-12]. A felmérésben résztvevők gyakran rendelkeznek a kockázatok felismeréséhez szükséges tudással, de ezt nem képesek hatékony védelmi viselkedéssé alakítani [S-12]. Tehát **a kiberbiztonsági ismeretek és a technikai készségek önmagukban nem elegendőek a valódi kiberrezilienciához**. **A pszichológiai erőforrások,** mint a stressztűrés, az érzelmi szabályozás és az önszabályozási képességek, önkontroll, önreflexió, önhatékonyság, önértékelés, legalább annyira, ha nem még **fontosabb szerepet játszanak** [98], [99], [S-7].

A demográfiai elemzések tovább árnyalják a képet, jelezve, hogy **a nem és a generációs hovatartozás befolyásolja ezeket a profilokat** [S-12]. Az eredmények, például **a nők** felülreprezentáltsága **a mentálisan sérülékenyebb csoportban** [110], vagy az Alfa generáció túlzott online bizalma [63], összhangban vannak azokkal a szakirodalmi megállapításokkal, amelyek a nemek és generációk közötti eltérő digitális szocializációs utakat és kockázati kitettséget hangsúlyozzák [42], [43], [107], [S-7].

Az előző fejezetekben bemutatott elméleti háttér, módszertani keret, valamint a kvantitatív és kvalitatív vizsgálatok eredményei átfogó képet nyújtottak a problémás internethasználat, a reziliencia és a kiberbiztonsági tudatosság összetett kapcsolatrendszeréről a Z és Alfa generáció körében. A következő fejezet a kutatási eredmények konklúzióját összegzi és hipotézisek igazolását foglalja össze. A disszertáció záró szakaszaként szintetizálja a kutatás főbb megállapításait és értékeli azok tudományos és gyakorlati jelentőségét.

6 ÖSSZEGZETT KÖVETKEZTETÉSEK

A fejezet elsődleges célja a kutatási kérdések megválaszolása és a hipotézisek értékelése, igazolása. Ezt követően bemutatásra kerül a kutatás elméleti hozzájárulása a tudományterülethez, különös tekintettel a kiberreziliencia új fogalmi keretére és a generációspecifikus digitális viselkedésminták megértésére, valamint a kutatási eredmények gyakorlati alkalmazhatósága az oktatás, és a prevenció programok tervezésében. A fejezet ezen felül részletesen tárgyalja a jelen kutatás metodológiai és tartalmi korlátait, valamint javaslatot tesz olyan jövőbeli kutatási irányokra.

6.1 Főbb kutatási kérdések megválaszolása, hipotézisek igazolása

A kutatás során megfogalmazott kutatási kérdések és hipotézisek értékelésének összefoglalását, és a kapcsolódó tézispontok azonosítóit hipotézisenként összevonva a 3. táblázat mutatja be röviden, majd a részletes eredmények a táblázatot követően kerülnek kifejtésre. A kutatási kérdésekhez rendelt hipotézisek adatgyűjtési módszerének, alkalmazott statisztikai eljárásainak és kapcsolódó publikációinak részletes összefoglalását az egyes tézispontokhoz rendelten az 5. melléklet tartalmazza.

3. táblázat A kutatási kérdések és hipotézisek áttekintése

Kutatási kérdés	***Hipotézis***	***Státusz***	***Tézis***	***Kapcsolódó publikáció***
K1: Milyen különbségek, összefüggések és ok-okozati kapcsolatok (direkt és indirekt hatások) figyelhetők meg a Z és Alfa generációk kiberbiztonsági tudatossága, rezilienciája és problémás internethasználata között, valamint hogyan befolyásolják ezeket a mintázatokat a demográfiai tényezők (nem, generáció, internethasználati idő)?			**T1**	[S-12]
	H1: A napi internethasználati idő és a problémás internethasználat közötti összefüggés erőssége szignifikánsan eltér nemek és generációs hovatartozás szerint.	***Igazolt***	**T2**	[S-8], [S-9]
	H2: A reziliencia szintje szignifikáns különbségeket mutat a generációs hovatartozás és a nemek függvényében.	***Igazolt***	**T3**	[S-10]
	H3: A kiberbiztonsági tudatosság szintje szignifikáns eltéréseket mutat az internethasználat ideje, a nemek és a generációs hovatartozás függvényében.	***Igazolt***	**T4**	[S-3], [S-7], [S-11]
K2: Milyen online helyzetek okoznak leggyakrabban szorongást vagy bizonytalanságot a fiatalok körében, és hogyan kezelik ezeket?			**T5**	[S-6], [S-10]
K3: Hogyan jellemezhetők a Z és Alfa generációs internetezők kiberreziliencia-profiljai, és milyen szignifikáns különbségek mutatkoznak a két generáció között ezen profilok és a kiberreziliencia aldimenziói mentén?	H4: A kiberbiztonsági tudatosság, pszichológiai reziliencia és problémás internethasználat alapján szignifikánsan elkülönülő kiberreziliencia-profilok azonosíthatók.	***Igazolt***	**T6**	[S-12]
	H5: Az Alfa generáció tagjai szignifikánsan eltérő kiberreziliencia profilt mutatnak a Z generációhoz képest.	***Igazolt***	**T7**	[S-12]

Megjegyzés: A kutatási célok, kérdések és hipotézisek vizsgálati módszereinek, statisztikai eljárásainak, szignifikanciájának és kapcsolódó publikációinak tézispontonkénti részletes összefoglalóját az 5. melléklet tartalmazza.

A dolgozat következő pontjában a Z és Alfa generáció kiberbiztonsági tudatosságát, rezilienciáját és problémás internethasználatát vizsgáltam. A **vizsgálat célja** az volt, hogy **feltérképezze a generációk közötti különbségeket, az összefüggéseket és a direkt, valamint indirekt ok-okozati mintázatokat a kiberbiztonsági tudatosság, a reziliencia és a problémás internethasználat területén.** Az **eredmények alapján a H1, H2 és H3 hipotézisek igazolódtak**, miszerint a napi internethasználati idő és a problémás internethasználat közötti összefüggés erőssége szignifikánsan eltér nemek és generáció között *(H1 hipotézis)*, a reziliencia szintje szignifikáns különbségeket mutat a nemek és generációs hovatartozás függvényében *(H2 hipotézis)*, és a kiberbiztonsági tudatosság mértéke szoros összefüggést mutat a napi internethasználati idővel, a nemmel és a generációs hovatartozással *(H3 hipotézis)*. Az eredmények alapján vált lehetővé a következő tézisek megfogalmazása és a generációk közötti eltérések elemzése.

1. tézis (T1): Kombinált mediációs és moderációs regressziós elemzéssel **igazoltam, hogy a problémás internethasználat és a kiberbiztonsági tudatosság között egyaránt kimutatható közvetlen és a reziliencián keresztül érvényesülő indirekt, negatív hatás. Kimutattam**, hogy a **problémás internethasználat csökkenti a reziliencia szintjét** *($b = -0.384;\ p < 0.001$)*, **amely viszont erőteljes pozitív hatást gyakorol a kiberbiztonsági tudatosságra** *($b = 0.851;\ p < 0.001$)*. Ez a részleges mediációs mechanizmus azt jelzi, hogy a problémás internethasználat nemcsak közvetlenül rontja a kiberbiztonsági kompetenciákat *($b = -0.167;\ p = 0.009$)*, hanem közvetve, a reziliencia készség gyengítésén keresztül is *($b = -0.327;\ 95\%\ CI\ [-0.395;\ -0.263]$)*, ami részleges mediációs mechanizmust igazol. **Megállapítottam**, hogy a vizsgált összefüggésrendszer generációtól és internethasználati időtől függetlenül érvényesül, ugyanakkor **a nem szignifikáns moderátorként jelenik meg a reziliencia és a kiberbiztonsági tudatosság útvonalon** *($b = -0.190,\ p = 0.005$)*, ahol **a reziliencia védő hatása a férfiak körében** *($b = 0.960$)* **erősebb**, mint a nők körében*($b = 0.770$)*, mely az indirekt hatás mértékében is megmutatkozik *($b_{férfi} = -0.369,\ b_{nő} = -0.296,\ index = 0.073,\ 95\%\ CI\ [0.010;\ 0.138]$)*. A mediációs mechanizmus a generációtól és a napi internethasználat mértékétől függetlenül érvényesül, és a problémás internethasználat minősége meghatározóbb a kiberbiztonsági tudatosság szempontjából, mint a használat mennyisége. [S-12]

2. tézis (T2): Regressziós és moderációs elemzések alkalmazásával **igazoltam, hogy a napi internethasználati idő a problémás internethasználat legerősebb prediktora** *($b = 1.18,\ p < .001$)*, amely a vizsgált modellben a variancia több mint 10%-át

magyarázza *($R^2 = .103–.123$)*. Kimutattam továbbá, hogy a napi internethasználati idő és a problémás internethasználat kapcsolatában a *nem* szignifikáns főhatással rendelkezik, ahol a nők átlagosan magasabb problémás internethasználati értéket értek el *($b = 0.99$, $p < .001$)*. Moderációs elemzésekkel **bizonyítottam, hogy a napi internethasználati idő és a problémás internethasználat közötti pozitív kapcsolat erőssége szignifikánsan függ mind a nemtől, mind a generációs hovatartozástól**. Az összefüggés a nőknél erőteljesebb *($b = 0.67$)*, mint a férfiaknál *($b = 0.45$)*, továbbá az **Alfa generációban az internethasználat növekedése szintén erősebb hatással van a problémás internethasználat emelkedésére** *($b = 2.25$),* mint a Z generáció esetében *($b = 1.65$)*. Összességében a **H1 hipotézis empirikusan igazolódott**. Az eredmények alapján megállapítottam, hogy a problémás internethasználat kialakulását nem kizárólag a használat mennyisége, hanem annak demográfiai kontextusa is jelentősen befolyásolja, különös tekintettel a női felhasználókra és az Alfa generáció tagjaira, akik magasabb kockázatot mutatnak a fokozott internethasználat mellett [S-8], [S-9].

3. tézis (T3): Nemparaméteres statisztikai vizsgálatokkal és klaszteranalízissel **igazoltam, hogy a reziliencia szintje szignifikáns különbségeket mutat mind a generációs hovatartozás, mind a nem függvényében.** A Mann–Whitney U-próba eredményei *($U = 923181.50$, $z = –4.119$, $p < .001$)* alapján kimutattam, hogy az **Alfa generáció** tagjai szignifikánsan **alacsonyabb reziliencia értékekkel rendelkeznek** *(Mean Rank = 1521.96)*, mint a Z generáció tagjai *(Mean Rank = 1677.84)*. A nemi különbségek szintén szignifikánsak *($U = 1148668.50$, $z = –6.902$, $p < .001$)*, **a lányok alacsonyabb reziliencia szintet érnek el** *(Mean Rank = 1516.25)*, mint a fiúk *(Mean Rank = 1744.61)*. Klaszteranalízissel **három eltérő rezilienciaprofilt azonosítottam**, amelyek eloszlása **szignifikáns kapcsolatot mutatott mind a generációval** *($\chi^2(2) = 16.415$, $p < .001$; Cramer's $V = .071$)*, mind **a nemmel** *($\chi^2(2) = 55.949$, $p < .001$; Cramer's $V = .131$)*. Eredményeim alapján **megállapítottam, hogy az Alfa generáció és a lányok felülreprezentáltak az alacsony rezilienciájú** *(„Törékenyek”)* **klaszterben** (27.1%, 29.0%), míg a Z generáció és a fiúk nagyobb arányban tartoznak a magas rezilienciájú *(„Megállíthatatlan”)* profilba (36.8%, 39.3%), ami rámutat a demográfiai tényezők meghatározó szerepére a pszichológiai ellenálló képesség alakulásában. Összességében a **H2 hipotézis empirikusan igazolódott**. A reziliencia mértékét mind a generációs, mind a nemi tényezők érdemben befolyásolják [S-10].

4. tézis (T4): Korrelációs és regressziós elemzésekkel **igazoltam, hogy a napi internethasználati idő szignifikáns, ugyanakkor gyenge negatív kapcsolatban áll a kiberbiztonsági tudatosság több dimenziójával**, így különösen a személyes adatok védelmével *(r_s = - 0.233, $p < .001$)*, a használt jelszavak erősségével *(r_s = -0.126, $p < .001$)*, valamint az ismeretlen források elkerülésével *(r_s = -0.108, $p = .002$)*. Lineáris regressziós modellel **kimutattam, hogy az internethasználat ideje szignifikáns negatív prediktora a kiberbiztonsági tudatosságnak** (*(β = -0.076, $p < .001$)*, míg a nem és a generációs hovatartozás hatása elsősorban közvetett módon érvényesül. Eredményeim alapján **megállapítottam, hogy az Alfa generáció alacsonyabb kiberbiztonsági tudatossággal, ugyanakkor magasabb szubjektív biztonságérzettel jellemezhető** *(OR = 0.49, $p < .001$)*. Az Alfa generáció tagjai tehát gyakrabban vélik biztonságosnak például az online, felhőben történő adattárolást, míg a Z generáció kritikusabb és reálisabb kockázatészlelést mutat. A nemi különbségek eredményei alapján **a nők szignifikánsan fejlettebb kockázatészlelést és magasabb óvatosságot tanúsítottak az ismeretlen e-mailekkel és online kommunikációval, kapcsolattartással kapcsolatban** *(OR = 1.54, $p < .001$),* **míg a férfiak a technikai védekezés, a vírusírtó és a tűzfalhasználat terén mutattak magasabb tudatosságot** *(OR = 1.81, $p < .001$)*. Az eredmények összességében igazolják, hogy a kiberbiztonsági tudatosság alakulását az internethasználat intenzitása mellett a generációs és nemi sajátosságok is differenciált módon befolyásolják. Az eredmények alapján a **H3 hipotézis megerősítést nyert,** a napi internethasználat növekedése szignifikánsan alacsonyabb kiberbiztonsági tudatossággal jár együtt, különösen az Alfa generáció körében szignifikáns, és a biztonságérzet naivitással jár együtt, míg a Z generáció esetében reálisabb és kritikusabb kockázatészlelés tapasztalható [S-3], [S-7], [S-11].

A következőkben az online környezetben, helyzetekben tapasztalható szorongás és bizonytalanság forrásait vizsgáltam. A vizsgálat **célja az volt, hogy feltérképezze mely online helyzetek okoznak leggyakrabban szorongást vagy bizonytalanságot a fiatalok körében, és hogyan kezelik ezeket**. A kvalitatív fókuszcsoport felmérések eredményei alátámasztották, hogy a technikai problémák, negatív online visszajelzések, online zaklatás és adatbiztonsági fenyegetések váltják ki leggyakrabban stresszt, szorongást, ahol az Alfa generáció lányai impulzívabb reakciókat mutatnak. A megküzdési stratégiákat vizsgálva, az online stressz kezelése leggyakrabban a gyors

probléma-megoldás, figyelemelterelés és külső támogatás igénybevétele révén történik, amely megalapozza a következő tézis megfogalmazását.

5. tézis (T5): Kvalitatív vizsgálatok és tematikus tartalomelemzés segítségével **feltártam, hogy a fiatalok körében az online térben megélt stresszt, szorongást és bizonytalanságot első sorban a technikai jellegű problémák** (pl. internet lassulás, hozzáférési nehézségek), **az online visszajelzésekhez kapcsolódó negatív élmények, valamint az online zaklatás és adatbiztonsági fenyegetések okozzák**. Megállapítottam, hogy ezek a helyzetek gyakran **intenzív, impulzív érzelmi reakciókat** váltanak ki, jellemzően frusztráció, idegesség és dühkitörés formájában jelentkeznek, **különösen az Alfa generációnál, azon belül is a lányok körében** figyelhető meg. Ezzel szemben az önreflexió, érzelmi önszabályozás, mint egyfajta tudatosan használt megküzdési stratégia, elsősorban a Z generációnál, ezen belül is főként a lányoknál jelenik meg nagyobb arányban. Kimutattam továbbá, hogy a nemek között eltérő stresszorok és reakcióminták jelennek meg. A nők esetében az online visszajelzések és kritikák jelentenek fokozott érzelmi terhelést, míg a férfiaknál elsősorban a technikai jellegű, kontrollvesztéssel járó helyzetek idéznek elő impulzívabb stresszreakciókat. Eredményeim alapján **megállapítottam**, hogy bár mind az Alfa, mind a Z generáció online rezilienciája még fejlődőben van, **a pszichológiai alkalmazkodóképesség és önkontroll jelei már megfigyelhetők, különösen a Z generáció esetében, míg az Alfa generációnál a korai, preventív fejlesztés kiemelt jelentőségű** [S-6], [S-10]

A következő kutatási rész **vizsgálati célja annak feltérképezése, hogy milyen szignifikáns különbségek mutatkoznak a Z és Alfa generáció között a kiberreziliencia profilok és aldimenziói mentén**. A kérdőíves felmérés **eredményei igazolták a H4 és H5 hipotéziseket**, amelyek szerint a kiberbiztonsági tudatosság, pszichológiai reziliencia és problémás internethasználat alapján jól elkülöníthető kiberreziliencia-profilok azonosíthatók *(H4 hipotézis),* valamint a generációhoz való tartozás szignifikánsan befolyásolja ezek eloszlását *(H5 hipotézis)*. Az eredmények rámutattak arra, hogy az Alfa generáció tagjai technológiacentrikus, ugyanakkor alacsonyabb mentális erő- és önkontrollszinttel jellemezhetők, míg a Z generáció hibrid, adaptív profilú. Ezek a megállapítások alapozták meg a következő tézisek megfogalmazását.

6. tézis (T6): Klaszteranalízissel **négy, egymástól jól elkülöníthető kiberreziliencia-profilt azonosítottam, amelyek a kiberbiztonsági tudatosság, a pszichológiai reziliencia és a problémás internethasználat dimenziói mentén szignifikánsan differenciálódnak**. Kimutattam, hogy a profilok között a kiberbiztonsági tudatosság aldimenziói, különösen **az aktív technikai védelem** *(F(1, 3271) = 10.30, p = .001)* és a **kiberfenyegetések észlelése** *(F(1,3271) = 14.36, p < .001)* mentén szignifikáns **különbségek figyelhetők meg**. A pszichológiai reziliencia tekintetében a **mentális erő és önkontroll dimenziója** mutatta a legerősebb eltéréseket *(F(1,3271) = 49.47, p < .001),* míg a problémás internethasználathoz kapcsolódó **offline jóllét faktor** mentén szintén szignifikáns differenciáló tényezőnek tapasztalható *(F(1,3271) = 11.89, p < .001).* Az azonosított klaszterek közül a *„passzív, mentálisan sérülékeny problémamegoldók”* (21.7%) és a *„magas rezilienciájú, proaktív és tudatosak”* (30.7%) a spektrum két végpontját képviselik, míg a köztes csoportokat az *„óvatos navigálók”* (31.6%) és a *„magas kockázatú sérülékenyek”* (15.9%) alkotják. **Eredményeim empirikusan alátámasztják a kiberreziliencia multidimenzionális modelljének érvényességét és differenciáló képességét, a H4 hipotézis igazolást nyert** [S-12].

7. tézis (T7): Khi-négyzet próbával **igazoltam, hogy a profilok eloszlása szignifikáns különbséget mutat a Z és az Alfa generáció között** *($\chi^2(3) = 11.07$, $p = .011$).* A kiberreziliencia aldimenzióinak vizsgálata alapján **megállapítottam, hogy a Z generáció szignifikánsan magasabb mentális erővel** *($p = .005$)*, **offline jólléttel** *($p = .007$)* és **online problémamegoldó képességgel** *($p < .001$)* jellemezhető, míg az **Alfa generáció** esetében szignifikánsabb **magasabb az online adattárolásba vetett bizalom** *($p < .001$)*. Eredményeim rámutatnak, hogy **a Z generáció egy kiegyensúlyozott, hibrid védelmi modellt alkalmaz**, amelyben a mentális ellenálló képesség, a tudatos digitális jelenlét egyaránt meghatározó és esetükben lehetővé válik a rugalmas alkalmazkodás és reaktív-adaptív reakciók készsége, míg **az Alfa generáció inkább technológiacentrikus megközelítést képvisel,** amelyet fokozott, naiv bizalom, és gyengébb offline megküzdési és problémamegoldó képesség jellemez, ami növelheti sérülékenységüket online incidensek esetén, a **H5 hipotézis igazolást nyert** [S-12].

6.2 Elméleti hozzájárulások

A kutatás több szempontból is jelentős elméleti hozzájárulást nyújt a digitális generációk és kiberreziliencia kutatásához. Először is, az **Alfa generáció átfogó vizsgálata** önmagában újdonságot jelent a hazai tudományos diskurzusban. A felnövekvő generáció

és a Z generáció összehasonlító elemzése lehetővé tette a **generációspecifikus kiberbiztonsági attitűdök, viselkedési mintázatok és pszichológiai jellemzők feltárását**, amelyek mindeddig hiányoztak a magyar kutatási kontextusból.

Másodszor, a kutatás során sor került a **kiberbiztonság tudatosság kérdőív (CS-C) magyar nyelvű adaptálására és validálására,** amely módszertani szempontból fontos lépésnek tekinthető. Az eszköz hazai alkalmazhatósága **lehetővé teszi a nemzetközi összehasonlíthatóságot**, és hozzájárul a kiberbiztonsági tudatosság mérésének megbízhatóságához magyar nyelvi környezetben [S-7].

Harmadszor, a kutatás **sikeresen integrálta és validálta a személyes kiberreziliencia skálát (PCRS)** [S-12]**, egy többdimenziós eszközt, amely képes megragadni a fiatalok online megküzdési képességeinek komplexitását**. A skála alkalmazásával a kutatás túllépett a *„digitális bennszülöttek”* homogén szemléletén, és négy, jellegzetes kiberreziliencia-profilt tárt fel, amelyek a sérülékenység és az erősségek eltérő mintázatait mutatják. A kiberreziliencia-profilok azonosításával és a köztük feltárt szignifikáns generációs és nemi különbségek feltárásával túlmutat a hagyományos digitális írástudás fogalmán. **Az eredmények új értelmezési keretet nyújtanak a felhasználói sebezhetőség megértéséhez**, mivel a kiberrezilenciát nem egységes képességként, hanem többrétegű, differenciált folyamatként írják le. Ez a szemléletváltás lehetővé teszi, hogy a megelőzési és beavatkozási stratégiák ne általános készségfejlesztésre, hanem az egyes profilok sajátos pszichológiai, viselkedéses és tudás béli jellemzőire épülő, célzott módszerekre irányuljanak. Ezáltal a kutatás hozzájárul ahhoz az elméleti váltáshoz, amely a digitális biztonságot nem pusztán technikai vagy ismereti kérdésként, hanem komplex, demográfiai és pszichoszociális tényezők által formált reziliencia-rendszerként értelmezi [S-12].

6.3 Gyakorlati alkalmazhatóság

A kutatás eredményei több területen is hasznosíthatók. Az **oktatási szektorban** a kiberbiztonsági tudatosság validált mérőeszköze lehetővé teszi a tanulók kiberbiztonsági tudatosságának objektív felmérését, amely alapján célzott fejlesztési programok tervezhetők a tudáshiányos és kritikus területek kiemelten történő fejlesztésére.

A **PCRS skála diagnosztikai eszközként** használható az oktatásban a **kockázati csoportok azonosítására,** a négy azonosított kiberreziliencia-profil differenciált pedagógiai intervenciók kidolgozását támogatja, figyelembe véve a generációspecifikus

és nemi különbségeket. Az azonosított profilok pedig lehetővé teszik a *„one-size-fits-all”* megközelítés meghaladását és célzott, differenciált intervenciók kidolgozását. Míg a *„magas kockázatúak"* csoportja alapvető tudás- és készségfejlesztést igényel, addig a *„passzív problémamegoldók”* esetében a mentális egészségre, a stresszkezelésre és az önszabályozásra fókuszáló programok lehetnek hatékonyak.

A kutatás továbbá **alapot nyújt az evidenciaalapú prevenciós stratégiák és digitális kompetenciafejlesztési programok kialakításához**. Az eredmények hozzájárulhatnak a Nemzeti Kiberbiztonsági Stratégia oktatási elemeinek finomításához.

A **vállalati szektorban** a generációspecifikus biztonsági tudatosság mintázatok ismerete segíti a munkáltatókat a **célzott kiberbiztonsági képzések tervezésében és a fiatal munkavállalók digitális kompetenciáinak, puha készségeinek, kiberrezilienciájának fejlesztésében.**

6.4 Kutatás korlátai és jövőbeli irányok

A kutatás korlátai közé tartozik a minta egyetlen magyar megyére való korlátozódása, ami csökkenti az eredmények általánosíthatóságát, valamint a keresztmetszeti adatok nem teszik lehetővé ok-okozati kapcsolatok feltárását. Jövőbeli longitudinális vizsgálatok szükségesek a kiberreziliencia profilok időbeli stabilitásának és kialakulásuk családi-iskolai tényezőinek feltárásához. A PCRS skála nemzetközi mintákon történő további validálása és egy alacsony faktortöltésű tétel átdolgozása is indokolt a faktor belső koherenciájának erősítése érdekében.

Következtetések és implikációk összegzése

Összefoglalva, ezen tanulmány eredményeképpen egy új, megbízható eszköz jött létre a fiatalok kiberrezilienciájának mérésére, és az azonosított profilok révén mélyebb betekintést nyújt a digitális bennszülöttek online megküzdési stratégiáinak heterogenitásába. A konklúzió fejezetben átfogóan értékeltem a disszertáció kutatási eredményeit és azok tudományos, valamint gyakorlati jelentőségét. A kutatási kérdésekre adott válaszok megerősítették, hogy a problémás internethasználat, a reziliencia és a kiberbiztonsági tudatosság között összetett kapcsolatrendszer áll fenn, amely generációkon átívelő érvényességgel bír, ugyanakkor a nem szerinti különbségek jelentős moderáló szerepet játszanak. A hipotézisek igazolást nyertek.

7 ÖSSZEFOGLALÁS

A digitális társadalom korában a kiberbiztonság nem csupán technológiai kérdés, hanem alapvetően viselkedésalapú jelenség, mivel az online támadások többsége az emberi sebezhetőséget célozza meg. Jelen disszertáció a Z és Alfa generáció kiberbiztonsági attitűdjét, rezilienciáját és problémás internethasználati szokásait vizsgálja integrált megközelítésben, különös tekintettel a generációspecifikus viselkedési mintázatokra és a digitális térben való adaptív működésre.

A kutatás elsődleges célja, hogy átfogó képet nyújtson a digitális bennszülött generációk (Z és Alfa generáció) kiberbiztonsági tudatosságáról, rezilienciájáról és problémás internethasználatáról, valamint ezek komplex kapcsolatrendszeréről. Másodsorban a kutatás elméleti és gyakorlati szinten is hozzájárul a kiberreziliencia fogalmának tudományos megalapozásához egy többdimenziós modell integrálása és validálása révén. A kutatás további eredménye egy kiberbiztonsági tudatosságot mérő eszköz magyar nyelvű adaptációja és validációja, amely lehetővé teszi a hazai populáció szisztematikus vizsgálatát.

A disszertáció vegyes módszertani megközelítést alkalmaz, amely a kvantitatív és kvalitatív kutatási módszertant ötvözi, az attitűdvizsgálat komplex vizsgálati sajátossága miatt. A kvantitatív vizsgálatban 3275 fős, Fejér vármegyei mintán keresztmetszeti kérdőíves adatfelvétel történt, amely validált mérőeszközöket (Problémás internethasználati kérdőív PIHK-6, Connor-Davidson reziliencia skála CD-RISC-10) és az adaptált kiberbiztonsági tudatosság kérdőívet tartalmazott. Az elemzés induktív, feltáró és deduktív, megerősítő szakaszokból állt, lehetővé téve a komplex összefüggések statisztikai feltárását és a hipotézisek empirikus tesztelését. A kvalitatív fókuszcsoportos vizsgálatok célja a generációk kiberbiztonsági attitűdjeinek, tudatosságának, viselkedési szándékának és érzelmi reakcióinak mélyebb megértése volt. A kutatás öt hipotézist vizsgált és erősített meg empirikusan.

Az eredmények empirikusan megerősítik, hogy a kiberreziliencia többdimenziós jelenség, amelyet a kiberbiztonsági tudatosság, a pszichológiai reziliencia és a problémás internethasználat alacsony szintje együttesen határoznak meg. A klaszterelemzés négy jól elkülönülő kiberreziliencia-profilt azonosított, amelyek a kiberbiztonsági tudatosság, reziliencia és problémás internethasználat dimenzióinak jellegzetes mintázatait reprezentálják. A kutatás négy fő kiberreziliencia profilt azonosított, amelyek a

kiberbiztonsági tudatosság, pszichológiai reziliencia és problémás internethasználat mentén szignifikánsan elkülönülnek. A problémás internethasználat direkt és indirekt módon, a reziliencia közvetítésével negatívan befolyásolja a kiberbiztonsági tudatosságot, különösen a nők és az Alfa generáció körében erősebb ez a kapcsolat.

Az Alfa generáció technológiacentrikus paradigmát követ, azaz magasabb bizalmat mutat a digitális rendszerek iránt, de alacsonyabb mentális erőt, gyengébb offline problémamegoldó képességet és naivabb kockázatészlelést tanúsít. A Z generáció hibrid-adaptív modellt alkalmaz, kiegyensúlyozottabb mentális állóképességgel, kritikusabb kockázatészleléssel és fejlettebb megküzdési stratégiákkal rendelkezik.

A nők óvatosabb viselkedést és erősebb kockázatészlelést mutatnak, míg a férfiak magasabb technikai tudatossággal és erősebb reziliencia védő hatással rendelkeznek. A napi internethasználati idő növekedése mindkét generációnál csökkenti a kiberbiztonsági tudatosságot, azonban a problémás használat minősége kritikusabb tényező, mint mennyisége.

A kutatás eredményei rávilágítanak arra, hogy a kiberbiztonsági oktatás és az ehhez kapcsolódó prevenció nem épülhet kizárólag technikai ismeretekre épülő megközelítésre. A sikeres fejlesztéshez pszichológiai erőforrások is szükségesek, mint a stresszkezelési képesség, az érzelmek szabályozása és az önkontroll készségének fejlesztése. Ezen puha készségek meghatározó szerepet játszanak a hatékony kiberreziliencia kialakításában, természetesen a naprakész technikai tudással karöltve.

A generációspecifikus különbségek alapján az Alfa generáció körében kiemelt figyelmet kell fordítani a kritikus gondolkodás és az egészséges szkepticizmus fejlesztésére, míg a Z generáció esetében a meglévő tudás alkalmazása, ennek a motivációja jelenti a fő kihívást. A nemi különbségek figyelembevétele szintén elengedhetetlen a differenciált pedagógiai intervenciók tervezésekor.

A kidolgozott kiberreziliencia-modell és a validált magyar nyelvű mérőeszköz lehetőséget biztosít a hazai oktatási intézmények számára a diákok kiberbiztonsági felkészültségének diagnosztizálására és a célzott fejlesztési programok kidolgozására. A kutatás eredményei hozzájárulnak a Z és Alfa generációk digitális kompetenciáinak fejlesztéséhez és a 21. századi munkaerőpiaci elvárásoknak megfelelő készségek kialakításához, ezáltal elősegítve a biztonságosabb és tudatosabb jelenlétüket a kibertérben.

HIVATKOZOTT IRODALOMI FORRÁSOK

[1] Simon Kemp, „Digital 2024: Global Overview Report — DataReportal – Global Digital Insights”, https://datareportal.com/reports/digital-2024-global-overview-report.

[2] M. McCrindle és A. Fell, *Understanding Generation Alpha*. McCrindle Research, 2020.

[3] E. Slamet és Z. Ruhwanya, *Factors Influencing Generation Z's Cybersecurity Practices: An Empirical Analysis*, köt. 709. 2024. doi: 10.1007/978-3-031-66986-6_9.

[4] Candiwan, B. P. Sudirman, és P. K. Sari, „Differences in Information Security Behavior of Smartphone Users in Indonesia Using Pearson's Chi-square and Post Hoc Test”, *Int. J. Adv. Sci. Eng. Inf. Technol.*, köt. 13, sz. 2, 2023, doi: 10.18517/ijaseit.13.2.17975.

[5] G. Gerontakis, P. Yannakopoulos, és I. Voyiatzis, „Evaluating Cybersecurity Certifications: A Framework for Extracting Educational Scenarios in Cybersecurity Training”, in *ACM International Conference Proceeding Series*, 2023. doi: 10.1145/3635059.3635097.

[6] Magyar Közlöny, „110/2012. (VI. 4.) Korm. rendelet a Nemzeti alaptanterv kiadásáról, bevezetéséről és alkalmazásáról”, https://njt.hu/jogszabaly/2012-110-20-22.

[7] E. N. Gökhan és P. A. Çerçi, *Cybersecurity applications in Industry 4.0*. 2025. doi: 10.4018/979-8-3693-6417-8.ch003.

[8] D. C. Uprety *és mtsai.*, „Securing the smart revolution: Navigating security and privacy concerns in Industry 4.0 vs. Industry 5.0”, in *Applications of Artificial Intelligence in 5g and Internet of Things Proceedings of the 1st International Conference on Applications of AI in 5g and Iot Icaai5gi 2024*, 2025, o. 427–431. doi: 10.1201/9781003532521-81.

[9] R. Kour, R. Karim, P. Dersin, és N. Venkatesh, „Cybersecurity for Industry 5.0: trends and gaps”, *Front. Comput. Sci.*, köt. 6, júl. 2024, doi: 10.3389/fcomp.2024.1434436.

[10] A. Chaudhuri, R. K. Behera, és P. K. Bala, „Factors impacting cybersecurity transformation: An Industry 5.0 perspective”, *Comput. Secur.*, köt. 150, 2025, doi: 10.1016/j.cose.2024.104267.

[11] Bereczki Enikő, *A rejtélyes Z generáció: Együttműködés a mai tizen- és huszonévesekkel*, ISBN 9789635651382. HVG Könyvek, 2022.

[12] H. Turóczi és Á. Kun, „A digitális jóllét pozitív pszichológiai megközelítésben”, *Magyar Pszichológiai Szemle*, köt. 79, sz. 4, o. 727–753, febr. 2025, doi: 10.1556/0016.2024.00098.

[13] Á. Szapáry *és mtsai.*, „Internetfüggőség: a 21. század orvosi kihívása?”, *Orv. Hetil.*, köt. 163, sz. 38, 2022, doi: 10.1556/650.2022.32538.

[14] D. S. Reddy és S. V. Rao, „Cybersecurity skills: The moderating role in the relationship between cybersecurity awareness and compliance”, in *AMCIS 2016: Surfing the IT Innovation Wave - 22nd Americas Conference on Information Systems*, 2016.

[15] M. Ö. Atalay, Y. E. Tunç, és H. C. Erkengel, „Cyber-spirituality in the workplace”, in *Spirituality Management in the Workplace: New Strategies and Approaches*, 2023. doi: 10.1108/978-1-83753-450-020231016.

[16] M. Iftikhar, Z. Waheed, Um-E-Laila, S. Khan Yousafzai, és M. Imran Qureshi, „Traditional bullying and cyber bullying: Prevalence, effects and workplace spirituality as an anti-bullying policy”, *International Journal of Management (IJM*, köt. 11, sz. 11, 2020.

[17] S. Mahmood, M. Chadhar, és S. Firmin, „Digital resilience framework for managing crisis: A qualitative study in the higher education and research sector”, *Journal of Contingencies and Crisis Management*, köt. 32, sz. 1, 2024, doi: 10.1111/1468-5973.12549.

[18] A. McCormac, D. Calic, K. Parsons, M. Butavicius, M. Pattinson, és M. Lillie, „The effect of resilience and job stress on information security awareness”, *Information & Computer Security*, köt. 26, sz. 3, o. 277–289, júl. 2018, doi: 10.1108/ICS-03-2018-0032.

[19] K. J. Katkar, M. A. Fernandes, F. Prajapati, K. R. Dodiya, A. Khunt, és D. Patel, „Cyber Security for Preserving Mental Wellness and Preventing Abuse”, in *Exploiting Machine Learning for Robust Security*, IGI Global, 2025, o. 275–304. doi: 10.4018/979-8-3693-7758-1.ch013.

[20] N.-K. Naeem és C. P. Mushibwe, „Navigating digital worlds: a scoping review of skills and strategies for enhancing digital resilience among higher education students on social media platforms”, *Discover Education*, köt. 4, sz. 1, o. 39, febr. 2025, doi: 10.1007/s44217-025-00432-7.

[21] 1089/2025. (III. 31.) Korm. határozat Magyarország Kiberbiztonsági Stratégiájáról, „Magyar Közlöny”, https://njt.hu/jogszabaly/2025-1089-30-22.

[22] Európai Bizottság, „Az európai oktatási térség 2025-ig történő megvalósítása, valamint az oktatás és a képzés átalakítása a digitális kornak megfelelően”, https://ec.europa.eu/commission/presscorner/detail/hu/ip_20_1743.

[23] Magyar Közlöny, „32/2024. (VIII. 8.) BM rendelet”, https://njt.hu/jogszabaly/2024-32-20-0A.

[24] Oktatási Hivatal, „Az országos mérések eredményei - 2.0”, https://okm.kir.hu/fit2.

[25] T. Palicz *és mtsai.*, „Biztonságtudatosság a kibertérben – a 2020-as országos lakossági felmérés eredményei”, *Belügyi Szemle*, köt. 70, sz. 2, o. 395–418, febr. 2022, doi: 10.38146/BSZ.2022.2.11.

[26] Mészáros Rezső, „A kibertér társadalomföldrajzi megközelítése”, *Magyar Tudomány*, köt. 7., o. 769–779, 2001.

[27] T. Palicz, B. Bencsik, és M. Szócska, „Kiberbiztonság a koronavírus idején – a COVID–19 nemzetbiztonsági aspektusai”, *Scientia et Securitas*, köt. 2, sz. 1, o. 78–87, júl. 2021, doi: 10.1556/112.2021.00001.

[28] J.-M. Chenou, „The contested meanings of cybersecurity: evidence from post-conflict Colombia”, *Conflict Security and Development*, köt. 21, sz. 1, o. 1–19, 2021, doi: 10.1080/14678802.2021.1888512.

[29] N. S. Sulaiman *és mtsai.*, „A Review of Cyber Security Awareness (CSA) Among Young Generation: Issue and Countermeasure”, 2022, o. 957–967. doi: 10.1007/978-3-030-85990-9_76.

[30] M. Veale és I. Brown, „Cybersecurity”, *Internet Policy Review*, köt. 9, sz. 4, o. 1–22, 2020, doi: 10.14763/2020.4.1533.

[31] S. Chaudhary, V. Gkioulos, és S. Katsikas, „Developing metrics to assess the effectiveness of cybersecurity awareness program”, *J. Cybersecur.*, köt. 8, sz. 1, 2022, doi: 10.1093/cybsec/tyac006.

[32] I. Corradini, *Developing Cybersecurity Awareness*, köt. 284. 2020. doi: 10.1007/978-3-030-43999-6_6.

[33] I. Dobak és S. Magyar, *Thoughts on the Place and Role of Cybersecurity Awareness*, köt. Part F2433. 2024. doi: 10.1007/978-3-031-47990-8_36.

[34] M. Khader, M. Karam, és H. Fares, „Cybersecurity Awareness Framework for Academia”, *Information*, köt. 12, sz. 10, o. 417, okt. 2021, doi: 10.3390/info12100417.

[35] A. Sangwan, „Human Factors in Cybersecurity Awareness”, in *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)*, IEEE, máj. 2024, o. 1–7. doi: 10.1109/ISCS61804.2024.10581139.

[36] M. Saleem, R. Kumar, C. Chawla, és M. Singh, „Understanding the Human Factors in the Psychology of Cyber Threats”, 2024, o. 39–52. doi: 10.4018/979-8-3693-9235-5.ch003.

[37] Varinos, „Cybersecurity Statistics and Trends”, https://www.varonis.com/blog/cybersecurity-statistics/.

[38] ISC, „Cybersecurity Workforce Study: A critical need for cybersecurity professionals persists amidst a year of cultural and workplace evolution.”, https://www.isc2.org/Research/Workforce-Study#.

[39] Tom. Butler-Bowdon, *50 psychology classics : your shortcut to the most important ideas on the mind, personality, and human nature*. Nicholas Brealey Publishing, 2017.

[40] I. Zahid, S. Hussein, és S. Mahdi, „Measuring Individuals Cybersecurity Awareness Based on Demographic Features”, *Iraqi Journal for Electrical and Electronic Engineering*, köt. 20, sz. 1, o. 58–67, jún. 2024, doi: 10.37917/ijeee.20.1.6.

[41] C. S. Lee és D. Kim, „Pathways to Cybersecurity Awareness and Protection Behaviors in South Korea”, *Journal of Computer Information Systems*, köt. 63, sz. 1, o. 94–106, jan. 2023, doi: 10.1080/08874417.2022.2031347.

[42] I. Arpaci és K. Sevinc, „Development of the cybersecurity scale (CS-S): Evidence of validity and reliability”, *Information Development*, köt. 38, sz. 2, o. 218–226, jún. 2022, doi: 10.1177/0266666921997512.

[43] R. Rohan, D. Pal, J. Hautamäki, S. Funilkul, W. Chutimaskul, és H. Thapliyal, „A systematic literature review of cybersecurity scales assessing information security awareness”, *Heliyon*, köt. 9, sz. 3, o. e14234, márc. 2023, doi: 10.1016/j.heliyon.2023.e14234.

[44] A. Almansoori, M. Al-Emran, és K. Shaalan, „Exploring the Frontiers of Cybersecurity Behavior: A Systematic Review of Studies and Theories”, *Applied Sciences*, köt. 13, sz. 9, o. 5700, máj. 2023, doi: 10.3390/app13095700.

[45] Nyikes Zoltán, „Az információbiztonság növelése a felhasználó támogatásának lehetőségeivel”, 2019, *Biztonságtudományi Doktori Iskola, Budapest*.

[46] R. Gyaraki, „A biztonságtudatosság szerepe, avagy kérdések a kiberbiztonságról”, *Magyar Rendészet*, köt. 22, sz. 2, o. 245–261, nov. 2022, doi: 10.32577/mr.2022.2.16.

[47] I. Tolstikova, O. Ignatjeva, K. Kondratenko, és A. Pletnev, „Genesis of ethical norms in the digital environment as a factor of personality anomie of generation Z”, in *CEUR Workshop Proceedings*, 2021.

[48] M. Drugas, „Screenagers or ‘Screamagers’? Current perspectives on Generation Alpha”, *Psychological Thought*, köt. 15, sz. 1, o. 1, 2022.

[49] B. Boro, R. Laltlanzova, és F. Chanchinmawia, „Examining Digital Literacy Skills Among Gen Z Students of Mizoram University”, *DESIDOC Journal of*

Library & Information Technology, köt. 44, sz. 1, o. 32–36, jan. 2024, doi: 10.14429/djlit.44.1.19291.

[50] M. Yang és A. Salman, „Analysis of correlating factors: Social media addiction in Shanghai's Generation Z", *International Journal of Advanced and Applied Sciences*, köt. 11, sz. 1, 2024, doi: 10.21833/ijaas.2024.01.016.

[51] Y. Yağmur, „An Exploratory Research to Reveal the Habits, Motivations, and Tendencies of Generation Z to Use Social Media Platforms as A Leisure Activity", *Advances in Hospitality and Tourism Research (AHTR)*, köt. 12, sz. 2, o. 172–199, jún. 2024, doi: 10.30519/ahtr.1452356.

[52] R. Singha és Y. Kanna S., „Peer Influence on Students' Online Addiction Behaviors", 2024, o. 1–20. doi: 10.4018/979-8-3693-4191-9.ch001.

[53] M. Jambulingam, J. Francis, és M. Dorasamy, „What is Generation Zs' Preferred Social Media Network?", in *2018 Fourth International Conference on Advances in Computing, Communication & Automation (ICACCA)*, IEEE, 2018, o. 1–4. doi: 10.1109/ICACCAF.2018.8776817.

[54] S. S. Katavić, H. Ivanović, és A. Papić, „Digital privacy and data protection knowledge and skills of university students in Croatia: Preliminary findings", *Education for Information*, köt. 39, sz. 4, o. 493–515, nov. 2023, doi: 10.3233/EFI-230056.

[55] A. R. Albescu és A.-V. Vevera, „Living the phygital era: Generation Alpha is redefining our world", *19th International Conference on Virtual Learning, ICVL 2024*, köt. 19, o. 205–215, 2024.

[56] J. A. Cortés-Quesada és A. Vizcaíno-Verdú, „Swipe, interact, engage: Analysis of generation Alpha's consumer behavior on TikTok", *Revista ICONO 14. Revista científica de Comunicación y Tecnologías emergentes*, köt. 23, sz. 1, febr. 2025, doi: 10.7195/ri14.v23i1.2183.

[57] J. A. Vera és S. Ghosh, „They've Over-Emphasized That One Search: Controlling Unwanted Content on TikTok's For You Page", in *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, ápr. 2025, o. 1–8. doi: 10.1145/3706598.3713666.

[58] J. A. Cortés-Quesada és A. Vizcaíno-Verdú, „Fragmented-brand consumerism on TikTok: The advertising impact on generation Alpha”, *Revista de Comunicación*, köt. 24, sz. 1, o. 109–125, márc. 2025, doi: 10.26441/RC24.1-2025-3659.

[59] P. He és B. Yuan, „On the Information Cocoon Effect in the TikTok Recommendation Algorithm”, in *2024 5th International Conference on Artificial Intelligence and Computer Engineering (ICAICE)*, IEEE, nov. 2024, o. 94–98. doi: 10.1109/ICAICE63571.2024.10863939.

[60] P. Gerbaudo, „TikTok and the algorithmic transformation of social media publics: From social networks to social interest clusters”, *New Media Soc.*, dec. 2024, doi: 10.1177/14614448241304106.

[61] S. Shahidi Hamedani, L. Cheng Siang, M. A. Bashir Elnewiri, G. Babanejaddehaki, és S. Aslam, „The role of attention span in neuromarketing: A social psychological exploration of multi-sensory engagement among generation Z”, *Environment and Social Psychology*, köt. 10, sz. 6, jún. 2025, doi: 10.59429/esp.v10i6.3731.

[62] H. Flavian, „Promoting Social Skills among Generation Alpha Learners with Special Needs”, *Educ. Sci. (Basel).*, köt. 14, sz. 6, o. 619, jún. 2024, doi: 10.3390/educsci14060619.

[63] A. Höfrová, V. Balidemaj, és M. A. Small, „A systematic literature review of education for Generation Alpha”, *Discover Education*, köt. 3, sz. 1, o. 125, 2024.

[64] N. K. Ranganathan, N. Chauhan, S. V., J. W. A., és P. Rajendran, „How Millennial parents guide Generation Alpha in using educational apps”, *Quality Assurance in Education*, jún. 2025, doi: 10.1108/QAE-01-2025-0019.

[65] M. A. Kuhail, J. Mrabet, R. Hijazi, és J. Thomas, „Why Would I Befriend a Bot? Assessing Factors Influencing the Usage of Social Chatbots for Digital Natives”, *Hum. Behav. Emerg. Technol.*, köt. 2025, sz. 1, jan. 2025, doi: 10.1155/hbe2/8825536.

[66] S.-M. Wang, M. A. Yaqin, és F.-H. Hsu, „Improving Emotional Intelligence in the New Normal Using Metaverse Applications for Digital Native”, 2022, o. 527–541. doi: 10.1007/978-3-031-05311-5_37.

[67] K. P. Wong és J. Qin, „Evaluating the Efficacy of Immersive Virtual Learning Programme on Verbal and Nonverbal Interactions in Children with Attention Deficit Hyperactivity Disorder”, 2025, o. 228–238. doi: 10.1007/978-3-031-93851-1_18.

[68] E. E. Soares, K. Bausback, C. L. Beard, M. Higinbotham, E. L. Bunge, és G. W. Gengoux, „Social Skills Training for Autism Spectrum Disorder: a Meta-analysis of In-person and Technological Interventions”, *J. Technol. Behav. Sci.*, köt. 6, sz. 1, o. 166–180, nov. 2020, doi: 10.1007/s41347-020-00177-0.

[69] J. E. Opie *és mtsai.*, „Outcomes of Best-Practice Guided Digital Mental Health Interventions for Youth and Young Adults with Emerging Symptoms: Part I. A Systematic Review of Socioemotional Outcomes and Recommendations”, *Clin. Child Fam. Psychol. Rev.*, köt. 27, sz. 2, o. 424–475, jún. 2024, doi: 10.1007/s10567-024-00469-4.

[70] T. Chen, J. Ou, G. Li, és H. Luo, „Promoting mental health in children and adolescents through digital technology: a systematic review and meta-analysis”, *Front. Psychol.*, köt. 15, márc. 2024, doi: 10.3389/fpsyg.2024.1356554.

[71] I. O. Ukonu és D. J. Warlimont, „Rethinking learning techniques for the digital age”, *Analele Universitatii Ovidius Constanta, Seria Filologie*, köt. 36, sz. 1, o. 641–666, 2025.

[72] A. Gyivicsán, „A Z generáció internethasználati szokásai és az internetfüggőség”, *Módszertani Közlemények*, köt. 63, sz. 1, o. 121–137, ápr. 2023, doi: 10.14232/modszertani.2023.1.121-137.

[73] D. K. Szabó-Prievara és K. Tarkó, „A problémás mértékű internethasználat gyermekek körében”, *Iskolakultúra*, köt. 33, sz. 1–2, o. 77–92, febr. 2023, doi: 10.14232/iskkult.2023.1-2.77.

[74] F. Gioia, V. Rega, és V. Boursier, „Problematic internet use and emotional dysregulation among young people: A literature review”, *Clin. Neuropsychiatry*, köt. 18, sz. 1, o. 41, 2021.

[75] M. Zhou, W. Zhu, X. Sun, és L. Huang, „Internet addiction and child physical and mental health: Evidence from panel dataset in China”, *J. Affect. Disord.*, köt. 309, o. 52–62, 2022.

[76] Y. Theopilus, A. Al Mahmud, H. Davis, és J. R. Octavia, „Preventive Interventions for Internet Addiction in Young Children: Systematic Review”, *JMIR Ment. Health*, köt. 11, o. e56896, 2024, doi: 10.2196/56896.

[77] M. Schmitt és M. D. Schmitt, *iGen: Why Today's Super-Connected Kids are Growing Up Less Rebellious, More Tolerant, Less Happy—and Completely Unprepared for Adulthood: and What That Means for the Rest of Us. By Jean M. Twenge: A Book Review*. 2024.

[78] C. Li, P. Wang, M. Martin-Moratinos, M. Bella-Fernández, és H. Blasco-Fontecilla, „Traditional bullying and cyberbullying in the digital age and its associated mental health problems in children and adolescents: a meta-analysis”, *Eur. Child Adolesc. Psychiatry*, köt. 33, sz. 9, o. 2895–2909, 2024.

[79] N. Nazhifah, O. Handini, M. Putri, Z. A. Siregar, N. Nami, és A. Yenita, „The Role of Guidance and Counseling Teachers in the Prevention of Bullying in the Alpha Generation”, in *BICC Proceedings*, 2024, o. 91–96. doi: 10.30983/bicc.v1i1.110.

[80] E. Bozzola *és mtsai.*, „The use of social media in children and adolescents: Scoping review on the potential risks”, *Int. J. Environ. Res. Public Health*, köt. 19, sz. 16, o. 9960, 2022.

[81] M. Pohl *és mtsai.*, „The Association of Internet Addiction with Burnout, Depression, Insomnia, and Quality of Life among Hungarian High School Teachers”, *Int. J. Environ. Res. Public Health*, köt. 19, sz. 1, o. 438, dec. 2021, doi: 10.3390/ijerph19010438.

[82] A. Lukács, B. Gál, és P. Sasvári, „Problémás internethasználat vizsgálata 10-15 éves általános iskolás tanulóknál”, *Egészségtudományi Közlemények*, köt. 7, sz. 2, o. 21–27, 2017.

[83] H. Kiss és B. Pikó, „A problémás internethasználat összefüggése a magányossággal középiskolás és egyetemi hallgatók körében. ”, *Iskolakultúra*, köt. 27, o. 77–85, 2017.

[84] J. M. Nagata *és mtsai.*, „Social epidemiology of early adolescent problematic screen use in the United States”, *Pediatr. Res.*, köt. 92, sz. 5, o. 1443–1449, nov. 2022, doi: 10.1038/s41390-022-02176-8.

[85] M. Sanchez-Fernandez és M. Borda-Mas, „Problematic smartphone use and specific problematic Internet uses among university students and associated predictive factors: a systematic review”, *Educ. Inf. Technol. (Dordr).*, köt. 28, sz. 6, o. 7111–7204, 2023.

[86] R. Ziatdinov és J. Cilliers, „Generation Alpha: Understanding the next cohort of university students”, *arXiv preprint*, 2022.

[87] B. Moore, S. Woodcock, és S. Kielblock, „How students’ pro-social behaviour relates to their resilience: Implications for an inclusive environment”, *International Journal of Educational Research Open*, köt. 5, o. 100269, dec. 2023, doi: 10.1016/j.ijedro.2023.100269.

[88] B. Pikó és C. Hamvai, „Stressz, coping és reziliencia korai serdülőkorban. ”, *Iskolakultúra*, köt. 22, sz. 9, o. 24–33, 2012.

[89] L. Pölczman *és mtsai.*, „Enhancing resilience: the impact of a near-peer mentoring program on medical students”, *Front. Educ. (Lausanne).*, köt. 9, jan. 2025, doi: 10.3389/feduc.2024.1523310.

[90] M. Rutter, „Psychosocial resilience and protective mechanisms.”, *American Journal of Orthopsychiatry*, köt. 57, sz. 3, o. 316–331, júl. 1987, doi: 10.1111/j.1939-0025.1987.tb03541.x.

[91] N. Garmezy, „Resiliency and Vulnerability to Adverse Developmental Outcomes Associated With Poverty”, *American Behavioral Scientist*, köt. 34, sz. 4, o. 416–430, márc. 1991, doi: 10.1177/0002764291034004003.

[92] U. Bronfenbrenner, „Ecological systems theory.”, in *Encyclopedia of Psychology, Vol. 3.*, New York: Oxford University Press, 2000, o. 129–133. doi: 10.1037/10518-046.

[93] S. S. Luthar, D. Cicchetti, és B. Becker, „The Construct of Resilience: A Critical Evaluation and Guidelines for Future Work”, *Child Dev.*, köt. 71, sz. 3, o. 543–562, máj. 2000, doi: 10.1111/1467-8624.00164.

[94] G. E. Richardson, „The metatheory of resilience and resiliency”, *J. Clin. Psychol.*, köt. 58, sz. 3, o. 307–321, márc. 2002, doi: 10.1002/jclp.10020.

[95] S. Parsons, A.-W. Kruijt, és E. Fox, „A Cognitive Model of Psychological Resilience”, *J. Exp. Psychopathol.*, köt. 7, sz. 3, o. 296–310, nov. 2016, doi: 10.5127/jep.053415.

[96] F. Luthans, M. C. Youssef, és B. J. Avolio, *Psychological capital: Developing the human competitive edge*. Oxford University Press, 2006.

[97] S. S. Tirumala, M. R. Valluri, és G. Babu, „A survey on cybersecurity awareness concerns, practices and conceptual measures”, in *2019 International Conference on Computer Communication and Informatics (ICCCI)*, IEEE, jan. 2019, o. 1–6. doi: 10.1109/ICCCI.2019.8821951.

[98] R. S. Qamaria, D. Kuswandi, N. Setiyowati, és A. M. Bahodirovna, „Digital resilience in adolescence: A systematic review of models, methods and theoretical perspectives”, *Multidisciplinary Reviews*, köt. 8, sz. 9, o. 2025287, márc. 2025, doi: 10.31893/multirev.2025287.

[99] H. Sun, C. Yuan, Q. Qian, S. He, és Q. Luo, „Digital Resilience Among Individuals in School Education Settings: A Concept Analysis Based on a Scoping Review”, *Front. Psychiatry*, köt. 13, márc. 2022, doi: 10.3389/fpsyt.2022.858515.

[100] M. Thinyane és D. Christine, „SMART Citizen Cyber Resilience (SC2R) Ontology”, in *13th International Conference on Security of Information and Networks*, New York, NY, USA: ACM, nov. 2020, o. 1–8. doi: 10.1145/3433174.3433617.

[101] F. Björck, M. Henkel, J. Stirna, és J. Zdravkovic, „Cyber Resilience – Fundamentals for a Definition”, 2015, o. 311–316. doi: 10.1007/978-3-319-16486-1_31.

[102] B. Dupont, C. Shearing, M. Bernier, és R. Leukfeldt, „The tensions of cyber-resilience: From sensemaking to practice”, *Comput. Secur.*, köt. 132, o. 103372, szept. 2023, doi: 10.1016/j.cose.2023.103372.

[103] L. Bognár és L. Bottyán, „Evaluating Online Security Behavior: Development and Validation of a Personal Cybersecurity Awareness Scale for University Students”, *Educ. Sci. (Basel).*, köt. 14, sz. 6, o. 588, máj. 2024, doi: 10.3390/educsci14060588.

[104] I. Arpaci, O. Aslan, és I. E. Oner, „Cybersecurity Awareness Scale (CSAS) for Social Media Users: Development, Validity and Reliability Study”, *Information Development*, ápr. 2025, doi: 10.1177/02666669251336562.

[105] R. Járai, D. Vajda, R. Hargitai, L. Nagy, K. Csókási, és E. C. Kiss, „A Connor–Davidson reziliencia kérdőív 10 itemes változatának jellemzői”, *Alkalmazott pszichológia*, köt. 15, sz. 1, o. 129–136, 2015.

[106] H. Jonkman, M. van Rooijen, M. Wiersma, és R. van Goor, „Validation Study of the Child and Youth Resilience Measure (CYRM-28) Among Dutch Youth”, *Front. Psychiatry*, köt. 13, máj. 2022, doi: 10.3389/fpsyt.2022.637760.

[107] C. Qi és N. Yang, „Digital resilience in Chinese adolescents: a portrayal of the current condition, influencing factors, and improvement strategies”, *Front. Psychiatry*, köt. 15, febr. 2024, doi: 10.3389/fpsyt.2024.1278321.

[108] Eurostat - Statistics Explained, „Young people - digital world”, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Young_people_-_digital_world.

[109] M. Anderson, M. Faverio, és J. Gottfried, „Teens, Social Media and Technology 2023”, https://www.pewresearch.org/internet/2023/12/11/teens-social-media-and-technology-2023.

[110] V. Stavropoulos, F. Motti-Stefanidi, és M. D. Griffiths, „Risks and Opportunities for Youth in the Digital Era”, *Eur. Psychol.*, köt. 27, sz. 2, o. 86–101, ápr. 2022, doi: 10.1027/1016-9040/a000451.

[111] V. Pérez-Torres, „Social media: a digital social mirror for identity development during adolescence”, *Current Psychology*, köt. 43, sz. 26, o. 22170–22180, júl. 2024, doi: 10.1007/s12144-024-05980-z.

[112] A. Evans és K. Luna, „Speaking of Psychology: Stress in America – Generation Z. American Psychological Association.”, https://www.apa.org/news/podcasts/speaking-of-psychology/teen-stress.

[113] J. R. Saura, V. Gelashvili, és J. G. Martínez-Navalón, „The impact of social media on Gen Z’s mental health and privacy”, *Journal of Competitiveness*, márc. 2025, doi: 10.7441/joc.2025.01.11.

[114] The Annie E. Casey Foundation, „The impact of social media and technology on gen alpha.”, https://www.aecf.org/blog/impact-of-social-media-on-gen-alpha.

[115] D. Sutresna, „Decoding Generation Alpha: How the Youngest Digital Natives Use, Think, and Choose. Medium”, https://dsutresna.medium.com/decoding-generation-alpha-how-the-youngest-digital-natives-use-think-and-choose-b8ab81047259.

[116] R. Barr, „Growing Up in the Digital Age: Early Learning and Family Media Ecology”, *Curr. Dir. Psychol. Sci.*, köt. 28, sz. 4, o. 341–346, aug. 2019, doi: 10.1177/0963721419838245.

[117] L. Piccerillo, A. Tescione, A. Iannaccone, és S. Digennaro, „Alpha generation’s social media use: sociocultural influences and emotional intelligence”, *Int. J. Adolesc. Youth*, köt. 30, sz. 1, dec. 2025, doi: 10.1080/02673843.2025.2454992.

[118] N. Mishra, H. Sharma, és R. Garg, „Generational Contrasts: A Comparative Analysis of Resilience, Interpersonal Communication, and Life Values in Gen X and Gen Z ”, *International Journal of All Research Education & Scientific Methods*, köt. 12, sz. 3, o. 943–948, 2024.

[119] S. Smojver-Ažić, S. Bradić, és T. Martinac Dorčić, „Social Media Use”, *Psihologijske teme*, köt. 33, sz. 1, o. 133–154, ápr. 2024, doi: 10.31820/pt.33.1.7.

[120] T. K. Wong és C. A. Hamza, „Online Self-Presentation, Self-Concept Clarity, and Depressive Symptoms: A Within-Person Examination”, *J. Youth Adolesc.*, köt. 54, sz. 4, o. 997–1013, ápr. 2025, doi: 10.1007/s10964-024-02109-0.

[121] A. Acuña *és mtsai.*, „Increased default mode network activation in depression and social anxiety during upward social comparison”, *Soc. Cogn. Affect. Neurosci.*, köt. 20, sz. 1, febr. 2025, doi: 10.1093/scan/nsaf012.

[122] D. Seo, A. Ahluwalia, M. N. Potenza, és R. Sinha, „Gender differences in neural correlates of stress-induced anxiety”, *J. Neurosci. Res.*, köt. 95, sz. 1–2, o. 115–125, jan. 2017, doi: 10.1002/jnr.23926.

[123] N. Extremera, C. Quintana-Orts, N. Sánchez-Álvarez, és L. Rey, „The Role of Cognitive Emotion Regulation Strategies on Problematic Smartphone Use: Comparison between Problematic and Non-Problematic Adolescent Users”, *Int.*

J. Environ. Res. Public Health, köt. 16, sz. 17, o. 3142, aug. 2019, doi: 10.3390/ijerph16173142.

[124] J. D. Elhai, H. Yang, A. E. Dempsey, és C. Montag, „Rumination and negative smartphone use expectancies are associated with greater levels of problematic smartphone use: A latent class analysis", *Psychiatry Res.*, köt. 285, o. 112845, márc. 2020, doi: 10.1016/j.psychres.2020.112845.

[125] R. N. Ramadhan *és mtsai.*, „Impacts of digital social media detox for mental health: A systematic review and meta-analysis", *Narra J*, köt. 4, sz. 2, o. e786, aug. 2024, doi: 10.52225/narra.v4i2.786.

[126] J. M. Twenge és G. N. Martin, „Gender differences in associations between digital media use and psychological well-being: Evidence from three large datasets", *J. Adolesc.*, köt. 79, sz. 1, o. 91–102, febr. 2020, doi: 10.1016/j.adolescence.2019.12.018.

[127] M. M. L. Leijse, I. M. Koning, és R. J. J. M. van den Eijnden, „The influence of parents and peers on adolescents' problematic social media use revealed", *Comput. Human Behav.*, köt. 143, o. 107705, jún. 2023, doi: 10.1016/j.chb.2023.107705.

[128] A. Manole, R. Cârciumaru, R. Brînzaș, és F. Manole, „Harnessing AI in Anxiety Management: A Chatbot-Based Intervention for Personalized Mental Health Support", *Information*, köt. 15, sz. 12, o. 768, dec. 2024, doi: 10.3390/info15120768.

[129] M. Karhiy, M. Sagar, M. Antoni, K. Loveys, és E. Broadbent, „Mindfulness based stress reduction: A randomised trial of a virtual human, teletherapy, and a chatbot", in *2023 11th International Conference on Affective Computing and Intelligent Interaction Workshops and Demos (ACIIW)*, IEEE, szept. 2023, o. 1–7. doi: 10.1109/ACIIW59127.2023.10388195.

[130] J. Park és H.-Y. Kim, „Avatars as Coping Mechanisms for Body Image Inadequacy: A Snapshot of Generation Z Consumers in the Metaverse", *Clothing and Textiles Research Journal*, márc. 2025, doi: 10.1177/0887302X251324578.

[131] L. Yang, Y. Xu, és P. Hui, „Framing metaverse identity: A multidimensional framework for governing digital selves”, *Telecomm. Policy*, köt. 49, sz. 3, o. 102906, ápr. 2025, doi: 10.1016/j.telpol.2025.102906.

[132] A. Tashakkori és C. Teddlie, *SAGE Handbook of Mixed Methods in Social & Behavioral Research*. 2455 Teller Road, Thousand Oaks California 91320 United States : SAGE Publications, Inc., 2010. doi: 10.4135/9781506335193.

[133] KSH, „Népszámlálási adatbázis – Központi Statisztikai Hivatal”, https://nepszamlalas2022.ksh.hu/adatbazis/.

[134] KSH, „22.1.2.1. A lakónépesség nem, vármegye és régió szerint, január 1.”, https://www.ksh.hu/stadat_files/nep/hu/nep0034.html.

[135] Zs. Demetrovics és others, „Presentation of the Problematic Internet Use Questionnaire - A Problémás Internethasználat Kérdőív bemutatása”, *Psychiat Hung*, köt. 19, sz. 2, o. 141–160, 2004.

[136] Zs. Demetrovics és others, „The three-factor model of internet addiction: The development of the Problematic Internet Use Questionnaire”, *Behav. Res. Methods*, köt. 40, o. 563–574, 2008.

[137] K. M. Connor és J. R. T. Davidson, „Development of a new resilience scale: The Connor-Davidson Resilience Scale (CD-RISC)”, *Depress. Anxiety*, köt. 18, sz. 2, o. 76–82, szept. 2003, doi: 10.1002/da.10113.

[138] L. Campbell-Sills és M. B. Stein, „Psychometric analysis and refinement of the connor–davidson resilience scale (CD-RISC): Validation of a 10-item measure of resilience”, *J. Trauma. Stress*, köt. 20, sz. 6, o. 1019–1028, dec. 2007, doi: 10.1002/jts.20271.

[139] National Institute of Standards and Technology, „Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1”, Gaithersburg, MD, ápr. 2018. doi: 10.6028/NIST.CSWP.04162018.

[140] D. B. . Parker, *Fighting computer crime : a new framework for protecting information*. Wiley, 1998.

[141] D. A. Hall *és mtsai.*, „A good practice guide for translating and adapting hearing-related questionnaires for different languages and cultures”, *Int. J. Audiol.*, köt. 57, sz. 3, o. 161–175, márc. 2018, doi: 10.1080/14992027.2017.1393565.

[142] L. Sajtos és A. Mitev, *SPSS Kutatási és adatelemzési kézikönyv*. Budapest: Alinea Kiadó, 2007.

[143] Wim. Janssens, Katrien. Wijnen, P. de. Pelsmacker, és Patrick. Van Kenhove, *Marketing research with SPSS*. [FT Publishing International], 2010.

[144] L. J. Cronbach, „Coefficient Alpha and the Internal Structure of Tests”, *Psychometrika*, köt. 16, sz. 3, o. 297–334, szept. 1951, doi: 10.1007/BF02310555.

[145] S. Carpenter, „Ten Steps in Scale Development and Reporting: A Guide for Researchers”, *Commun. Methods Meas.*, köt. 12, sz. 1, o. 25–44, jan. 2018, doi: 10.1080/19312458.2017.1396583.

[146] J. Rácz, S. Karsai, és V. Tóth, *Kvalitatív pszichológia kézikönyv*. ELTE Eötvös Kiadó, Budapest, 2023. doi: 10.21862/KvalPsziKK/2023/5930.

[147] V. Braun és V. Clarke, „Using thematic analysis in psychology”, *Qual. Res. Psychol.*, köt. 3, sz. 2, o. 77–101, jan. 2006, doi: 10.1191/1478088706qp063oa.

[148] A. Partington és A. Marchi, „Using corpora in discourse analysis”, in *The Cambridge Handbook of English Corpus Linguistics*, Cambridge University Press, 2015, o. 216–234. doi: 10.1017/CBO9781139764377.013.

[149] D. Hooper, J. Coughlan, és M. R. Mullen, „Structural Equation Modelling: Guidelines for Determining Model Fit”, *Electronic Journal of Business Research Methods*, köt. 6, sz. 1, o. 53–60, 2008.

[150] A. Khan, G. Thomas, S. Karatela, A. Morawska, és A. Werner-Seidler, „Intense and problematic social media use and sleep difficulties of adolescents in 40 countries”, *J. Adolesc.*, köt. 96, sz. 5, o. 1116–1125, júl. 2024, doi: 10.1002/jad.12321.

[151] I. Kokka *és mtsai.*, „Exploring the Effects of Problematic Internet Use on Adolescent Sleep: A Systematic Review”, *Int. J. Environ. Res. Public Health*, köt. 18, sz. 2, o. 760, jan. 2021, doi: 10.3390/ijerph18020760.

[152] Y. Kang *és mtsai.*, „Gender differences in response to a school-based mindfulness training intervention for early adolescents”, *J. Sch. Psychol.*, köt. 68, o. 163–176, jún. 2018, doi: 10.1016/j.jsp.2018.03.004.

[153] J. A. Haugan, P. Frostad, és P.-E. Mjaavatn, „Girls suffer: the prevalence and predicting factors of emotional problems among adolescents during upper secondary school in Norway”, *Social Psychology of Education*, köt. 24, sz. 3, o. 609–634, jún. 2021, doi: 10.1007/s11218-021-09626-x.

[154] C. Nobles, „The Cyber Talent Gap and Cybersecurity Professionalizing”, *International Journal of Hyperconnectivity and the Internet of Things*, köt. 2, sz. 1, o. 42–51, 2018, doi: 10.4018/978-1-7998-2466-4.ch004.

[155] C. Berényi és Á. Csiszárik-Kocsir, „A digitális szocializáció hatása a középiskolás fiatalok eszközhasználatára”, *Vállalkozásfejlesztés a XXI. században*, köt. 2023/2, o. 241–254, 2023.

[156] B. Meggyesfalvi, „Kockázati tényezők a digitális térben”, *Belügyi Szemle*, köt. 71, sz. 12, o. 2163–2178, dec. 2023, doi: 10.38146/BSZ.2023.12.3.

[157] D. Szabó és E. Dani, „Smartphones and social media as status symbol of Gen Z”, *Folia Toruniensia*, köt. 22, 2021.

[158] B. B. Budai, „Digitális készségfejlesztés”, https://akademiai.hu/ptudx00468-digitalis-keszsegfejlesztes.html.

A disszertációhoz kapcsolódó saját publikációk

[S-1] J. Módné Takács és M. Pogátsnik, „A systematic review of Human Aspects in Industry 4.0 and 5.0: Cybersecurity Awareness and Soft Skills”, *27th IEEE International Conference on Intelligent Engineering Systems (INES 2023)*, Piscataway, NJ, Amerikai Egyesült Államok: IEEE Hungary Section, o. 33–39, 2023. doi: https://doi.org/10.1109/INES59282.2023.10297768

[S-2] J. Módné Takács és M. Pogátsnik, „Az IR4 és IR5 új kihívásai: puha készségek és kiberbiztonságtudatosság a digitális átalakulás korában: Szisztematikus szakirodalomelemzés”, *Biztonságtudományi Szemle*, köt. 5, sz. 3, o. 23–36, 2023.

[S-3] J. Módné Takács és M. Pogátsnik, „The Presence of Cybersecurity Competencies in the Engineering Education of Generation Z”, *Acta Polytechnica Hungarica*, köt. 21, sz. 6, o. 107–127, 2024. doi: https://doi.org/10.12700/APH.21.6.2024.6.6

[S-4] J. Módné Takács, „The importance and development of safety awareness with soft skills in industrial environment”, *Opus et Educatio: Munka és Nevelés*, köt. 8, sz. 3, o. 314–323, 2021.

[S-5] J. Módné Takács és M. Pogátsnik, „The Importance of Resilience in Engineering Education”, *Recent Advances in Intelligent Engineering*, Cham, Svájc: Springer Nature Switzerland, 2024, o. 291–304, fejezet 16. doi: https://doi.org/10.1007/978-3-031-58257-8_16

[S-6] J. Módné Takács és M. Pogátsnik, „Megküzdési technikák és stressz faktorok feltérképezése a mérnökhallgatók szemszögéből”, *Szakképzés-Pedagógiai Tudományos Közlemények 4. 2023/1*, Budapest, Magyarország: Budapesti Műszaki és Gazdaságtudományi Egyetem, Gazdaság- és Társadalomtudományi Kar, Műszaki Pedagógia Tanszék, o. 113–130, 2023.

[S-7] J. Módné Takács és M. Pogátsnik, „A Comprehensive Study on Cybersecurity Awareness: Adaptation and Validation of a Questionnaire in Hungarian Higher Technical Education”, *Acta Polytechnica Hungarica*, köt. 21, sz. 10, o. 533–552, 2024.

[S-8] J. Módné Takács, N. Tolner és M. Pogátsnik, „Trapped in the Virtual World: The Prevalence of Problematic Internet Use Among Generation Z”, *AIS 2024 – 19th*

International Symposium on Applied Informatics and Related Areas, Székesfehérvár, Magyarország: Óbudai Egyetem, 2024, o. 64–69.

[S-9] J. Módné Takács és M. Pogátsnik, „Screen Natives Becoming Digital Orphans: The Online Challenges of Generation Alpha”, *AIS 2025 - 20th International Symposium on Applied Informatics and Related Areas*, Székesfehérvár, Magyarország: Óbudai Egyetem, 2025, o. 197-202.

[S-10] J. Módné Takács és M. Pogátsnik, „Resilience Profiles of Vulnerable and Unstoppable Youth in Generations Z and Alpha”, *Opus et Educatio: Munka és Nevelés*, köt. 12, sz. 3, o. 271–282, 2025.

[S-11] J. Módné Takács és M. Pogátsnik, „Kiberbiztonsági profilok a Z és Alfa generáció körében”, *Biztonságtudományi Szemle*, köt. 7, sz. 3, o. 15–27, 2025. doi: https://doi.org/10.12700/btsz.2025.7.3.15

[S-12] J. Módné Takács és M. Pogátsnik, „Profiling Cross-Generational Cyber Resilience through Scale Development”, *International Journal of Engineering Pedagogy (iJEP)*, köt. 15, sz. 7, o. 69–84, 2025. doi: https://doi.org/10.3991/ijep.v15i7.58939

A disszertáció témakörén kívüli saját publikációk

[S-13] J. Módné Takács és M. Pogátsnik, „The impact of digital education from a teacher’s perspective”, *15th International Symposium on Applied Informatics and Related Areas organized in the frame of Hungarian Science Festival 2020 (AIS 2020)*, Székesfehérvár, Magyarország: Óbudai Egyetem, o. 6–9, 2020.

[S-14] J. Módné Takács, N. Tolner, G. T. Orosz és M. Pogátsnik, „Modular education framework supported by IT project management methods”, *15th IEEE International Symposium on Applied Computational Intelligence and Informatics (SACI 2021)*, Budapest, Magyarország és Piscataway, NJ, Amerikai Egyesült Államok: Óbudai Egyetem, IEEE, o. 485–490, 2021.

[S-15] M. Pogátsnik és J. Módné Takács, „OPENSEL Project: To establish new open, online courses to develop social emotional skills, in cooperation for innovation and the exchange of good practices”, *Opus et Educatio: Munka és Nevelés*, köt. 8, sz. 3, o. 330–332, 2021. doi: https://doi.org/10.3311/ope.464

[S-16] J. Módné Takács, T. Kersánszki és M. Pogátsnik, „Gamifikáció az online oktatásban, avagy a motiváció fokozása és a puha készségek fejlesztése járvány idején”, *HuCER 2021: Tanuló társadalom. Oktatáskutatás járvány idején = Learning society. Educational research during an epidemic*, Budapest, Magyarország: Magyar Nevelés- és Oktatáskutatók Egyesülete (HERA), o. 11, 2021.

[S-17] J. Módné Takács és M. Pogátsnik, „Az egyetemi hallgatók stresszkezelési technikáinak vizsgálata”, *Módszertani újítások és kutatások a szakképzés és a felsőoktatás területén: X. Trefort Ágoston Szakképzés- és Felsőoktatás-pedagógiai Konferencia Tanulmánykötet*, Budapest, Magyarország: Óbudai Egyetem, o. 262–278, 2021.

[S-18] J. Módné Takács és M. Pogátsnik, „The online learning from the students’ perspective”, *IEEE 19th World Symposium on Applied Machine Intelligence and Informatics (SAMI 2021)*, Budapest, Magyarország: IEEE Hungary Section, o. 27–32, 2021. doi: https://doi.org/10.1109/SAMI50585.2021.9378665

[S-19] J. Módné Takács, N. Tolner és M. Pogátsnik, „Diverse approach of Cybersecurity culture in Education”, *AIS 2021 – 16th International Symposium on Applied Informatics and Related Areas*, Székesfehérvár, Magyarország: Óbudai Egyetem, o. 64–68, 2021.

[S-20] N. Tolner, A. Dávid, J. Módné Takács és M. Pogátsnik, „Online vizsgáztatás a felsőoktatásban oktatói szemmel”, *Oktatás egy változó világban – Kutatás, innováció, fejlesztés: Absztraktfüzet*, Budapest, Magyarország: Budapesti Műszaki és Gazdaságtudományi Egyetem, o. 232–233, 2022.

[S-21] N. Tolner, J. Módné Takács, A. Dávid és M. Pogátsnik, „Online examination from the point of view of teachers”, *AIS 2022 – 17th International Symposium on Applied Informatics and Related Areas*, Székesfehérvár, Magyarország: Óbudai Egyetem, o. 169–173, 2022.

[S-22] J. Módné Takács, M. Pogátsnik és I. Simonics, „Behaviour of students in stressful situations in different cultures”, *ICL 2022 – 25th International Conference on Interactive Collaborative Learning*, Vienna, Ausztria: International Society for Engineering Pedagogy (IGIP), o. 433–444, 2022.

[S-23] J. Módné Takács, M. Pogátsnik és T. Kersánszki, „A gamifikáció, a puha készségek fejlesztésének egyik eszköze”, *Tanuló társadalom: Oktatáskutatás járvány idején*, Budapest és Debrecen, Magyarország: Debreceni Egyetemi Kiadó, Magyar Nevelés- és Oktatáskutatók Egyesülete (HERA), o. 117–137, 2022.

[S-24] J. Módné Takács, M. Pogátsnik és T. Kersánszki, „Improving Soft Skills and Motivation with Gamification in Engineering Education”, *24th International Conference on Interactive Collaborative Learning (ICL 2021)*, Volume 1, Cham, Svájc: Springer Cham, o. 823–834, fejezet 81, 2022. doi: https://doi.org/10.1007/978-3-030-93904-5_81

[S-25] T. Kersánszki, J. de Meester, S. Spikic és J. Módné Takács, „Opportunities for integrated education in STEM”, *Opus et Educatio: Munka és Nevelés*, köt. 9, sz. 2, o. 127–133, 2022. doi: https://doi.org/10.3311/ope.502

[S-26] J. Módné Takács és M. Pogátsnik, „Stress-management skills among Dutch and Hungarian students”, *IEEE 20th Jubilee World Symposium on Applied Machine Intelligence and Informatics (SAMI 2022)*, Poprad, Szlovákia: IEEE, o. 407–411, 2022. doi: https://doi.org/10.1109/SAMI54271.2022.9780731

[S-27] N. Tolner, M. Pogátsnik és J. Módné Takács, „A mesterséges intelligencia szerepe az online vizsgáztatásban”, Iskolakultúra: Pedagógusok szakmai-tudományos folyóirata, köt. 33, sz. 10, o. 39–55, 2023. doi: https://doi.org/10.14232/iskkult.2023.10.39

[S-28] N. Tolner, J. Módné Takács, A. Dávid és M. Pogátsnik, „Vizsgáztatás online felületen az oktatók szemszögéből”, *Oktatás egy változó világban: Kutatás, innováció, fejlesztés*, Budapest és Debrecen, Magyarország: Magyar Nevelés- és Oktatáskutatók Egyesülete (HERA), Debreceni Egyetemi Kiadó, o. 276–291, 2023.

[S-29] N. Tolner, J. Módné Takács, J. Halász, T. Bekk, É. Takács, A. Dávid, C. Bráda, I. P. Csuka és M. Pogátsnik, „Well-being among students in dual and traditional education”, *AIS 2023 – 18th International Symposium on Applied Informatics and Related Areas*, Székesfehérvár, Magyarország: Óbudai Egyetem, o. 159–163, 2023.

[S-30] J. Módné Takács, N. Tolner és M. Pogátsnik, „A mesterséges intelligencia szerepe az online vizsgáztatásban: előnyök és hátrányok a felhasználási lehetőségek szempontjából”, *Az oktatás határdimenziói: Absztraktkötet, Hungarian Conference on Educational Research (HuCER 2023)*, Szombathely, Magyarország: Magyar Nevelés- és Oktatáskutatók Egyesülete (HERA), o. 187, 2023.

[S-31] J. Módné Takács, M. Pogátsnik és I. Simonics, „Students’ Behaviour in Stressful Situations in Diverse Cultures”, 25th International Conference on Interactive Collaborative Learning (ICL 2022), Volume 2, Cham, Svájc: Springer Cham, o. 361–371, fejezet 37, 2023. doi: https://doi.org/10.1007/978-3-031-26190-9_37

[S-32] J. Módné Takács, N. Tolner és M. Pogátsnik, „University teachers' perceptions of AI integration: Insights from a qualitative focus group study”, *Opus et Educatio: Munka és Nevelés*, köt. 10, sz. 3, o. 230–235, 2023.

[S-33] J. Módné Takács, M. Pogátsnik és I. Simonics, „Investigation of Stress Management Among University Students Using the Document Analysis Method”, 26th International Conference on Interactive Collaborative Learning (ICL 2023), Volume 3, Cham, Svájc: Springer Nature Switzerland, o. 338–349, fejezet 35, 2024. doi: https://doi.org/10.1007/978-3-031-53022-7_35

[S-34] M. Mohammed, J. Takács, A. Mosavi, I. Felde és N. Nabipour, „Deep Learning and Machine Learning for Materials Design”, *6th IEEE International Symposium on Logistics and Industrial Informatics (LINDI 2024)*, Piscataway, NJ, Amerikai Egyesült Államok: IEEE, o. 73–82, 2024. doi: https://doi.org/10.1109/LINDI63813.2024.10820388

[S-35] J. Módné Takács, M. Pogátsnik és I. Simonics, „Qualitative Study of Students’ Emotional Responses and Coping Strategies in Relation to Stress in Higher Education”, *in Lecture Notes in Networks and Systems*, köt. 1261, o. 382–393, fejezet 37, 2025. doi: https://doi.org/10.1007/978-3-031-85649-5_37. ISBN: 978-3-031-85648-8.

[S-36] T. Máté és J. Módné Takács, „Sportrendezvények biztonsága”, *Magyar Sporttudományi Szemle*, köt. 26, sz. 114, o. 77–78, 2025.

[S-37] M. Pogatsnik, J. Módné Takács és É. Takács, „Exploring Industry Perspectives on Dual Education”, *AIS 2025 - 20th International Symposium on Applied Informatics and Related Areas*, Székesfehérvár, Magyarország: Óbudai Egyetem, 2025, o. 192-196.

[S-38] T. Máté és J. Módné Takács, „Beyond the Sport: A Holistic Understandig of Safety in the Sports Industry – A Systematic Literature Review”, *Acta Polytechnica Hungarica*, köt. 23, sz. 2, o. 183-202, 2026.

[S-39] J. Módné Takács, T. Máté és N. Tolner, „Development of Cybersecurity Awareness and Soft Skills in Higher Education, Designing Interactive eLearning Curricula”, *Innovation via Collaborative Learning in Engineering Education Proceedings of the 28th International Conference on Interactive Collaborative Learning (ICL2025)*, Volume 2, Springer Nature Switzerland – ***elfogadva, megjelenés alatt***

[S-40] M. Pogátsnik, J. Módné Takács és É. Takács, „A Decade of Practice-Based Engineering Education”, *IEEE 24th World Symposium on Applied Machine Intelligence and Informatics* (SAMI 2026), Piscataway, NJ, Amerikai Egyesült Államok: IEEE, o. 107–111, 2026.

JEGYZÉKEK

Fogalomtár

Alfa generáció: Az Alfa generáció (2010–2024 között születettek) az első teljesen digitális korszakban született nemzedék, akik természetes módon használják az érintőképernyős és okoseszközöket, így életükben az online és offline világ szinte teljesen összemosódik [48].

Digitális detox: A digitális detox a szándékos offline időszakok beiktatása, amely csökkenti a kognitív terhelést és javítja a pszichológiai jóllétet [125].

Digitális reziliencia: A digitális reziliencia az egyének alkalmazkodóképessége a digitális környezet változásaihoz és kockázataihoz, amely során képesek felismerni, kezelni és tanulni az online fenyegetésekből, ezáltal ellenállóbbá válnak [97].

Kiberbiztonság: A kiberbiztonság az adatok, információs rendszerek és hálózatok integritását, bizalmasságát és rendelkezésre állását biztosító védelem folyamatos fenntartása a digitális térben, technikai, stratégiai és nemzetközi intézkedések révén [9].

Kiberbiztonsági tudatosság: A kiberbiztonsági tudatosság a kibertér veszélyeinek ismeretét, az információk megértésének és feldolgozásának képességét, valamint a biztonságos online magatartás gyakorlati alkalmazásának igényét jelenti [32].

Kiberreziliencia: A kiberreziliencia a kiberfenyegetésekre adott proaktív, tanuláson alapuló alkalmazkodás, amely a biztonságos online működés és a kiberbiztonsági kompetenciák fejlesztésének kulcsa [34].

Kibertér: A kibertér egy globális, összekapcsolt digitális ökoszisztéma, ahol emberek, számítógépek és hálózati rendszerek kommunikálnak, adatokat tárolnak és dolgoznak fel egy közös információs környezetben [21].

Phygital élmény: A phygital élmény a fizikai és digitális valóság összefonódását jelenti, ahol az egyén egyszerre van jelen a valós és a virtuális térben, ezáltal új kommunikációs, tanulási és kognitív minták alakulnak ki [55].

Problémás internethasználat: A problémás internethasználat a túlzott vagy kontrollvesztett online tevékenységet jelenti, amely során az egyén nehezen

szabályozza internethasználatát, és ez negatívan befolyásolja az életének más területeit, mint az alvást, a tanulást vagy a társas kapcsolatokat [76], [77].

Reziliencia: A reziliencia az egyén vagy közösség képessége a stressz, kihívások és krízisek hatékony kezelésére, a negatív hatások minimalizálására és a visszaállásra vagy magasabb szintű működésre [90].

Z generáció: A Z generáció (1995–2010 között születettek) az első digitális bennszülött nemzedék, akik számára az online tér az élet természetes közege, a tanulás, a kapcsolattartás és az önkifejezés fő színtere [47].

Rövidítésjegyzék

AI – Artificial Intelligence – Mesterséges Intelligencia

CD-RISC – Connor-Davidson Resilience Scale – Connor-Davidson reziliencia skála

CIA elv – Confidentiality Integrity Availability – Bizalmasság, sértetlenség, rendelkezésre állás

CYRM – Child and Youth Resilience Measurement – Child és Youth reziliencia mérőeszköz

CSA – Cybersecurity Scale – Kiberbiztonsági skála

CS-C-H – Kiberbiztonsági tudatosság kérdőív magyar nyelvű adaptált változata

ENISA – European Union Agency for Cybersecurity – Európai Uniós kiberbiztonsági ügynökség

FOMO – Fear of Missing Out – Kimaradástól való félelem

ISA – Information Security Awareness – Információbiztonsági Tudatosság

KAB modell – Knowledge Attitude Behaviour model – Tudás attitűd viselkedés modell

KSH – Központi Statisztikai Hivatal

NAT – Nemzeti Alaptanterv

PCRS – Personal Cyberresilience Scale – Személyes kiberrezziliencia skála

PIH – Problémás internethasználat

PMT – Protection Motivation Theory – Védelmi motivációs elmélet

PsyCap model – Psychological Capital model – Pszichológiai tőke modell

TPB – Theory of Planned Behaviour – Tervezett viselkedés elmélet

TTAT – Technology Threat Avoidance Theory – Technológiai fenyegetések elkerülésének elmélete

VR – Virtual Reality – Virtuális valóság

Táblázatjegyzék

Ábrajegyzék

MELLÉKLETEK

1. melléklet: Kvantitatív kutatási kérdőívek

1/A. melléklet: Demográfiai adatok

1. Az Ön neme:

o	nő	o	férfi

2. Kérem adja meg a születési évét (pl.1976):

3. Milyen oktatási intézményben végzi a tanulmányait?

o	általános iskola	o	gimnázium
o	középiskola/technikum	o	egyetem

4. A tanulmányokhoz köthető szak/specializáció megnevezése:

o	általános	o	elektronika/villamos
o	matematika	o	nyelv
o	informatika	o	művészet
o	gépészet	o	egyéb

5. Mi az Ön állandó lakhelye?

o	Főváros	o	Város
o	Megyeszékhely	o	Község, falu

6. A szülei legmagasabb iskolai végzettsége (a szülőket együttesen figyelembe véve a magasabbat jelölje meg)?

o	általános iskolai végzettség	o	érettségi
o	szakmunkás végzettség	o	egyetem/főiskola

7. Mennyi az a napi, átlagos idő, melyet internetezéssel tölt el (számítógépen, mobil eszközökön stb. együttesen)?

o	0-1 óra	o	6-7 óra
o	2-3 óra	o	7 óránál több
o	4-5 óra		

1/B. melléklet: Demográfiai adatok jellemzői generációs bontásban

Demográfiai változó	Kategória	Z generáció (*N*=2438)	Alfa generáció (*N*=837)	Teljes minta (*N*=3275)
Nem	lány	1117 (45.8%)	412 (49.2%)	1529 (46.7%)
	fiú	1321 (54.2%)	425 (50.8%)	1746 (53.3%)
Intézmény típusa	általános iskola	532 (21.8%)	684 (81.7%)	1215 (37.1%)
	középiskola	1573 (64.5%)	153 (18.3%)	1726 (52.7%)
	felsőoktatás	334 (13.7%)	0 (0.0%)	334 (10.2%)
Szakirány	általános	661 (27.1%)	667 (79.7%)	1328 (40.5%
	humán	859 (35.2%)	69 (8.3%)	928 (28.3%)
	reál	918 (37.7%)	101 (12.0%)	1019 (31.2%)
Lakhely	község, falu	942 (38.6%)	236 (28.2%)	1178 (36.0%)
	város	937 (38.4%)	283 (33.8%)	1220 (37.3%)
	megyeszékhely	514 (21.1%)	305 (36.4%)	819 (25.0%)
	főváros	45 (1.9%)	13 (1.6%)	58 (1.7%)
Szülők legmagasabb iskolai végzettsége	általános iskola	71 (2.9%)	30 (3.6%)	101 (3.1%)
	szakmunkás	382 (15.7%)	65 (7.8%)	447 (13.6%)
	érettségi	980 (40.2%)	232 (27.7%)	1212 (37.0%)
	egyetem/főiskola	1005 (41.2%)	510 (60.9%)	1515 (46.3%)

Megjegyzés: A minta demográfiai jellemzői generációs bontásban (N = 3275), ahol a százalékos értékek az adott oszlopon belüli megoszlást mutatják, az N a résztvevők számát jelöli.

1/C. melléklet: Problémás Internethasználat kérdőív 6 tételes változata

Az alábbiakban az internet-használatával kapcsolatos állításokat olvashat. Kérjük, jelezze az 1-től 5-ig terjedő skálán, hogy az egyes állítások mennyire jellemzőek Önre! 1 = soha - 2 = ritkán - 3 = néha - 4 = gyakran - 5 = mindig/majdnem mindig

Milyen gyakran…

PIH1. Milyen gyakran érzi úgy, hogy csökkentenie kellene az internetezéssel töltött időt?

PIH2. Milyen gyakran érzi nyugtalannak, feszültnek magát, ha nem internetezhetett annyit, amennyit szeretett volna?

PIH3. Milyen gyakran internetezik olyankor, amikor inkább aludnia kellene?

PIH4. Milyen gyakran próbálja titkolni, hogy mennyi időt töltött internetezéssel?

PIH5. Milyen gyakran panaszkodnak a környezetében lévők arra, hogy túl sokat internetezik?

PIH6. Milyen gyakran fordul elő Önnel, hogy depressziósnak, szomorúnak, idegesnek érzi magát, amikor nem internetezik, és ez az érzés elmúlik, amikor újra internetezni kezd?

1/D. melléklet: Reziliencia kérdőív 10 tételes változata

Kérjük, jelölje meg minden állításnál, hogy milyen mértékben volt jellemző Önre az adott kijelentés az elmúlt hónapban. Válaszlehetőségek: 0 – Egyáltalán nem igaz; 1 – Ritkán igaz; 2 – Néha igaz; 3 – Gyakran igaz; 4 – Szinte mindig igaz.

RISC1. Képes vagyok arra, hogy alkalmazkodjak a változásokhoz.
RISC2. A stresszel való megküzdés megerősít.
RISC3. Mindig a legnagyobb erőbedobással cselekszem, mindegy, hogy miről van szó.
RISC4. Amikor a dolgok reménytelennek tűnnek, akkor sem adom fel.
RISC5. Tisztán gondolkodom és koncentrálok, amikor nyomás alatt vagyok.
RISC6. Erős emberként gondolok magamra.
RISC7. A megérzéseim alapján kell cselekednem.
RISC8. Nagyon céltudatos vagyok.
RISC9. Úgy érzem, én irányítom az életemet.
RISC10. Dolgozom azért, hogy elérjem a céljaimat.

1/E. melléklet: CS-C-H kiberbiztonsági tudatosság mérő kérdőív

Kérjük, jelölje meg minden állításnál, hogy milyen mértékben volt jellemző Önre az adott kijelentés: Válaszlehetőségek: "határozottan nem értek egyet (1)" és a "határozottan egyetértek (5)" között.

CSCH1. Óvatos vagyok a kibertérben megosztott személyes adatokkal kapcsolatban.
CSCH2. Nem osztok meg olyan információkat és dokumentumokat a kibertérben, amelyeket a való életben nem szeretnék megosztani másokkal.
CSCH3. Ügyelek arra, hogy a kibertérben megosztott adataimat csak a megfelelő személyek láthassák.
CSCH4. Nem osztom meg az elérhetőségeimet a kibertérben.
CSCH5. A fiókjaimhoz tartozó jelszavaimat nem osztom meg senkivel.
CSCH6. Jelszavaim létrehozásakor nehezen kitalálható jelszót választok, amely szimbólumokat, számokat és nagybetűket tartalmaz.
CSCH7. Telefonos megerősítési funkciót használok az e-mail jelszavam védelmére.
CSCH8. Megfelelő választ adok a fiókjaim jelszavainak visszaállításához szükséges biztonsági kérdésre.
CSCH9. Nem engedem, hogy a bankkártyám adatait tárolják, miközben a kibertérben vásárolok.
CSCH10. Biztonságos az adatok tárolása a kibertérben.
CSCH11. A kibertérben tárolt információim és dokumentumaim nem vesznek el vagy törlődnek.
CSCH12. Az adatok kibertérben történő megosztása nem jár semmilyen kockázattal.
CSCH13. A kibertérben tárolt információkhoz és dokumentumokhoz nem férhetnek hozzá idegenek.
CSCH14. Ismeretlen személyektől érkező e-mailekben nem bízom.
CSCH15. Nem bízom a biztonsági tanúsítvány nélküli weboldalakban.
CSCH16. Nem nyitom meg az e-mail címemre küldött spam leveleket.
CSCH17. Figyelmen kívül hagyom az e-mail címemre küldött adathalász e-maileket.

CSCH18. Nem nyitok meg ismeretlen forrásból származó linkeket és mellékleteket.

CSCH19. Naprakész vírusirtó programot használok az eszközeimen.

CSCH20. Rendszeresen ellenőrzöm az eszközeimet vírusirtó programmal.

CSCH21. Folyamatosan bekapcsolva tartom az eszközeimre telepített tűzfalat.

CSCH22. Nem nyitom meg az internetről letöltött fájlokat vírusirtó programmal történő ellenőrzés nélkül.

CSCH23. A kibertérben történő információmegosztáshoz közösségi médiaalkalmazásokat használok.

CSCH24. Problémák megoldására igénybe veszem a kibertér szolgáltatásait (például a Google Scholar, a felhőalkalmazások és a közösségi média).

CSCH25. Az információk kezeléséhez (információgyűjtés, -tárolás, -megosztás és -alkalmazás) a kibertérben nyújtott szolgáltatásokat használom.

2. melléklet: Kvalitatív Fókuszcsoportos interjú

2/A. melléklet: Tájékoztató a kutatásban való részvételről

A reziliencia, internethasználati szokások, és kiberbiztonsági tudatosság összefüggéseinek vizsgálata kérdőív

A 21. század digitális fejlődése miatt általánossá vált a kibertér folyamatos használata, mely különféle veszélyeket rejt. Kérdőíves felmérésem abban segítene, hogy vizsgálni tudjam többek között a válaszadók biztonsági és kapcsolódó készségeit, kompetenciáit. A folyamatos változás megköveteli az ezzel való megküzdés készségét, a veszélyeztetett életkörülmények ellenére történő sikeres alkalmazkodást.

A kitöltött kérdőíveket a titkos ügykezelés szabályai szerint kerülnek feldolgozásra. Garantálom egyben a kitöltő személyének névtelenségét.

Köszönöm, hogy figyelmesen és őszintén kitölti a kérdőívet, és ezzel segíti a PhD kutatásomat!

Módné Takács Judit

2/B. melléklet: Beleegyező szülői nyilatkozat mintája

Tisztelt Szülő!

Az Óbudai Egyetem a tanulók kiberbiztonsággal kapcsolatos szokásainak felméréséről végez kutatást. A beszélgetésben szereplő kérdéscsoportok a kiberbiztonság-tudatosság szintjének felmérését célozzák meg az internet használói körében, illetve a reziliencia és a problémás internethasználati szokások hatásának feltérképezését szolgálják a kiberbiztonsági viselkedés aspektusából.

A kötetlen, **anonim beszélgetésről** hangfelvétel készül, amit *az egyetem kizárólag belső használatra készít*. A beszélgetést Módné Takács Judit tanárnő vezeti.

Kérjük szíves hozzájárulását annak érdekében, hogy a kutatásban gyermeke részt vehessen! Együttműködését köszönjük!

Alulírott, (szülő/törvényes képviselő neve) hozzájárulok, hogy ..... nevű gyermekem az Óbudai Egyetem kutatásában részt vegyen.

Székesfehérvár, 2024.09. .....

.....

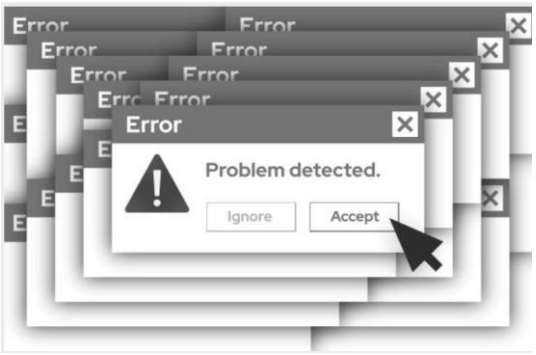
aláírás

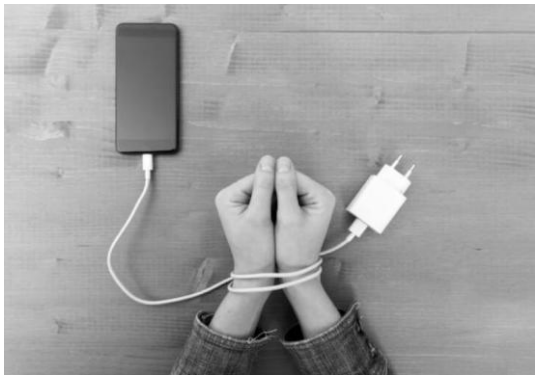
2/C. melléklet: Fókuszcsoport interjú kérdései, vezérfonala

1. Mennyi időt töltesz átlagosan az interneten naponta a telefonon, a számítógépen, a tableten?
2. Milyen típusú tevékenységeket végzel az interneten?
3. Milyen veszélyek lehetnek az online térben?
4. Biztonságban érzitek magatokat az interneten, online játékok, chat alkalmazások, online vásárlás, közösségi média használata közben? Ha igen, hol és miért? Ha nem, hol és miért?
5. Melyek azok a biztonsági beállítások, intézkedések, melyeket alkalmaztok a személyes adataitok, eszközeitek védelme érdekében? Van olyan védekezési mód, amiről hallottál, de nem tudod hogyan kell használni?
6. Milyen helyzetekben fordul elő, hogy tudod, mit kellene tenned a biztonságos internetezés érdekében, de mégsem teszed meg? Miért?
7. Hogyan jellemzed az online fiókjaidhoz használt jelszavaid? Hogyan jegyzed meg őket?
8. Voltál-e már te vagy egy ismerősöd valaha kibertámadás, vagy online átverés áldozata? Mi történt?
9. Mit teszel az üzenetben, smsben, chatben, megosztásban vagy e-mailben megjelenő linkekkel?
10. Mit teszel, ha egy idegen szexuális tartalmú üzenetet/képet küld neked?
11. Hogyan szerzel információt, új híreket az interneten? Mennyire tartod megbízhatónak, amit találsz?
12. Hogyan ismerhető fel a hamis weboldal, e-mail?
13. Mit érzel, ha hosszabb ideig (órákig, napokig) nincs internetelérésed?
14. Volt már veled olyan, hogy nem aludtál eleget, mert inkább interneteztél? Mit csináltál, mivel ütötted el az időt a neten?
15. Volt már, hogy egy online tevékenység, technikai probléma miatt ideges, stresszes lettél? Mondj rá példát!
16. Hogyan érzed magad, ha egy közösségi platformon negatív visszajelzést, kritikát, sértő megjegyzést kapsz, vagy valaki valótlan dolgot ír/tesz ki rólad?
17. Mi az, ami a legjobban aggaszt a kibertérben? Milyen helyzetek okoznak neked stresszt/szorongást az internet használata közben? *(képasszociációs kérdés)*

2/D. melléklet: Képasszociációs anyagok

Válasszátok ki a képek közül, melyek a legjobban jellemzik, leírják a válaszotok. Készítsetek egy képmontázst, majd foglalják össze, hogyan értelmezitek az elkészült montázst.

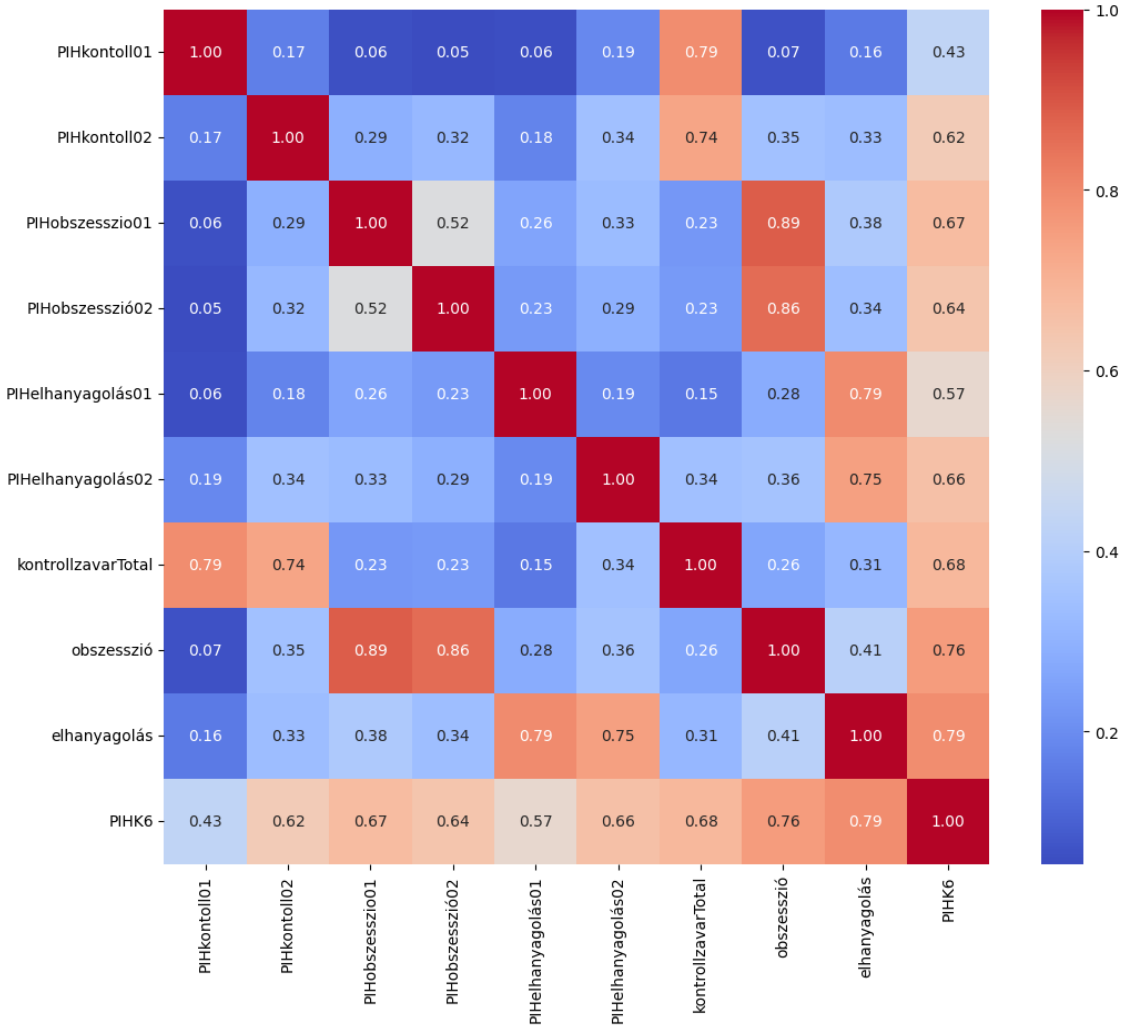




Megjegyzés: A mellékletben feltüntetett képek a kutatásban alkalmazott nagy terjedelmű képhalmaz reprezentatív mintáját képezik. A képek stresszhelyzetekre és online veszélyforrásokra vonatkozó asszociációkat hívnak elő, így például zaklatásra, bántalmazásra, kiközösítésre, félelemkeltésre, álhírekre, pánikkeltésre, online játékra, negatív visszajelzésre, sértő megjegyzésekre, vírusra, támadásra, fenyegetésre, rossz teljesítményre, like-vadászatra, fáradtságra és kimerültségre.

3. melléklet: Statisztikai eredmények

3/A. melléklet: Korrelációs hőtérkép a PIH skála dimenzionális struktúrájához



3/B. melléklet: CS-C-H kérdőív és dimenzióinak belső konzisztenciája

	Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N	Mean	Std. Deviation	N of Items
1. kör Pilot	,772	,788	35	96,13	12,027	25
1. kör Re-test	,836	,828		97,81	11,731	25
2. kör mérés	,858	,866	398	95,61	13,766	25
1. dimenzió - bizalmasság	,790	,802		16,97	3,032	4
2. dimenzió - sértetlenség	,718	,716		11,35	3,698	4
3. dimenzió - elérhetőség	,779	,775		14,03	4,148	4
4. dimenzió - hitelesség	,795	,799		21,18	3,897	5
5. dimenzió - felügyelet	,621	,632		20,53	3,735	5
6. dimenzió - hasznosság	,653	,664		11,56	2,571	3

Megjegyzés: A Pilot és a re-teszt, valamint a másidik körös mérés CS-C-H kérdőív és dimenzióinak belső konzisztenciájának értékelése, pilot és re-test N = 35, második kör N = 398 esetén

3/C. melléklet: A Személyes Kiberreziliencia Skála (PCRS) faktorszerkezete

Faktor	Tétel	Tartalom	Faktortölt.	Cronbach α
1. Proaktív adat- és hozzáférésvédelem	CSCH01	Adatvédelem	.704	.787
	CSCH02	Dokumentumvédelem	.763	
	CSCH03	Hozzáférés-szabályozás	.765	
	CSCH04	Elérhetőség védelem	.720	
	CSCH05	Jelszóbiztonság	.674	
	CSCH06	Erős jelszóalkotás	.457	
	CSCH07	Kétlépcsős hitelesítés	*.354*	
	CSCH08	Kiegészítő azonosítás	.439	
2. Mentális erő és önkontroll	RISC03	Maximális odaadás	.637	.785
	RISC04	Kitartás	.705	
	RISC05	Stressztűrő figyelem	.677	
	RISC06	Magabiztosság	.769	
	RISC08	Célorientáltság	.774	
	RISC09	Én-hatékonyság	.618	
3. Aktív technikai védelem	CSCH19	Vírusvédelem	.852	0.809
	CSCH20	Víruskeresés	.908	
	CSCH21	Tűzfal használat	.688	
	CSCH22	Fájlellenőrzés	.694	
4. Kiberfenyegetés észlelés	CSCH14	E-mail forrás-ellenőrzés	.648	0.776
	CSCH15	Biztonságos URL	.551	
	CSCH16	Spam tartalom kerülése	.751	
	CSCH17	Phising tudatosság	.669	
	CSCH18	Gyanús tartalom kerülése	.682	
5. Online problémamegoldás	CSCH23	Információmegosztás közösségi médián	.686	0.685
	CSCH24	Problémamegoldásra online szolgáltatások	.823	
	CSCH25	Információkeresés	.754	
6. Offline jóllét	PIH_02_rev	Internetidő őszinte kezelése	.813	0.644
	PIH_03_rev	Nyugalom offline állapotban	.798	
	PIH_04_rev	Kiegyensúlyozott offline állapotban	.677	
7. Online adattárolás bizalma	CSCH10	Bizalom az online adattárolásban	.817	0.614
	CSCH11	Adatvesztéstől való védettség érzés	.590	
	CSCH12	Illetéktelen hozzáféréstől való védettség érzése	.802	

Megjegyzés: Az itemek a tartalmuk alapján rövidítve lettek.

4. melléklet: Kvalitatív adatok

4/A. melléklet: Kvalitatív kódolási séma, kódrendszer

Kérdés	Mennyi időt töltesz átlagosan az interneten naponta a telefonon, a számítógépen, a tableten?									
Q01	**Téma**	**Kód**	**Magyarázat**	**Alfa**	férfi	nő	**Z**	férfi	nő	**Összesítve**
	I.Hétköznap (időtartam)	H_idő_alacsony	Kevesebb, mint 3 óra	30%	12%	**41%**	2%	0%	5%	17%
		H_idő_közepes	3-tól 6 óráig (de a 6-ot nem beleértve)	54%	**65%**	48%	40%	23%	57%	**47%**
		H_idő_magas	6 óra vagy annál több	15%	24%	10%	58%	**77%**	38%	36%
	II. Hétvége (időtartam)	HV_idő_alacsony	Kevesebb, mint 3 óra	11%	0%	**17%**	7%	0%	14%	9%
		HV_idő_közepes	3-tól 6 óráig (de a 6-ot nem beleértve)	39%	29%	**45%**	5%	0%	10%	22%
		HV_idő_magas	6 óra vagy annál több	37%	59%	24%	72%	**82%**	62%	**54%**
		HV_idő_nemSpecifikus	Nem ad meg konkrét időtartamot	13%	12%	14%	16%	**18%**	14%	15%
Kérdés	**Milyen típusú tevékenységeket végeztek az interneten?**									
Q02	**Téma**	**Kód**	**Magyarázat**	**Alfa**	férfi	nő	**Z**	férfi	nő	**Összesítve**
	I.Tevékenység típusa	Tev_Médiafogyasztás	Filmek, sorozatok, videók	85%	**88%**	83%	56%	55%	57%	**71%**
		Tev_Játék	Online/offline videojátékok	48%	**76%**	31%	30%	45%	14%	39%
		Tev_Kommunikáció	Chat, üzenetváltás	43%	35%	48%	44%	**45%**	43%	44%
		Tev_KözösségiMédia	Görgetés, profilnézés	35%	18%	**45%**	26%	18%	33%	30%
		Tev_Információszerzés	Keresés tanuláshoz, hobbihoz	11%	12%	10%	16%	**23%**	10%	13%
		Tev_Zenehallgatás	Streaming platformok (pl Spotify)	0%	0%	0%	9%	**14%**	5%	4%
		Tev_Olvasás	Online szöveges tartalmak (könyvek)	11%	6%	**14%**	5%	5%	5%	8%
		Tev_Hobbi	Offline hobbihoz kapcsolódó online tevékenység	11%	6%	**14%**	2%	5%	0%	7%
		Tev_Praktikus	Ügyintézés, vásárlás	4%	12%	0%	9%	**14%**	5%	7%
	II. Felhasználói szerep	Szerep_Tartalomfogyasztó	Passzív néző/hallgató	72%	60%	79%	96%	92%	**100%**	**81%**
		Szerep_Tartalomkészítő	Aktív tartalomlétrehozás és megosztás	28%	**40%**	21%	4%	8%	0%	19%
Kérdés	**Milyen veszélyek lehetnek az online térben?**									
Q3	**Téma**	**Kód**	**Magyarázat**	**Alfa**	férfi	nő	**Z**	férfi	nő	**Összesítve**
	I. Ismert online kockázatok, veszélyek	Vesz_Hacking	Fiókfeltörés	33%	**41%**	28%	9%	9%	10%	21%
		Vesz_Malware	Rosszindulatú szoftver, vírus	24%	**29%**	21%	2%	5%	0%	13%
		Vesz_PénzügyiCsalás	Pénzügyi csalás	13%	12%	14%	40%	**45%**	33%	**26%**
		Vesz_Adathalászat	Phishing	17%	18%	17%	28%	**32%**	24%	22%
		Vesz_SzemélyazonosságLopás	Személyazonosság-lopás	9%	6%	10%	19%	18%	**19%**	13%
		Vesz_Zaklatás	Online zaklatás (cyberbullying)	15%	18%	14%	21%	**23%**	19%	18%
		Vsez_Grooming	Megtévesztés	9%	12%	7%	14%	14%	14%	11%
		Vesz_KéretlenSzexTartalom	Kéretlen szexuális tartalom	7%	**12%**	3%	5%	0%	10%	6%
		Vesz_KéppelValóVisszaélés	Képpel vagy videóval való visszaélés	7%	0%	**10%**	5%	5%	5%	6%
		Vesz_Dezinformáció	Álinformáció	2%	6%	0%	5%	**9%**	0%	3%
		Vesz_MentálisHatás	Negatív mentális hatás	4%	6%	3%	7%	**9%**	5%	6%

		Vesz_Nyomonkövetés	Nyomonkövetés, lokáció megosztása	2%	0%	3%	2%	**5%**	0%	2%
		Vesz_NincsAzonosítva	Nem azonosított	7%	0%	**10%**	2%	5%	0%	4%
Kérdés	**Biztonságban érzitek magatokat az interneten, játékok, chat alkalmazások, vásárlás, közösségi média használata közben? Hol és miért?**									
Q4	**Téma**	**Kód**	**Magyarázat**	**Alfa**	férfi	nő	**Z**	férfi	nő	**Összesítve**
	I.Biztonságérzet	Bizt_Igen	Biztonságban érzi magát	59%	71%	52%	81%	73%	**90%**	**70%**
		Bizt_Nem	Nem érzi magát biztonságban	59%	35%	**72%**	42%	41%	43%	51%
	II. Biztonsági stratégiák ("miért igen" okai)	Strat_PrivátBeállítás	Profilok privátra állítása, láthatóság korlátozása	15%	6%	21%	26%	9%	**43%**	20%
		Strat_Körültekintés	Tudatos ellenőrzés, megbízhatósági vizsgálat	28%	47%	17%	35%	**41%**	29%	**31%**
		Strat_TechnikaiVédelem	2FA, vírusirtó, virtuális fiókok használata	9%	18%	3%	30%	**41%**	19%	19%
		Strat_Tartózkodás	Platformhasználat korlátozása, posztolás kerülése	11%	12%	10%	28%	**32%**	24%	19%
		Strat_MentálisVédelem	Negatív kommentek ignorálása	0%	0%	0%	7%	5%	**10%**	3%
	III. Főbb kockázati aggodalmak ("miért nem" okai)	Agg_Minden	Általános bizalmatlanság, semmi nem biztonságos	24%	18%	**28%**	14%	14%	14%	19%
		Agg_AdatlopásFélelem	Személyes/pénzügyi adatok ellopása	24%	12%	**31%**	19%	27%	10%	**21%**
		Agg_KameraLekövetés	Megfigyelés, adatgyűjtés félelem	9%	6%	**10%**	0%	0%	0%	4%
		Agg_SzociálisKockázat	Kamuprofilok, beszélgetésekkel visszaélés	11%	6%	**14%**	5%	5%	5%	8%
		Agg_OnlineJátékToxicitás	Zaklatás, szexizmus játékokban	0%	0%	0%	2%	**5%**	0%	1%
	IV. Kockázati kontextus (hol a legnagyobb a kockázat)	Kon_OnlineVásárlás	Ismeretlen oldalakon történő fizetés	2%	0%	3%	40%	**41%**	38%	20%
		Kon_KözösségiMédia	Facebook, Instagram, TikTok kockázatai	17%	6%	24%	26%	14%	**38%**	**21%**
		Kon_IsmeretlenOldal	Gyanús weboldalak, idegennyelvű források	17%	**24%**	14%	5%	9%	0%	11%
		Kon_OnlineJáték	Online játékok/szerverek, letöltések	11%	18%	7%	14%	**18%**	10%	12%
Kérdés	**Melyek azok a biztonsági beállítások, intézkedések, melyeket alkalmaztok a személyes adataitok, eszközeitek védelme érdekében? Van olyan védekezési mód, amiről hallottál, de nem tudod hogyan kell használni?**									
Q5	**Téma**	**Kód**	**Magyarázat**	**Alfa**	férfi	nő	**Z**	férfi	nő	**Összesítve**
	I. Alkalmazott védekezési módok (használatban)	Véd_JelszóKód	Erős, változatos jelszavak, PIN	30%	35%	28%	47%	**50%**	43%	38%
		Véd_2FA	Kétfaktoros hitelesítés (SMS, email, app)	9%	6%	10%	79%	**86%**	71%	**43%**
		Véd_Biometria	Ujjlenyomat, FaceID, arcfelismerés	7%	0%	10%	21%	**27%**	14%	13%
		Véd_AdatKorlátozás	Privát beállítás, adatmegosztás minimalizálása	28%	18%	**34%**	16%	5%	29%	22%
		Véd_Körültekintés	Gyanús oldalak/linkek kerülése	30%	**41%**	24%	7%	5%	10%	19%
		Véd_Vírusirtó	Külön szoftver vagy beépített védelem	50%	**65%**	41%	14%	9%	19%	33%
		Véd_TechnikaiEgyéb	Virtuális kártya, tranzakció-értesítés, célprofilok	4%	6%	3%	21%	**23%**	19%	12%
		Véd_SzülőiKontroll	Felügyeleti szoftver, jóváhagyás kérés	11%	0%	**17%**	2%	0%	5%	7%
	II. Ismert, de nem használt védekezési módok	NemHaszn_VPN	VPN ismerete van, de nem használja	2%	6%	0%	9%	**14%**	5%	**6%**
		NemHaszn_JelszóVariálás	Tudja hogy kellene, de nehéz megjegyezni	0%	0%	0%	0%	0%	0%	0%
		NemHaszn_JelszóKezelő	Szinkronizálási/nehézségek miatt nem alkalmazza	2%	6%	0%	5%	**9%**	0%	3%
		NemHaszn_Mentés	Adatok biztonsági mentés külső meghajtó/felhő	0%	0%	0%	2%	**5%**	0%	1%
	III. Tudás/alk. hiánya	Hiány_NincsKonkrét	Nem tud megnevezni//nem használ védekezést	20%	18%	**21%**	16%	14%	19%	**18%**
Kérdés	**Milyen helyzetekben fordul elő, hogy tudod, mit kellene tenned a biztonságos internetezés érdekében, de mégsem teszed meg? Miért?**									
Q6	**Téma**	**Kód**	**Magyarázat**	**Alfa**	férfi	nő	**Z**	férfi	nő	**Összesítve**
	I. A biztonsági szabályok megsértésének okai	Ok_KényelemLustaság	Biztonsági lépések elhagyása kényelem/sürgetés	11%	18%	7%	19%	**36%**	0%	15%
		Ok_Kíváncsiság	Figyelmeztetések ellenére tartalom megtekintése	7%	0%	10%	23%	**27%**	19%	15%
		Ok_PénzügyiElőny	Biztonság feladása megtakarítás érdekében	9%	18%	3%	14%	**18%**	10%	11%

		Ok_KözösségiNyomás	Elvárások követése, mások utánozása	4%	0%	7%	9%	5%	**14%**	7%
		Ok_FigyelmenKívül	Figyelmeztetések, engedélyek (sütik) hanyag elfogadása	26%	24%	28%	28%	**36%**	19%	**27%**
	II. A szabálysértés konkrét tevékenységi területei	Tev_IllegálisTartalom	Torrentezés, nem legális letöltések	9%	12%	7%	26%	**27%**	24%	**17%**
		Tev_OnlineVásárlás	Gyanús webáruházak ellenőrzés nélküli használata	2%	0%	3%	23%	14%	**33%**	12%
		Tev_OnlineJáték	Nem biztonságos letöltések, vírusvédelem kikapcsolása	15%	**24%**	10%	14%	18%	10%	15%
		Tev_KözösségiMédia	Gyakori posztolás, ismeretlenekkel való kommunikáció	11%	6%	**14%**	7%	9%	5%	9%
		Tev_WeboldalEllenőrzésHiány	Gyanús oldalak látogatása ellenőrzés nélkül	11%	0%	17%	14%	**18%**	10%	12%
	III. Szabálysértés nincs	Nincs_Nincs	Nem fordul elő ilyen helyzet	37%	**53%**	28%	12%	0%	24%	**25%**
		Nincs_NemTud/Ismer	Nem ismeri fel a veszélyt, nem releváns	7%	6%	**7%**	5%	5%	5%	6%
Kérdés	**Hogyan jellemzed az online fiókjaidhoz használt jelszavaid? Hogyan jegyzed meg őket?**									
Q7	**Téma**	**Kód**	**Magyarázat**	**Alfa**	férfi	nő	**Z**	férfi	nő	**Összesítve**
	I. Jelszó Jellemzők és Erősség	Jelszó_Egyszerű	Rövid, könnyen megjegyezhető, minimális komplexitás	30%	41%	24%	40%	**45%**	33%	35%
		Jelszó_Erős	Hosszú, vegyes karakterek (betű, szám, speciális)	26%	24%	28%	37%	**41%**	33%	31%
		Jelszó_Személyes	Személyes adatokhoz kötődik (név, dátum)	30%	18%	**38%**	30%	18%	**43%**	30%
		Jelszó_Variált	Különböző jelszavak fiókokhoz	43%	53%	38%	67%	55%	**81%**	**55%**
		Jelszó_Ugyanaz	Ugyanaz a jelszó több/minden fiókhoz	46%	35%	**52%**	28%	36%	19%	37%
	II. Jelszó Memorizálás és Tárolás	Mem_Fejben	Memorizálás tárolóeszköz nélkül	46%	65%	34%	60%	**82%**	38%	**53%**
		Mem_Papíralap	Füzet, cetli, elrejtve	35%	**35%**	34%	28%	14%	43%	31%
		Mem_DigitJegyzet	Telefon jegyzettömb, fájlok	20%	6%	**28%**	19%	9%	29%	19%
		Mem_Technológia	Jelszókezelő, jelszógenerátor	4%	0%	7%	19%	18%	**19%**	11%
		Mem_SzülőiSegítség	Szülő/rokon kezeli általában papíralapon	11%	6%	**14%**	0%	0%	0%	6%
Kérdés	**Voltál-e már te vagy egy ismerősöd valaha kibertámadás, vagy online átverés áldozata? Mi történt?**									
Q8	**Téma**	**Kód**	**Magyarázat**	**Alfa**	férfi	nő	**Z**	férfi	nő	**Összesítve**
	I. Érintettség (Ki az áldozat?)	Érint_Saját	Maga a válaszadó az áldozat	43%	**65%**	31%	37%	41%	33%	**40%**
		Érint_Család	Családtag (szülő, testvér, rokon) az áldozat	26%	29%	24%	28%	18%	**38%**	27%
		Érint_Ismerős	Barát, osztálytárs az áldozat	15%	0%	24%	35%	**41%**	29%	25%
		Érint_Nincs	Nem tud ilyen esetről a környezetében	22%	12%	**28%**	16%	14%	19%	19%
	II. Incidens típusa (Mi történt?)	Inc_PénzügyiCsalás	Pénz/banki adatok ellopása, hamis webshop	35%	41%	31%	40%	32%	**48%**	**37%**
		Inc_Fiókfeltörés	Közösségi média account/email/játék fiók ellopása	20%	24%	17%	51%	**55%**	48%	35%
		Inc_Zaklatás/Cyberbullying	Online bántalmazás, képpel való visszaélés, kiközösítés	24%	**29%**	21%	21%	23%	19%	22%
		Inc_Adathalászat/Scam	Phishing kísérletek, hamis nyeremények	26%	29%	24%	33%	**36%**	29%	29%
		Inc_Malware/Vírus	Vírusos fertőzés, zsarolóvírus	13%	**24%**	7%	5%	9%	0%	9%
	III. Hatás és reakció (következmény)	Hatás_ÉrzelmiReakció	Intenzív érzelmi reakció (sokk, sírás, düh, ijedtség)	17%	18%	17%	12%	14%	10%	15%
		Hatás_MentálisTeher	Paranoia, hosszú távú pszichológiai/mentális hatás	9%	**12%**	7%	0%	0%	0%	4%
		Hatás_AnyagiKár	Pénzösszeg elvesztése	15%	12%	17%	28%	**32%**	24%	21%
		Hatás_Tudatosulás	Tanulás, óvatosabbá válás, biztonsági lépések	24%	35%	17%	26%	23%	**29%**	**25%**
		Hatás_SikeresVédekezés	Támadás felismerése, kár elkerülése	24%	24%	24%	19%	18%	19%	21%
Kérdés	**Mit teszel az üzenetben, smsben, chatben, megosztásban vagy e-mailben megjelenő linkekkel?**									
Q9	**Téma**	**Kód**	**Magyarázat**	**Alfa**	férfi	nő	**Z**	férfi	nő	**Összesítve**
	I. Biztonságtudatos viselkedés	Strat_Ellenőrzés	Link/feladó előzetes vizsgálata (URL, HTTPS, helyesírás)	33%	35%	31%	42%	**50%**	33%	37%
		Strat_Visszakérdez	Feladó megerősítése	17%	12%	**21%**	9%	9%	10%	13%

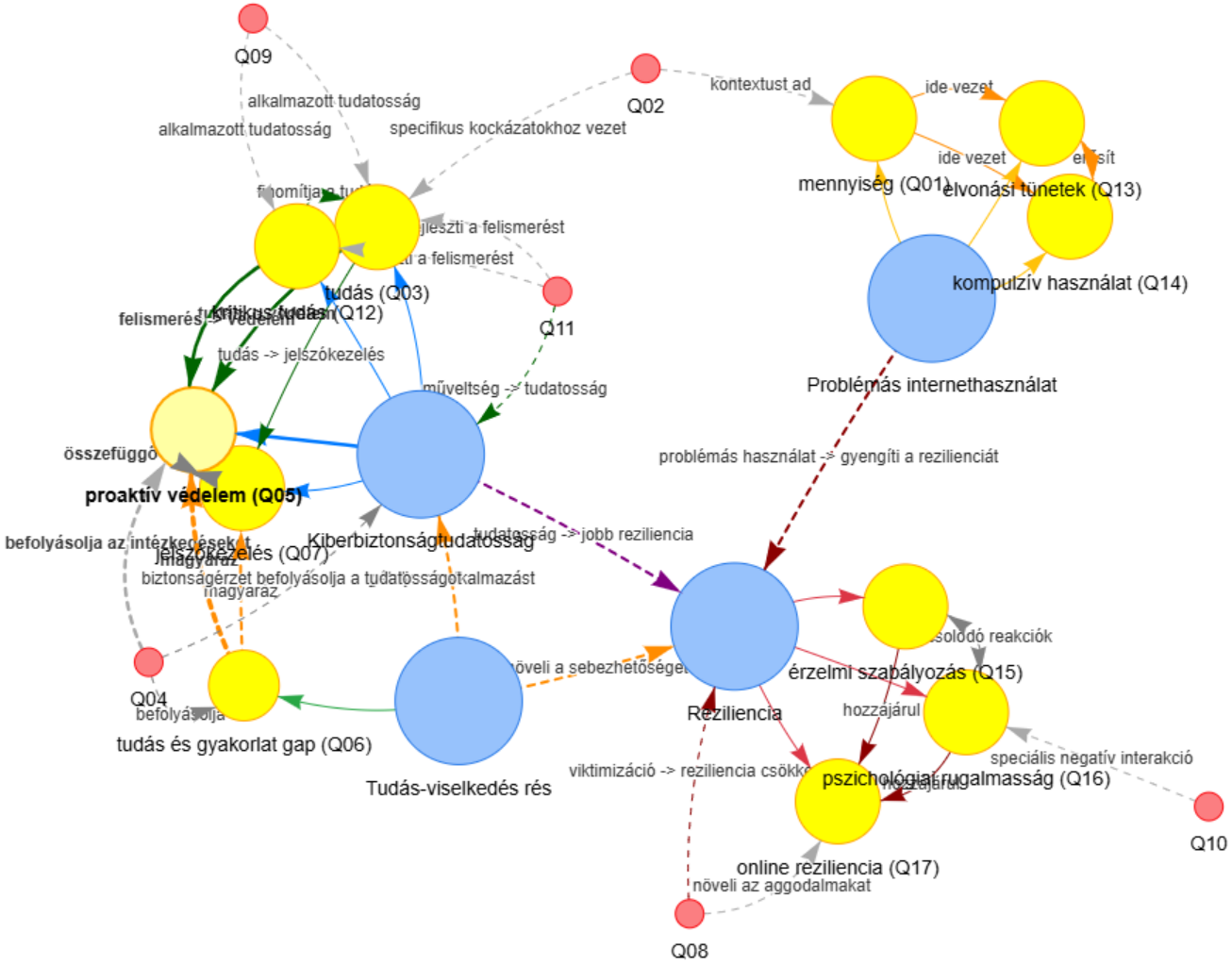
		Strat_Törlés/Tiltás	Gyanús üzenetek törlése, feladó blokkolása	46%	24%	59%	70%	64%	**76%**	**57%**
		Strat_Segítségkérés	Szülő/szakember bevonása	4%	0%	**7%**	2%	0%	5%	3%
		Strat_Technikai	Védőeszközök használata (virtuális gép, adblocker)	2%	0%	3%	2%	5%	0%	2%
	II. A Viselkedést befolyásoló tényezők (döntési alap)	Dönt_Feladó	Ismerős/megbízható személytől/intézménytől származik	41%	**47%**	38%	35%	32%	38%	**38%**
		Dönt_Tartalom	Vicces, érdekes témát ígér	4%	6%	3%	12%	5%	**19%**	8%
		Dönt_Gyanú	Gyanús felépítés (külföldi szám, rövidített link)	11%	18%	7%	26%	**36%**	14%	18%
		Dönt_Tevékenység	Online tevékenységhez kapcsolódik (vásárlás, csomag)	2%	0%	3%	12%	**18%**	5%	7%
	III. Nem biztonságtudatos viselkedés	NemBizt_Rákattintás	Gyanús linkek megnyitása a kockázat ellenére	24%	**41%**	14%	16%	18%	14%	**20%**
		NemBizt_Nemtörődöm	Figyelmen kívül hagyás, ellenőrzés nélküli bezárás	7%	**12%**	3%	7%	**9%**	5%	7%
Kérdés	**Mit teszel, ha egy idegen szexuális tartalmú üzenetet/képet küld neked?**									
Q10	**Téma**	**Kód**	**Magyarázat**	**Alfa**	férfi	nő	**Z**	férfi	nő	**Összesítve**
	I. Közvetlen reakció (cselekvés és jelentés)	Reak_TiltásTörlés	Feladó letiltása, üzenet törlése, ignorálás	76%	82%	72%	86%	86%	86%	**81%**
		Reak_Jelentés	Platform/rendőrségi jelentés	13%	18%	10%	14%	**23%**	5%	13%
		Reak_VerbálisKonfrontáció	Feladó kiosztása, konfliktus letiltás előtt	9%	6%	**10%**	7%	9%	5%	8%
		Reak_Megnéz	Tartalom megnyitása kíváncsiságból	15%	**18%**	14%	14%	23%	5%	15%
		Reak_Dokumentálás	Képernyőfotó készítése bizonyítékként	4%	0%	7%	0%	0%	0%	2%
	II. Segítségkérés és tudatosság	Segít_FelnőttBevonás	Szülő/szakértő bevonása, tanács kérése	28%	12%	**38%**	16%	5%	29%	**22%**
		Segít_Titkolás	Elhallgatás a felnőttek előtt	9%	18%	3%	16%	**27%**	5%	12%
	III. Attitűd és érzelmi kezelés	Att_Tudatosság	Éber, tudatos, azonnali reakció	9%	6%	10%	12%	9%	**14%**	10%
		Att_Nemtörődöm	Humor, jelentéktelenség érzés, elfedés	4%	12%	0%	16%	**18%**	14%	10%
Kérdés	**Hogyan szerzel információt, új híreket az interneten? Mennyire tartod megbízhatónak, amit találsz?**									
Q11	**Téma**	**Kód**	**Magyarázat**	**Alfa**	férfi	nő	**Z**	férfi	nő	**Összesítve**
	I. Információforrások	Forrás_Kereső/Portál	Google, hírportálok, online média	78%	76%	79%	84%	**86%**	81%	**81%**
		Forrás_SocialMedia	TikTok, Instagram, Facebook-csoportok	9%	12%	7%	16%	9%	**24%**	12%
		Forrás_Szakmai/Akadémiai	Szakmai, oktatási és hivatalos források, szakember	11%	6%	14%	12%	9%	**14%**	11%
		Forrás_AI/Chatbot	Generatív AI (ChatGPT, Gemini)	15%	24%	10%	16%	**23%**	10%	16%
		Forrás_KözösségiFórum	Reddit, Quora, szakmai blogok	7%	0%	10%	16%	**23%**	10%	11%
		Forrás_Személyes/Off	Család, barátok, nyomtatott sajtó	33%	12%	**45%**	19%	14%	24%	26%
	II. Ellenőrzési stratégiák	Strat_TöbbForrás	Több oldal összehasonlítása	26%	12%	34%	72%	**73%**	71%	**48%**
		Strat_Hitelesség	Forrás minőségének vizsgálata (helyesírás, logika)	13%	24%	7%	26%	**32%**	19%	19%
		Strat_VideóMegbízhatóság	Vizuális, videós tartalom alátámasztás preferálása	4%	6%	3%	9%	**14%**	5%	7%
	III. Megbízhatóságba vetett hit	Hit_Magas	Alapvetően megbízhatónak tartja	65%	65%	**66%**	33%	27%	38%	**49%**
		Hit_Alacsony	Alapvetően nem bízik benne	2%	**6%**	0%	2%	**5%**	0%	2%
		Hit_Bizonytalan	Forrás/téma függő, kritikus megközelítés	26%	18%	31%	49%	**55%**	43%	37%
Kérdés	**Hogyan ismerhető fel a hamis weboldal, e-mail?**									
Q12	**Téma**	**Kód**	**Magyarázat**	**Alfa**	férfi	nő	**Z**	férfi	nő	**Összesítve**
	I. Vizuális és tartalmi jelek	Fel_Nyelv/Design	Nyelvtani hiba, igénytelen felépítés, túl sok reklám	41%	41%	41%	67%	64%	**71%**	**54%**
		Fel_ManipulatívTartalom	Sürgetés, irreális ígéretek, érzelmi nyomás	30%	29%	**31%**	30%	23%	**38%**	30%
	II. Technikai és azonosítási jelek	Fel_Link/Cím	Gyanús URL/email, elírások, nem hivatalos domain	43%	65%	31%	44%	41%	**48%**	**44%**
		Fel_TechnikaiVédelem	HTTPS hiánya, vírusirtó/böngésző figyelmeztetés	7%	12%	3%	23%	**27%**	19%	15%

		Fel_HiányzóAdat	Cégjegyzék, elérhetőség, lábléc hiánya	0%	0%	0%	12%	9%	**14%**	6%
	III. Tudás hiánya	Hiány_NincsTudás	Nem tudja felismerni, bizonytalan	15%	6%	**21%**	7%	9%	5%	**11%**
Kérdés	**Mit érzel, ha hosszabb ideig (órákig, napokig) nincs internetelérésed?**									
Q13	**Téma**	**Kód**	**Magyarázat**	**Alfa**	férfi	nő	**Z**	férfi	nő	**Összesítve**
	I. Negatív kötődés és érzelmi reakció	Neg_Pánik/Idegesség	Azonnali erős negatív érzelem (frusztráció, harag)	48%	53%	45%	51%	50%	**52%**	**49%**
		Neg_ElvonásiTünet	Fizikai tünetek, függőségi viselkedés (remegés)	9%	6%	10%	12%	5%	**19%**	10%
		Neg_KimaradásFélelem	FOMO, lemaradás érzése, elszigetelődés	9%	6%	10%	30%	**36%**	24%	19%
		Neg_Kapcsolattartás	Kommunikáció nehézsége barátokkal, családdal	35%	29%	38%	53%	50%	**57%**	44%
		Neg_ZavartRutin	Mindennapi tevékenységek akadályozása	11%	18%	7%	51%	41%	**62%**	30%
	II. Pozitív kötődés és kompenzáció	Poz_Felszabadulás	Öröm, megkönnyebbülés, detox érzés	9%	6%	10%	19%	**27%**	10%	13%
		Poz_Kompenzáció	Offline tevékenységekkel való helyettesítés	28%	**35%**	24%	12%	23%	0%	**20%**
		Poz_Alkalmazkodás	Hozzászokás, beletörődés, kontextusfüggő reakció	11%	6%	14%	16%	14%	**19%**	13%
Kérdés	**Volt már veled olyan, hogy nem aludtál eleget, mert inkább interneteztél? Mit csináltál, mivel ütötted el az időt a neten?**									
Q14	**Téma**	**Kód**	**Magyarázat**	**Alfa**	férfi	nő	**Z**	férfi	nő	**Összesítve**
	I. Alváshiány gyakorisága és kiterjedtsége	Gyak_Rendszeres	Szinte minden nap előfordul	52%	65%	45%	70%	64%	**76%**	**61%**
		Gyak_Ritka/Kivételes	Ritkán, egyedi események, specifikus helyzetek	28%	24%	**31%**	19%	32%	5%	24%
		Gyak_NemÉrint	Soha nem fordult elő vagy szülői kontroll meggátolja	20%	12%	**24%**	12%	5%	19%	16%
		Gyak_TudatosKontroll	Leszokás (múltban volt), tudatos korlátozás	0%	0%	0%	9%	**18%**	0%	4%
	II. Tevékenységi típusok	Tev_Tartalomfogyasztás	Passzív tartalomfogyasztás, videók, TikTok pörgetés	54%	65%	48%	56%	50%	**62%**	**55%**
		Tev_Játék	Videójáték, kihívás/érdeklődés/továbbjutás miatt	22%	47%	7%	28%	**45%**	10%	25%
		Tev_Kommunikáció	Közösségi média/chat, barátokkal beszélgetés	22%	18%	24%	30%	27%	**33%**	26%
		Tev_Egyéb	Tanulás, kutatás, tartalomgyártás	9%	0%	14%	14%	**18%**	10%	11%
	III. A fentmaradás belső indítéka	Indít_Érdeklődés	Kíváncsiság, lekötöttség, szórakozás vágya	13%	12%	14%	21%	**23%**	19%	**17%**
		Indít_Unalom/Alvászavar	Elalvás nehézsége, unalom	20%	**24%**	17%	9%	9%	10%	15%
		Indít_SzülőiKontroll	Szülői felügyelet hiánya/kijátszása	17%	**18%**	17%	0%	0%	0%	9%
Kérdés	**Volt már, hogy egy online tevékenység, technikai probléma miatt ideges, stresszes lettél? Mondj rá példát!**									
Q15	**Téma**	**Kód**	**Magyarázat**	**Alfa**	férfi	nő	**Z**	férfi	nő	**Összesítve**
	I. Kiváltó okok (a probléma természete)	Ok_Technikai/Rendszerhiba	Internet lassúság, eszköz lefagyás, szoftverhiba	72%	59%	79%	77%	64%	**90%**	**74%**
		Ok_JátékKudarc	Vesztés, alacsony teljesítmény, cél el nem érése	28%	47%	17%	30%	**55%**	5%	29%
		Ok_Tartalom	Reklámok, sorozat félbeszakadás, nem várt befejezés	13%	0%	**21%**	0%	0%	0%	7%
		Ok_Szociális	Együttműködés hiánya, kommunikációs problémák	13%	0%	**21%**	2%	5%	0%	8%
	II. Érzelmi reakció és stresszkezelés	Reak_DühTombolás	Ordibálás, kiabálás, káromkodás	28%	**35%**	24%	26%	45%	5%	27%
		Reak_Frusztráció	Idegesség, stressz, bepánikolás	65%	53%	**72%**	63%	45%	81%	**64%**
		Reak_Testi	Düh, stressz testi megnyilvánulása (vérnyomás, kéz ökölbe)	4%	6%	3%	5%	**9%**	0%	4%
		Reak_Elfojtás	Düh befelé fordítása, nem mutatja ki	2%	**6%**	0%	0%	0%	0%	1%
		Reak_TudatosKezelés	Konstruktív megoldáskeresés (mély levegő, váltás)	2%	6%	0%	12%	5%	**19%**	7%
	III. A Feszültség levezetési módja (hol adja ki)	Kiad_Rongálás	Tárgyak törése-zúzása	24%	**35%**	17%	23%	45%	0%	**24%**
		Kiad_Befelé	Belső őrlődés, alvászavar	7%	18%	0%	9%	9%	**10%**	8%
		Kiad_JátékbanMásokFelé	Trollkodás, kilépés, verbális agresszió	0%	0%	0%	12%	**18%**	5%	6%
	IV. Nincs érintettség	Nincs_Érintettség	Nem volt még ilyen	7%	6%	7%	12%	**14%**	10%	**9%**
Kérdés	**Hogyan érzed magad, ha egy közösségi platformon negatív visszajelzést, kritikát, sértő megjegyzést kapsz, vagy valaki valótlan dolgot ír/tesz ki rólad?**									

	Téma	Kód	Magyarázat	Alfa	férfi	nő	Z	férfi	nő	Összesítve
Q16	I. Érzelmi reakció és szubjektív érintettség	Reak_DühTombolás	Erős harag, felháborodás, hangos megnyilvánulás	15%	12%	17%	16%	5%	**29%**	16%
		Reak_Szomorúság/Pánik	Kínos/rossz érzés, szomorúság, lelki megviseltség	30%	18%	38%	33%	23%	**43%**	**31%**
		Reak_Ignore	Nem veszi magára, nem érdekli	26%	29%	24%	33%	**45%**	19%	29%
		Reak_HumorElfojtás	Humorral palástolja, valódi érzések elfedése	13%	**18%**	10%	9%	5%	14%	11%
	II. Megküzdési stratégiák	Strat_Konfrontáció	Verbális visszatámadás, veszekedés, bosszú	39%	**59%**	28%	28%	18%	38%	**34%**
		Strat_KülsőEllenőrzés	Valóságtartalom ellenőrzése (szülők/személyes beszélgetés)	28%	12%	**38%**	7%	0%	14%	18%
		Strat_Törlés/Tiltás	Blokkolás, saját tartalom eltávolítása	15%	24%	10%	19%	14%	**24%**	17%
		Strat_ÉpítőKritika	Kritika elfogadása, valóságtartalom átgondolása	4%	6%	3%	23%	**32%**	14%	13%
	III. Reakciót befolyásoló tényező	Bef_Ismerőstől	Barát/család támadása jobban érinti	26%	**29%**	24%	16%	5%	29%	**21%**
		Bef_Tartalom	Negatív reakció kontextusa (valótlan állítás/fénykép hatása)	20%	**24%**	17%	12%	9%	14%	16%
Kérdés	**Mi az, ami a legjobban aggaszt a kibertérben? Milyen helyzetek okoznak neked stresszt/szorongást az internet használata közben?**									
Q17	**Téma**	**Kód**	**Magyarázat**	**Alfa**	férfi	nő	**Z**	férfi	nő	**Összesítve**
	I. Aggodalmak (online veszélyek)	Agg_Adat/Pénzügy	Adatlopás, jelszavak, bankkártya adatokkal visszaélés	48%	41%	52%	77%	73%	**81%**	62%
		Agg_Zaklatás/Tartalom	Bántalmazás, hamis tartalom, valóság torzulása	83%	76%	**86%**	74%	82%	67%	**79%**
		Agg_Megfigyelés	Állandó lekövetés, kamerák/mikrofonok adatgyűjtés	15%	24%	10%	28%	**41%**	14%	21%
		Agg_AI/Deepfake	Mesterséges intelligencia technológia gyors fejlődése	4%	0%	7%	5%	0%	**10%**	4%
	II. Aggodalmak (belső/társadalmi)	Agg_Függőség/Szoc	Túlzott használat, elszigetelődés, kapcsolatok hiánya	46%	41%	48%	56%	**64%**	48%	**51%**
		Agg_Mentális/Önkép	Szorongás, önbizalom hiány, mentális jóllét problémák	28%	29%	28%	44%	**45%**	43%	36%
		Agg_Játék	Játékbeli problémák érzelmi hatása	11%	18%	7%	21%	**27%**	14%	16%
	III. Érzelmi reakciók kifejezése	Reak_Pánik/Szorongás	Erős, kifejezett félelem, pánik, ijedtség, szorongás	24%	18%	**28%**	19%	14%	24%	21%
		Reak_DühTombolás	Erős düh, fizikai vagy verbális kitörésben nyilvánul meg	9%	**18%**	3%	5%	9%	0%	7%
		Reak_Frusztráció/Idegesség	Bosszúság, tehetetlenség, frusztráció	37%	41%	34%	77%	73%	**81%**	**56%**
		Reak_BelsőÖrlődés	Befelé fordított stressz, csendes szenvedés, önkontroll	2%	**6%**	0%	0%	0%	0%	1%

Megjegyzés: A mintában összesen N = 89 fő vett részt, akik közül N = 43 fő a Z generációhoz, N = 46 fő pedig az Alfa generációhoz tartozott. A Z generációs résztvevők nemek szerinti megoszlása N = 22 férfi és N = 21 nő, míg az Alfa generációban N = 17 férfi és N = 29 nő szerepelt. A táblázatban feltüntetett százalékos adatok a relatív gyakoriságot mutatja, amelyek számításának alapját az egyes alcsoportok elemszáma képezte, vagyis külön-külön a generációs hovatartozás, valamint az azon belüli nemi kategóriák szerint. Az induktív tematikus tartalomelemzés háromlépcsős kódolási eljárása során a válaszadók több tartalmi kategóriát is megjelölhettek, következésképpen az egy alcsoportra vonatkozó százalékos értékek összege meghaladhatja a 100 százalékot.

4/B. melléklet: Tematikus térkép



5. melléklet

Kutatási kérdés	Hipotézis	Státusz	Módszertan	Statisztikai eljárás	Főbb eredmények	Tézis	Kapcsolódó publikáció
K1: Milyen különbségek, összefüggések és ok-okozati kapcsolatok figyelhetők meg a Z és Alfa generációk kiberbiztonsági tudatossága, rezilienciája és problémás internethasználata között, valamint hogyan befolyásolják ezeket a mintázatokat a demográfiai tényezők?	–	–	Kérdőíves felmérés, PIU skála; RISC reziliencia skála; CS-C-H kiberbiztonsági tudatosság kérdőív; demográfiai adatfelvétel	Moderált mediációs elemzés, útelemzés	Problémás internethasználat csökkenti a kiberbiztonsági tudatosságot közvetlenül ($b = -0{,}167$; $p = 0{,}009$) és indirekt módon reziliencián keresztül ($b = -0{,}327$; 95% CI [-0,395; -0,263]); a reziliencia csökkentése ($b = -0{,}384$; $p < 0{,}001$) a tudatosságot erősen pozitívan prediktálja ($b = 0{,}851$; $p < 0{,}001$)	**T1:** A problémás internethasználat közvetlenül és a reziliencia csökkentésén keresztül rontja a kiberbiztonsági tudatosságot, a hatás generációtól független, csak a nem moderálja	[S-12]
	H1: A napi internethasználati idő és a problémás internethasználat közötti összefüggés erőssége szignifikánsan eltér nemek és generációs hovatartozás szerint	**Igazolt**		Lineáris regresszió, moderációs regresszió elemzés	Napi internethasználat legerősebb prediktora a problémás internethasználatnak ($b = 1{,}18$; $p < 0{,}001$, $R^2 = 0{,}103–0{,}123$); nőknél erősebb kapcsolat ($b = 0{,}67$), Alfa generációban erősebb hatás ($b = 2{,}25$)	**T2:** A napi internethasználati idő és a problémás internethasználat közötti pozitív kapcsolat erősebb a nők és az Alfa generáció körében	[S-8], [S-9]
	H2: A reziliencia szintje szignifikáns különbségeket mutat a generációs hovatartozás és a nemek függvényében	**Igazolt**		klaszteranalízis, Mann–Whitney U-próba, Khi²-próba, Cramer's V	Alfa generáció alacsonyabb reziliencia ($U = 923181$, $z = -4{,}119$, $p < 0{,}001$), Z generáció magasabb; fiúk magasabb reziliencia ($U = 1148668$, $z = -6{,}902$, $p < 0{,}001$); rezilienciaprofilok eloszlása szignifikánsan összefügg generációval ($\chi^2(2)=16{,}415$, $p<0{,}001$) és nemekkel ($\chi^2(2)=55{,}949$, $p<0{,}001$)	**T3:** Az Alfa generáció és a lányok csoportja szignifikánsan alacsonyabb reziliencia szinttel jellemezhető a Z generációhoz és a fiúkhoz képest.	[S-10]
	H3: A kiberbiztonsági tudatosság szintje szignifikáns eltéréseket mutat az internethasználat ideje, a nemek és a generációs hovatartozás függvényében	**Igazolt**		Spearman-korreláció, lineáris regresszió, multinomiális logisztikus regresszió	Negatív korreláció az internethasználat és kiberbiztonsági tudatosság között: adatvédelem ($r_s=-0{,}233$, $p<0{,}001$), jelszóhasználat ($r_s=-0{,}126$, $p<0{,}001$), ismeretlen források kerülése ($r_s=-0{,}108$, $p=0{,}002$); Alfa generáció alacsonyabb tudatosság, nők nagyobb kockázatészlelés, férfiak magasabb technikai tudatosság ($OR=1{,}81$; $p<0{,}001$)	**T4:** Az internethasználat idejének növekedése szignifikánsan csökkenti a kiberbiztonsági tudatosság szintjét, különösen az Alfa generáció körében, továbbá a nemek eltérő kockázatészlelési és technikai mintázatokkal jellemezhetők, a nők óvatosabb viselkedést, a férfiak magasabb technikai védekezési tudatosságot mutatnak..	[S-3], [S-7], [S-11]

Kutatási kérdés	Hipotézis	Státusz	Módszertan	Statisztikai eljárás	Főbb eredmények	Tézis	Kapcsolódó publikáció
K2: Milyen online helyzetek okoznak leggyakrabban szorongást vagy bizonytalanságot, és hogyan kezelik ezeket?			Kvalitatív vizsgálat, fókuszcsoport beszélgetés	Tematikus tartalomelemzés, induktív kódolás, témakategóriák azonosítása	Technikai problémák, negatív visszajelzések, online zaklatás és adatbiztonsági fenyegetések váltják ki a szorongást; Alfa generáció lányait impulzívabb reakciók, Z generációt fejlettebb önszabályozás jellemez	**T5:** Az online szorongást elsősorban technikai problémák, negatív visszajelzések, valamint az online zaklatás és adatbiztonsági fenyegetések váltják ki, az Alfa generáció lányai impulzívabb reakciókat mutatnak, míg a Z generáció fejlettebb önszabályozással jellemezhetők.	[S-6], [S-10]
K3: Hogyan jellemezhetők a Z és Alfa generációs internetezők kiberreziliencia-profiljai, és milyen szignifikáns különbségek mutatkoznak ezen profilok és a kiberreziliencia aldimenziói mentén?	**H4:** A kiberbiztonsági tudatosság, pszichológiai reziliencia és problémás internethasználat alapján szignifikánsan elkülönülő kiberreziliencia-profilok azonosíthatók	**Igazolt**	Kérdőíves felmérés, kiberreziliencia skála és aldimenziói, demográfiai adatok (generáció, nem)	Klaszteranalízis, Varianciaanalízis (ANOVA),	Négy jól elkülönülő klaszter; „passzív, mentálisan sérülékeny problémamegoldók” (21,7%), „óvatos navigálók” (31,6%), „magas kockázatú sérülékenyek” (15,9%), „magas rezilienciájú, proaktív és tudatosak” (30,7%); szignifikáns különbségek minden fő dimenzió mentén ($p \leq 0{,}001$), legerősebb eltérés a pszichológiai reziliencia (mentális erő, önkontroll) esetében ($F = 49{,}47$).	**T6:** A kiberbiztonsági tudatosság, pszichológiai reziliencia és problémás internethasználat mentén négy, egymástól szignifikánsan elkülönülő kiberreziliencia-profil azonosítható.	[S-12]
	H5: Az Alfa generáció tagjai szignifikánsan eltérő kiberreziliencia profilt mutatnak a Z generációhoz képest	**Igazolt**	Kérdőíves felmérés	Khi²-próba, Mann–Whitney U-próba	Alfa generáció: technológiacentrikus, magas bizalom, alacsonyabb mentális erő és önkontroll; Z generáció: hibrid, adaptív profil; $\chi^2(3)=11{,}07$, $p=0{,}011$.	**T7:** A kiberreziliencia-profilok eloszlása és aldimenziói szignifikánsan eltérnek a generációk között, ahol a Z generáció hibrid, adaptív kiberreziliencia-modellt, míg az Alfa generáció technológiacentrikus, alacsonyabb belső erőforrásokra épülő mintázatot követ, ami eltérő sérülékenységi és alkalmazkodási mechanizmusokat eredményez.	[S-12]

Megjegyzés: A hipotézisek vizsgálati módszerei, statisztikai eljárásai, kulcseredményei és téziskapcsolatai, valamint a kapcsolódó publikációk

KÖSZÖNETNYILVÁNÍTÁS

Mindenekelőtt szeretnék köszönetet mondani Dr. habil. Pogátsnik Monikának, témavezetőmnek, aki fáradhatatlan szakmai iránymutatásával, értékes észrevételeivel, kitartásával és bátorító szavaival mindvégig támogatta munkámat. Szakmai példamutatásából komoly erőt meríthettem az elmúlt évek közös munkája során, a kutatás nehezebb szakaszaiban, és nélküle nem sikerült volna ezt a disszertációt befejeznem.

Hálával tartozom családomnak, férjemnek és gyermekeimnek a türelmükért és folyamatos támogatásukért. A kutatómunka különösen az iskolai szünetekben jelentett számukra megterhelést, sok esetben lemondással is járt, amelyet türelemmel, szeretettel és megértéssel viseltek.

Köszönettel tartozom a doktori képzésben közreműködő oktatóimnak az átadott tudásért és szakmai tapasztalatokért, melyeket megosztottak. Külön köszönöm a féléves beszámolókat értékelő oktatóimnak a kutatási fázisokban nyújtott segítségüket és hasznos tanácsaikat, amelyek hozzájárultak a munka előrehaladásához.

Köszönöm Hronyecz Erikának és Lévay Katalinnak az adminisztratív feladatokban való közreműködésüket és folyamatos segítségüket, különösen a határidők betartásában.

Hálás vagyok a kutatásban részt vevő iskoláknak, pedagógusoknak, hallgatóknak, gyermekeknek és szüleiknek, akik időt és energiát fordítottak az empirikus kutatás megvalósítására. Köszönöm továbbá mindazoknak a kutatóknak, akiknek munkája hozzájárult dolgozatom elméleti alapjainak kialakításához.

Végül köszönöm kollégáimnak és barátaimnak, hogy mindvégig mellettem álltak a kutatómunka hosszú évei alatt, folyamatos szakmai és emberi támogatásukkal segítettek.