ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉSTERVEZET

ZÁHONYI LAJOS

Általános iskolás korú fiatalok információbiztonságának vizsgálata az újpesti „DigiÓ” kutatás tükrében

Témavezető: Dr. Szűcs Endre

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2025 szeptember 18.

TARTALOMJEGYZÉK

BEVEZETÉS

Tudományos probléma megfogalmazása és aktualitása

Az Egyesült Nemzetek Gyermekalapja (United Nations International Children's Emergency Fund továbbiakban: UNICEF) megállapítása szerint világszerte gyermekek milliói töltenek egyre több időt az interneten. A digitális környezet számos előnyt biztosít számukra: javítja a hozzáférést a magas színvonalú és inkluzív oktatáshoz – ideértve a távoktatást és a mobil tanulást is – valamint bővíti az információhoz való hozzáférés lehetőségét. Ugyanakkor a fokozott online jelenlét kockázatokat is hordoz, hiszen a félretájékoztatás, a szexuális kizsákmányolás, az online zaklatás és erőszak, valamint a mentális egészségügyi problémák egyaránt veszélyeztethetik a gyermekek biztonságát, egészségét és jogaik érvényesülését [1].

A jövő alakulását meghatározza, hogy a fiatalabb generáció milyen környezeti és szocializációs hatások között nevelkedik. Az alábbiak szerint fogalmaz Péterfalvi Attila a Nemzeti Adatvédelmi és Információszabadság Hatóság (továbbiakban: NAIH) elnöke: „A személyes adatok védelme egyfelől mindenkit megillet – kortól függetlenül –, másfelől a digitális eszközhasználat korhatára egyre jobban csúszik lefelé" [2, p. 1]. Mindez arra utal, hogy a gyermekek különösen sérülékeny csoportot képeznek az online térben, ahol az eszközhasználat gyakran nem párosul megfelelő tudatossággal.

A digitális generáció sajátossága, hogy együtt nő fel az eszközökkel, ám a technikai hozzáférés önmagában nem biztosítja a biztonságos és felelős használatot. A fiatalok nagy száma és az eszközök széles körű elterjedtsége miatt az információbiztonság és az adatvédelem kérdése nemcsak egyéni, hanem intézményi és társadalmi szinten is egyre sürgetőbb feladat. A tudományos probléma abban ragadható meg, hogyan biztosítható a gyermekek védelme egy olyan digitális környezetben, amely egyszerre kínál fejlődési lehetőségeket és hordoz veszélyeket, miközben a kitettséget a szülők eszközhasználathoz való hozzáállása, a gyermekek életkora és iskolai évfolyama, az okostelefonhoz jutás ideje, a pedagógusok felkészültsége, valamint az állami és intézményi támogatás egyaránt alakítja.

Célkitűzések

A kutatás elméleti megalapozásához elengedhetetlen annak a társadalmi és digitális környezetnek az alapos feltérképezése, amelyben az általános iskolás korú gyermekek mindennapjaikat élik. Disszertációmban olyan összetett jelenségeket vizsgálok, amelyek egyszerre érintenek gyermekeket, szülőket, pedagógusokat és a szabályozói oldalt. A célom az volt, hogy a kutatás tényleges célkitűzéseit olyan tudományos és gyakorlati összefüggésbe helyezzem, amely egyaránt megalapozza az empirikus vizsgálatot és a későbbi következtetések levonását is.

Az információbiztonság kérdésköre az elmúlt évtizedekben alapjaiban változtatta meg a gyermekkort. A digitális eszközökkel való egyre korábbi találkozás, a közösségi média aktív használata, valamint az iskolai környezet fokozatos digitalizációja olyan kihívásokat teremt, amelyekkel a gyermekeknek, a szülőknek és a pedagógusoknak egyaránt szembe kell nézniük. Ez a komplexitás ugyanakkor új kutatási módszereket eredményez – olyanokat, amelyek egyszerre veszik figyelembe a különböző szereplők eltérő tapasztalatait, attitűdjeit és felkészültségét.

A gyermekek jelenléte a digitális térben ma már nem kérdés, hanem tény. Ugyanakkor e jelenlét nem mentes a kockázatoktól: a zaklatás, a manipuláció, a biztonsági események, az adatvédelmi incidensek vagy épp a nem megfelelő tartalmakkal való találkozás mindennapossá váltak. A kihívásokkal való szembesülés képessége – vagy annak hiánya – nagymértékben függ attól, milyen kontrollmechanizmusokat képesek a gyermekek működtetni és milyen tudással, mintával, támogatással rendelkeznek a környezetükből.

A gyermekek mellett lévő szülők digitális nevelési stratégiái sokfélék lehetnek. Vannak, akik aktívan kommunikálnak a biztonságról, mások inkább a technológiai tiltásokra építenek. A kutatásomban ezeket a különböző megközelítéseket vizsgálom meg. Vajon a kommunikáció jellege, időzítése vagy összefüggése hatással van a szereplőkre? Vajon csökkenti-e a kockázatot a gyakori kommunikáció vagy épp azok a gyermekek szenvednek el több online incidenst, ahol a szülők napi szinten foglalkoznak a témával?

Kutatásomban megvizsgálom továbbá a pedagógusok szerepét, mint azon közvetítő kulcsfontosságú szereplőkét, akik napi szinten kapcsolatban állnak a gyerekekkel és hatással lehetnek azok információbiztonsági tudatosságának fejlesztésére. Vajon ők hogyan értékelik saját felkészültségüket? Elégtelennek érzik-e vagy kellő magabiztossággal rendelkeznek ahhoz, hogy tanítványaikkal beszéljenek erről. Igényelnek-e támogatást és ha igen akkor milyen jellegű támogatást tartanának hasznosnak. Önállóan hasznosítható oktatási eszközöket vagy inkább intézményi szintű vagy jogi támogatást tartanának-e szükségesnek?

Az információbiztonság összetett keretrendszerében nem csupán a gyermek–szülő–pedagógus hármas együttműködése bír jelentőséggel, hanem a szabályozási környezet és az állami szerepvállalás is meghatározó szerepet játszik a fiatalok védelmének biztosításában. Az iskolai rendszerben egyre erőteljesebben jelenik meg a digitális átállás, ugyanakkor a felkészítés és a megelőző tevékenységek sok esetben esetlegesek és nem épülnek szilárd, rendszerszintű alapokra. E körülmények vezettek el kutatásom célkitűzéseinek megfogalmazásához, amelyek az alábbiak:

C1: Megvizsgálni, hogy befolyásolja-e a gyermek érintettsége a szülők állami segítség iránti igényét az információbiztonsági kihívásokkal kapcsolatban?

C2: Megvizsgálni, hogy befolyásolja-e a szülők rendszeres biztonságról való kommunikációja a gyermekek információbiztonsági tudatosságát és védelmét, illetve van-e valamilyen hatással a szülők általi közösségi média használat korlátozás, valamint az első saját okostelefon átadásának időpontja, a gyermekek digitális események általi érintettségében?

C3: Megvizsgálni, hogy milyen összefüggés van a gyermekek iskolai osztálya és az információbiztonsági kockázatok mértéke között és hogyan változik a gyermekek kontrollképessége az információbiztonsági kockázatokkal szemben az iskolai osztályok előrehaladtával?

C4: Megvizsgálni, hogy mit gondolnak a különböző generációjú szülők arról, hogy mikor van az ideális életkor arra, hogy a gyermekek okostelefont kapjanak és hogyan viszonyul ez a valóságban történt időponthoz képest?

C5: Megvizsgálni azt, hogy a pedagógusok felkészültnek tartják-e magukat az információbiztonságról való tudásátadásra és befolyásolja-e a pedagógusok saját információbiztonsági felkészültségének megítélése a felkészüléshez és oktatáshoz szükséges támogatási igényeiket? Milyen támogatási formákat tartanak szükségesnek azok a pedagógusok, akik úgy érzik, hogy nem elég felkészültek az információbiztonsági oktatásra?

A téma kutatásának hipotézisei

Az alábbiakban megfogalmazott hipotézisek a kutatás központi kérdéseit és feltételezéseit tükrözik, amelyek a DigiÓ kutatás keretében nyert adatokkal empirikusan vizsgálhatók. E hipotézisek mentén válik lehetővé annak feltárása, hogy milyen kapcsolat áll fenn a gyermekek információbiztonsági kitettsége, a szülői attitűdök és magatartásminták, valamint a pedagógusok felkészültsége és támogatásigénye között.

Hipotézisek:

H1: Feltételezem, hogy azon szülők esetében, ahol gyermekük valamilyen információbiztonsági eseménnyel érintett volt ott nagyobb arányban várják az államtól a segítséget, illetve az állam feladatának is tekintik a felvilágosítást vagy megelőzést.

H2: Feltételezésem szerint a szülők digitális eszközhasználathoz való hozzáállása meghatározza, hogy a gyermekek milyen mértékben válnak érintetté a digitális térben előforduló események által.

H3: Feltételezem, hogy az általános iskolás korú gyermekek információbiztonsági kockázatokkal szembeni védettsége és kontrollképessége összefügg az iskolai osztályukkal.

H4: Feltételezem, hogy a szülők által ideálisnak tartott életkor, amikor a gyermekek okostelefont kapnak, eltér attól az életkortól, amikor valójában megkapják azt és ez a különbség a szülők generációja szerint változik.

H5: Feltételezem, hogy azok a pedagógusok, akik kevésbé érzik magukat felkészültnek az információbiztonsági oktatásra, nagyobb mértékben igénylik a jogi segítségnyújtást és az állandó, belső támogatást nyújtó szakemberek jelenlétét, mint a magabiztosabb pedagógusok.

Kutatási módszerek

A fenti hipotézisek vizsgálatához kevert kutatásmódszertani megközelítést alkalmaztam, amely a kvalitatív és kvantitatív eljárások ötvözésére épült, biztosítva ezzel a kérdéskör komplex megközelítését. Az elméleti kereteket szakirodalmi áttekintés alapozta meg, majd megfigyelések és interjúk révén feltáró jellegű kvalitatív vizsgálatot végeztem. Ezt követte a DigiÓ program keretében megvalósított kérdőíves adatfelvétel és annak statisztikai elemzése, amely empirikus alapot nyújtott a kutatás központi kérdéseinek megválaszolásához. Az eredmények érvényességét és megbízhatóságát szakértői interjúk segítségével ellenőriztem, miközben a trianguláció módszerével a gyermekek, szülők és pedagógusok nézőpontjainak összevetésével árnyaltam a kutatás következtetéseit.

Ez a módszer lehetővé tette számomra, hogy egyszerre használjam ki a kvalitatív vizsgálatok feltáró jellegét és a kvantitatív elemzések számszerűsíthető, általánosítható eredményeit. A kétféle adatgyűjtés nemcsak párhuzamosan, hanem szekvenciálisan is kapcsolódhatott egymáshoz. [3, pp. 95-96] Meggyőződésem, hogy a különböző típusú adatok összehangolása nemcsak gazdagabb értelmezést tett lehetővé, hanem hozzájárult a kutatás érvényességének és megbízhatóságának megerősítéséhez is.

A kutatásom egymásra épülő szakaszokból áll, amelyek célja az általános iskolás korú gyermekek információbiztonsági kihívásainak vizsgálata. A kutatásom során alkalmazott módszerek kombinációja biztosította, hogy a kutatási eredményeim megbízhatóbbak és alaposabbak legyenek.

A kutatás lezárása

A kutatási folyamat 2025. szeptember 18-án fejeződött be, amely a vizsgálat hivatalos lezárásának időpontja.

1 A KUTATÁS ELMÉLETI ÉS KONTEXTUÁLIS MEGALAPOZÁSA

A digitális térben megjelenő információbiztonsági kihívások nem csupán technikai jellegű problémákat jelentenek, hanem mélyen összefonódnak a biztonságtudomány alapvető kérdéseivel is. Különösen igaz ez akkor, amikor kiskorúakról, általános iskolás gyermekekről van szó, akik különösen sérülékeny szereplői az online környezetnek. A biztonságtudományi megközelítésből Berek Lajos az Óbudai Egyetem kutatóprofesszora által meghatározottakat vettem alapul. „A biztonságtudomány szempontjából a személy léte és a szervezetek rendeltetésszerű működése a veszélyeztetett és ami veszélyezteti az a szándékos jogellenes magatartás, cselekmény. Így a biztonságtudomány szempontjából a biztonság valakinek a léte, vagy valaminek a rendeltetésszerű működése és az azt veszélyeztető szándékos jogellenes magatartások együtthatása.” [4, p. 6] Ez az értelmezés különösen releváns a gyermekek információbiztonsága szempontjából, hiszen az ő digitális jelenlétük során számos olyan szándékos és jogellenes cselekmény fordulhat elő, amely veszélyezteti mind az online identitásukat, mind mentális és érzelmi jólétüket.

Mivel kutatásom egy összetett, több tudományterületet is érintő kérdésre – az általános iskolás gyermekek információbiztonsági kihívásaira – irányul, alapvetőnek tartottam a szakirodalmi források áttekintését és a fogalmi keretek pontosítását. E fejezetben a kutatás módszertanát, valamint a fogalmi és értelmezési hátteret mutatom be.

1.1 Az információbiztonság szakirodalmi, elméleti és szabályozási alapjai

A szakirodalmi áttekintésem célja, hogy bemutassam azokat az elméleti kereteket, amelyekre az értekezésem épül. Ebben a fejezetben feltárom az információbiztonság fogalmának kérdéskörét, történeti fejlődését, valamint áttekintettem azokat a legfontosabb elméleteket és kutatásokat, amelyek a gyermekek digitális eszközhasználatát és a kapcsolódó kockázatokat vizsgálják. A szakirodalmi áttekintés keretében az alábbi kutatási tevékenységeket végeztem el:

- Megvizsgáltam az információbiztonság fogalmát és elhelyeztem azt a biztonságtudomány és a digitális kultúra kontextusában.
- Történeti áttekintést nyújtottam az információbiztonság fejlődéséről, amely bemutatja, hogyan alakult ki az biztonságtudomány és ebből az

információbiztonság mint kutatási terület, különös tekintettel a digitális korban felmerülő kihívásokra.

- Generációs szempontból vizsgáltam a kérdést, összehasonlítva az X, Y, Z és Alfa generáció információbiztonsági tudatosságát és viselkedését.
- Összefoglaltam és bemutattam azon releváns kiberbiztonsági kockázatokat, amelyekkel az általános iskolás gyermekek találkozhatnak és tapasztalhatnak az online zaklatás, az adathalászat vagy a személyes adatok védelme kapcsán.
- Összefoglaltam azon vonatkozó elméletek és releváns megközelítéseket, amelyek a témafeldolgozásánál megjelentek.
- Kitértem a jogszabályi környezet bemutatására és kialakulására, amely meghatározza a gyermekek online védelmére vonatkozó kereteket.
- Megvizsgáltam az Oktatási Hivatal által általános iskolák részére kiadott „Digitális Kultúra" tantárgy oktatásának anyagait.
- Bemutattam mindazon releváns hazai és nemzetközi projektet és szakpolitikai kutatást amely a téma feldolgozásánál elkerülhetetlenül figyelembe kellett vennem.

A szakirodalmi áttekintésben tehát célom volt, hogy megalapozzam a kutatásomat, összefoglaljam a korábbi eredményeket és egyértelművé tegyem, milyen kérdésekre keresem a választ az értekezésemben.

Kvalitatív kutatás: Megfigyelések és interjúk

A kutatás következő szakaszában kvalitatív módszereket alkalmaztam. [5, pp. 37-38] Ennek keretében megfigyeléseket végeztem, valamint interjúkat készítettem a témában érintett szakemberekkel. A célom az volt, hogy mélyebb képet kapjak a gyermekek digitális eszközhasználati szokásairól, valamint a szülők és pedagógusok információbiztonsággal kapcsolatos tapasztalatairól és gyakorlatáról.

Alkalmazott módszerek:

- megfigyelés,
- interjúk

Cél: a téma alaposabb feltárása, a kérdőíves kutatás előkészítése.

Kvantitatív kutatás: „DigiÓ” kérdőíves vizsgálat

A kutatás következő szakaszában egy szélesebb körű, kvantitatív adatfelvételt valósítottam meg, amelynek alapját a DigiÓ program – az Óbudai Egyetem által támogatott és általam lebonyolított – kérdőíves vizsgálata képezte. [5, pp. 37-38] E kutatási szakasz célja az volt, hogy képet nyújtson a gyermekek, szülők és pedagógusok információbiztonsági kihívásokkal kapcsolatos tapasztalatairól, valamint az ezekre adott válaszaikról és stratégiáikról.

Alkalmazott módszerek:

- kérdőíves adatfelvétel,
- statisztikai elemzés

Cél: a gyermekek információbiztonsági szokásainak, valamint a szülői és pedagógusi hozzáállás feltérképezése

Visszamérés: Szakértői interjúk

Ezt követően a kérdőíves kutatás eredményeit szakértői interjúk segítségével ellenőriztem és pontosítottam. [5, pp. 37-38] Ezáltal lehetőség nyílt arra, hogy árnyaltabban értelmezzem az adatok mögötti folyamatokat, valamint összevessem a kvantitatív eredményeket a szakértők tapasztalataival.

Alkalmazott módszerek:

- strukturált interjúk szakértőkkel

Cél: a kérdőíves kutatás eredményeinek ellenőrzése és mélyebb értelmezése.

Tudományos kutatási alapelvek beépítése

A tudományos kutatómunkám során figyelembe vettem a tudományos kutatás legfontosabb alapelveinek érvényesüléseit. Az alábbiakban felsorolom mely alapelvek és hogyan érvényesültek a munkámban, valamint bemutatom, hogy mely befolyásoló és figyelembe veendő tényezők hatottak a kutatómunkám megvalósulására.

Alapelvek

- Objektivitás elve: Kutatásomban önállóan jártam el és következetesen törekedtem az objektivitás megőrzésére. A szekunder adatok feldolgozásakor, valamint az

általam összeállított kérdőívek eredményeinek elemzése során egyaránt arra törekedtem, hogy semleges, elfogulatlan szemlélettel értékeljem a kapott információkat.

- Történeti megközelítés elve: Bár a téma választásom szakirodalma nem tekint vissza hosszú múltra mégis folyamatosan tetten érhető a téma történetisége. Egyfelől maga az információbiztonság kutatása már rendelkezik egyfajta történetiséggel, illetve a terület rendkívüli aktualitásával összefüggésben a gyermekekre vonatkozóan az elmúlt 10 évben jelentősen megnőtt az igény a téma elemzésére. [6] Másfelől, tekintve hogy értekezésem az multidiszciplinaritás területein mozog, figyelembe vettem a témához kapcsolódó jogi terület meghatározó jogtörténeti mérföldköveit valamint a neveléstudomány fejlődéstörténetének témára vonatkozó tendenciáit és szabályozásait is.
- Megalapozott bizonyítás elve: A kutatott témát több irányból közelítettem meg a hipotézisek vizsgálata során. Ennek alapját egyrészt a gyermekek információbiztonsági helyzetének feltárását segítő szülői, tanulói és pedagógusi nézőpontok összevetése, másrészt a releváns szekunder kutatások eredményeinek beépítése jelentette.
- Az elmélet és gyakorlat pozítiv viszonyának elve „A 21. században a tudomány sem létezhet a társadalommal való folyamatos interakció nélkül. Reflektálnunk kell a társadalmat foglalkoztató kérdésekre, támpontot kell adnunk” – mondta az MTA Szegedi Területi Bizottságának tudományünnepi nyitórendezvényén Freud Tamás, az Akadémia elnöke, 2021-ben. Jelen disszertáció megvalósítja ezt az elvárást, hiszen a hipotézisem meghatározása eleve tudományos keretet adott az egyébként nagyfokú érdeklődéssel bíró téma kibontása során, és gyakorlati oldalról is kézzelfogható, aktuális eredményeket hozott, melyek felhasználása a társadalom számára is közvetlenül megvalósítható.
- Tudományos előrelátás elve: Az informatikai terület, az eszközökön tárolt információk kérdése, valamint gyermekeink biztonsága napi szinten fejlődik és az igény, hogy ezeken a területeken minél nagyobb emberi tudással és ismerettel rendelkezzünk pedig folyamatosan növekszik. A téma feldolgozása alapoz a már meglévő kutatásokra, a jelenkor tapasztalataira, valamint a jövőbe tekint és megpróbálja feltérképezni a terület kihívásait és a megoldáshoz hozzásegíteni a jövő generációját felnevelő társadalmi közösséget.

Multidiszciplinaritás

A téma vizsgálatához szükséges volt egyfajta multidiszciplináris szemlélet módra. A kutatásom biztonságtudományi alapokról indul és ezen tudományág szempontjából közelíti meg a tudományos célokat. Ugyanakkor a kutatásomban további - a Magyar Tudományos Akadémia nomenklatúra szerinti – tudományágak eszközrendszerei és ismeretanyagai lettek bevonva, illetve felhasználva [7, pp. 16-35].

A téma feldolgozásába bevont tudományágak:

Tudományos Osztályok	**Tudományterület**	**Tudomány kód**	**Tudomány ág**
VI.	Műszaki Tudományok	06 09 00	Informatika
II.	Filozófia és Történettudományok	02 02 09	Technikatörténet
		02 05 08	Nevelés- és pedagógiai pszichológia
		02 06 06	Oktatáspolitika, -igazgatás, -jog és -gazdaságtan
IX.	Gazdaság- és Jogtudomány	09 01 09	Polgári jog
		09 01 13	Büntető jog
		09 01 24	Európai jog
		09 03 04	Kultúra, társadalmi értékek és életmód szociológiája
		09 02 22	Statisztika és ökonometria
		09 04 04	Katonai biztonság és biztonságpolitika

1.sz. táblázat: érintett tudományágak (saját szerkesztés)

Trianguláció módszerének alkalmazása

A kutatásom során alkalmazkodnom kellett a vizsgált téma által érintett generációs közeg szempontjaihoz. A vizsgálatom fókuszában adott társadalmi rétegek kerültek ezért a módszertan megválasztásakor szükséges volt a szekunder források és a műszaki-informatikai anyagok elemzése mellett a valóságos tapasztalatok begyűjtése és ezek elemzése is, továbbá egyfajta humánirányúltsághoz illeszkedő módszertani megközelítés választása. Ez alapján a trianguláció tudományos kutatási módszerének alkalmazása mellett döntöttem.

A trianguláció egy kutatásmódszertani eljárás, amelynek célja a különböző forrásokból, módszerekből vagy perspektívákból származó adatok kombinálása a kutatás

megbízhatóságának és érvényességének növelése érdekében. [8, pp. 96-98] Az elnevezés a földrajzi triangulációból származik, amelyben egy adott pont vagy tereptárgy pontos helyzetét több nézőpontból határozzák meg. Analóg módon, a kutatásban is így használjuk azaz a különböző megközelítések együttes használatával pontosabb eredményeket kaphatunk. A trianguláció módszertana segítségével összehasonlítottam és integráltam azokat az eltérő megközelítéseket és az abból származó eredményeket, melyeket a kutatási folyamat során alkalmaztam. A többirányú megközelítés alkalmazásával és a többoldalú források vizsgálatával az alábbi kutatásmódszertani célokat valósítottam meg:

- Többirányú megközelítés: A különböző módszerek és források együttes alkalmazásával igyekeztem csökkenteni az adatokban és eredményekben rejlő szubjektivitást és torzítás lehetőségét. Ez a megközelítés nemcsak a kutatás megbízhatóságát erősítette, hanem lehetővé tette, hogy az egyes vizsgálati eredmények kölcsönösen megerősítsék, kiegészítsék egymást és ezáltal megalapozott következtetések születhessenek.
- A trianguláció módszertana segített a kutatás tárgyi komplexitásának jobb megragadásában, mivel különböző szempontokat vontam be az elemzésbe.
- Lehetővé tette számomra az ellentmondások és különbségek azonosítását, amelyeket – adott esetben - tovább tudtam vizsgálni.

Trianguláció a személyi megközelítésben – komplex nézőpontok

A kutatásomban három célcsoportot jelöltem ki: gyerekek, szülők és pedagógusok.

Gyermekek nézőpontja - A kutatásomban közvetlenül a gyermekektől gyűjtöttem adatokat, hogy feltérképezzem digitális eszközhasználati felhasználói szokásaikat, információbiztonsági ismereteiket és kedvenc alkalmazásaikat.

Szülők nézőpontja - A kutatásomban vizsgáltam, hogyan érzékelik a szülők gyermekeik digitális tevékenységeit, valamint milyen mértékben próbálnak alkalmazkodni a digitális világ kihívásaihoz.

Pedagógusok nézőpontja - A pedagógusok megkérdezésével a kutatásomban feltártam, hogy milyen nehézségekkel szembesülnek a digitális oktatás és a kiberbiztonság terén.

Trianguláció az időbeli megközelítésben

Kutatásomat egymásra épülő és egymást kiegészítő fázisokra osztottam, amely lehetővé tette a téma vizsgálatát. Időrendi sorrendből vizsgálva megjegyezhető, hogy a szekunder kutatási módszerek előkészítették és kiegészítették a primer kutatás folyamatát, majd együtt egy egységes kutatási képet alakítottak ki, amely segítette a hipotézisek vizsgálatát. A kvalitatív interjúk és megfigyelési módszerek alkalmazását követő kvantitatív kérdőíves kutatás majd az ezt követő eredményeket visszamérő kvalitatív szakasz triangulatív megközelítése biztosította számomra a kutatási eredményeim megalapozottságát.

1.2 A témához kapcsolódó fogalmi viszonyok

Biztonság fogalmának megközelítése

A biztonság fogalmának értelmezése régóta jelen van a társadalmi gondolkodásban. A Magyar Nyelv Értelmező Szótár korai kiadása szerint „a biztonság – a dolgoknak, életviszonyoknak olyan rendje, olyan állapot, amelyben kellemetlen meglepetésnek, zavarnak, veszélynek nincs vagy alig van lehetősége, amelyben ilyentől nem kell félni.” [9] Bár ez a meghatározás több mint hetven évvel ezelőtt született, jelentése a technológia gyors fejlődése ellenére sem veszített lényegi érvényéből. Az internet korában a technikai változások olyan ütemben zajlanak, hogy az emberi megértés és alkalmazkodás gyakran nem tud lépést tartani velük. Ebben a rendkívül dinamikus közegben próbáljuk megteremteni a jövő generációi számára azt a biztonságot, amelyben a zavar, veszély vagy kellemetlen meglepetés esélye minimális.

A fogalom tudományos megközelítése ennél összetettebb. Berek Lajos, az Óbudai Egyetem professzora szerint: „A biztonság személyek és szervezetek azon állapota, melyet a létüket, illetve rendeltetésszerű működésüket veszélyeztető szándékos jogellenes magatartások és az azokkal szemben alkalmazott védelmi erőforrások együtthatása határoz meg.” [10, p. 6] Ez a meghatározás már nem csupán a veszély hiányára, hanem annak aktív megelőzésére és kezelésére is ráirányítja a figyelmet. Különösen fontos ez akkor, amikor az általános iskolás korú gyermekek digitális biztonságáról beszélünk. Mindennapi küzdelmet jelent számunkra, hogy számukra olyan életviszonyokat teremtsünk, amelyekben a biztonság nem csupán vágyott állapot, hanem a gyakorlatban is fenntartható cél legyen.

A biztonságérzet napi szinten meghatározza, az emberek viszonyulását hogyan élik az életüket. A mai 40 év feletti generációk sokszor értetlenül és rémülten figyelik mi történik a fiatalokkal a képernyők előtt. Más-más szempontból, de mind a felnőtteknek - akik a gyermekeikért aggódnak - mind a mai általános iskolás korú fiataloknak olyan kétségeik vannak, amelyek aggodalomra adnak okot. Ez a harc már nem a csatatereken zajlik, hanem gyermekeink szobájában a számítógépek előtt ülve, a telefonok képernyőjét bámulva vagy éppen valamely applikációs platform használata közben. A következő generáció biztonságos létét veszélyeztető tényezők elsősorban az online térben keresendők. A mai fiatalok egy olyan világban nőnek fel, ahol a digitális környezet, az internet jelenléte és a digitális eszközök napi használata már társadalmi normának számítanak. Ezek az eszközök a közösségi lét szerves részévé váltak és alapvetően befolyásolják, hogyan igazítják egymáshoz viselkedésüket az egyének, illetve hogyan alakítják ki azokat az együttműködési szabályokat és normákat amelyek a társadalom működésének is alapját képezik. A társadalmi normák egyfajta logikai rendben épülnek fel. Először megfogalmazzák az adott körülményekhez tartozó elvárt viselkedési formákat, majd minősítik ezeket (például tilos, kötelező vagy megengedett), végül pedig rögzítik a normasértés lehetséges következményeit. [11] A digitális világban ezek a normák és szabályok új kihívások elé állítják a társadalmat, különösen a fiatalabb generációk szocializációja és biztonsága szempontjából.

Információbiztonság fogalma

Az információbiztonság (angolul: information security vagy rövidítve infosec) azokat az eszközöket és folyamatokat foglalja magában, amelyeket a személyek, szervezetek az információk védelmére használnak. Ide tartoznak azon beállítások is, amelyek megakadályozzák, hogy illetéktelenek hozzáférjenek személyes vagy üzleti információkhoz. Az információbiztonság védi az érzékeny információkat a jogosulatlan tevékenységektől, beleértve az ellenőrzést, a módosítást, a rögzítést, valamint az esetleges megszakítást vagy megsemmisítést. A biztonsági incidensek következményei közé tartozik a magáninformációk ellopása, az adatok meghamisítása és az adatok törlése.

Európai Adatvédelmi Biztos oldalán fellelhető meghatározás szerint, az információbiztonság alapvető eszköz a magánélet és a személyes adatok védelméhez. [12] Három általánosan elfogadott elem szükséges az információ megfelelő védelméhez:

- Bizalmasság (Confidentiality): csak a megfelelő személyek férhetnek hozzá az információhoz;
- Sértetlenség / Integritás (Integrity): csak a megfelelő személyek módosíthatják az információt a megfelelő módon;
- Rendelkezésre állás (Availability): az információ elérhető, amikor szükség van rá.

A Nemzetközi Elektrotechnikai Bizottság (International Electrotechnical Commission) által üzemeltetett online elektrotechnikai szótár az Electropedia így fogalmazza meg az információbiztonság fogalmát: „az információk bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése.” [13] további meghatározásként megfogalmazva „az információk védelme a véletlen vagy szándékos nyilvánosságra hozatal, átadás, módosítás vagy megsemmisítés ellen.” [14]

Az információbiztonság alapelvei a bizalmasság, az integritás és a rendelkezésre állás és erre a három alappillérre épül. Az első hogy az adott információ sértetlen legyen, pontos maradjon és ne torzuljon a második hogy az arra felhatalmazott felhasználó mindig hozzáférjen az adott információhoz és kapcsolódó értékekhez végül pedig a harmadik a jogosultság avagy bizalmasság kérdése azaz csak az arra jogosult vagy felhatalmazott személy számára legyen elérhető az adott információ. [15, p. 64]

Microsoft szerint az információbiztonság – gyakran rövidítve InfoSec – olyan biztonsági eljárások és eszközök összessége, amelyek átfogó védelmet nyújtanak az érzékeny vállalati adatok számára a visszaélésekkel, jogosulatlan hozzáféréssel, működési zavarokkal vagy megsemmisüléssel szemben. Az információbiztonság magában foglalja a fizikai és környezeti biztonságot, a hozzáférés-szabályozást, valamint a kiberbiztonságot is.” [16]

A kiberbiztonság fogalma

Az információbiztonság mind terjedelmében, mind céljában különbözik a kiberbiztonságtól. A két kifejezést gyakran szinonimaként használják, de ha pontosabban akarjuk definiálni akkor azt kell mondani hogy a kiberbiztonság az információbiztonság egyik alkategóriája. Az információbiztonság egy széles terület, amely számos területet foglal magában, például a fizikai biztonságot, a végpontbiztonságot, vagy például az adattitkosítást vagy a hálózati biztonságot. A kiberbiztonság elsősorban a technológiával kapcsolatos fenyegetésekkel foglalkozik, illetve olyan gyakorlatokkal és eszközökkel, amelyekkel mindezek megelőzhetőek vagy mérsékelhetőek.

Az Európai Parlament és a Tanács (EU) 2019/881 rendelete az Európai Uniós Kiberbiztonsági Ügynökségről szóló jogszabály a kiberbiztonság fogalmát a következőképpen fogalmazza meg: „azok a tevékenységek, amelyek a kiberfenyegetésekkel érintett hálózati és információs rendszereknek, az ilyen rendszerek felhasználóinak és más személyeknek a védelméhez szükségesek.” [17]

Ezt az értelemzést fejti tovább az Európai Unió Hálózat- és Információbiztonsági Ügynökségének (European Union Agency for Network and Information Security – ENISA) által kiadott definíciós dokumentum, amely megfogalmazása szerint, „Kiberbiztonság: azon intézkedések, eljárások és mechanizmusok összessége, amelyek a kibertér, annak felhasználói, valamint az érintett szervezetek és személyek védelmét szolgálják a kibertérből érkező fenyegetésekkel és kockázatokkal szemben. Magában foglalja a kibertérben bekövetkező események megelőzését, előrejelzését észlelését, kezelését és kivizsgálását, továbbá célja a rendszerek és információk rendelkezésre állásának, bizalmasságának, sértetlenségének és megbízhatóságának biztosítása, valamint a robusztusság, a rugalmasság, az elszámoltathatóság és a hitelesség fenntartása.” [18]

Két nagy szoftvergyártó a Microsoft és az SAP SE az alábbiakban definiálja a kiberbiztonság fogalmát:

- Microsoft magyarországi support oldala szerint: „A kiberbiztonság – más néven digitális biztonság – a digitális adatok, készülékek és eszközök védelmére irányuló lépések összessége. A védendő dolgok közé tartoznak az Ön személyes adatai, fiókjai, fájljai, fényképei, sőt még a pénze is. [19]
- Az SAP SE mint vállalatirányítási rendszerszoftvereket gyártó cég megfogalmazása szerint a „A kiberbiztonság: a hálózatok, eszközök, alkalmazások, rendszerek és adatok védelmének gyakorlata a kibertámadásokkal szemben.” [20]

Az ERP-rendszerek és az információbiztonság kapcsolatát korábban a Biztonságtudományi Szemle tudományos folyóiratban megjelent tanulmányomban részletesen bemutattam. [15]

Adatvédelem fogalma

Míg az információbiztonság és a kiberbiztonság elsősorban a rendszerek, hálózatok és adatok technikai, szervezeti és működési védelmét hangsúlyozza, addig az adatvédelem

kifejezetten az egyénekhez kapcsolódó adatok védelmét helyezi a középpontba. Az adatvédelem így az információbiztonság és kiberbiztonság kiegészítő, de önálló kategóriája, amely a személyes adatok jogszerű és felelős kezelését biztosítja. A Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) elérhető Adatvédelmi Értelmező Szótára alapján az „adatvédelem: a személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége. Személyes adatnak minősül minden olyan adat amely az adott személlyel kapcsolatba hozható és levonható belőle, az érintettre vonatkozó következtetés.” [21]

1.3 Információbiztonság fejlődés történeti áttekintése

Biztonságtudomány Történeti alapozás

A jelenkor biztonsági kihívásainak mélyebb megértéséhez elengedhetetlen, hogy visszatekintsünk a múlt tapasztalataira és tanuljunk a korábbi válaszokból. Ez a szemlélet a biztonságtudomány területén is érvényesül. Értekezésemben a tudományterület néhai kiemelkedő képviselője, Kiss Sándor felosztását veszem alapul, amely szerint a biztonság megismerésének folyamata történetileg négy szakaszra bontható. [22, pp. 26-28] A szakirodalmi feldolgozás szakaszában ezt a tudományos megközelítést és annak felosztását korábban részletesen kifejtettem a National Security Review tudományos folyóiratban megjelent publikációmban, amelyre az irodalomjegyzékben is hivatkozom. [23, p. 88]

Az első szakasz, az „ártatlanság kora”, az ipari forradalom előtti időszakot – egészen a tizenhetedik–tizennyolcadik századig – öleli fel. E korszak sajátossága, hogy az ember még nem foglalkozott tudatosan a biztonság mai értelemben vett kérdéseivel: nem mérte, nem elemezte azokat. A természeti csapásokat, katasztrófákat, járványokat, de még a háborúk jelenlétét is az élet természetes velejárójaként fogadták el. Bár a korszak konfliktusai kényszerű válaszokat hívtak elő, ezek inkább ösztönösnek, semmint tudatosnak tekinthetők. Ezt az ösztönös válaszképességet jól szemlélteti például a kutya házőrzőként való alkalmazása a történelem hajnalán [24, pp. 216-221], vagy a középkori járványokra adott – kezdetleges, de célszerű – társadalmi reakciók.

A második szakasz, a „felfedezés kora”, az ipari forradalmat követő időszaktól a tizenkilencedik–huszadik század fordulójáig tart. Ekkor már megjelent a biztonság tudatos igénye és kialakultak annak elméleti alapjai. A műszaki tudományok és az

orvostudomány olyan eszközökkel gazdagodtak, amelyek lehetővé tették a biztonsági problémák felismerését, dokumentálását és kezelését. A társadalmi fejlődés új kihívásokat hozott, s vele együtt az igényt a biztonság tudatosabb megteremtésére. Az új technológiák és eszközök alkalmazása során az ember felismerte a biztonsági kockázatokat maga körül és megtette az első lépéseket azok kezelésére. [23, p. 88]

A harmadik szakasz, a „rendszerbiztonság kora", a huszadik század elejétől kezdődő, gyors ütemű ipari és technológiai fejlődéshez köthető. Ezt az időszakot a hadipar fellendülése, valamint olyan új találmányok, mint a repülőgép, az automobil, majd később az űripar megjelenése és elterjedése jellemzi. A biztonság iránti igény itt már rendszerszintű megoldások kidolgozását tette szükségessé.

A negyedik szakasz, a „biztonságtudomány kora", napjainkig tart és a tudomány, illetve a technológia fejlődésére adott egzakt, megalapozott válaszokat jelenti. Az ember felismeri a biztonsággal kapcsolatos alapelveket és összefüggéseket, létrehozza saját eszközrendszereit és ezek segítségével képes tudományosan megalapozott, rendszerszintű válaszokat kidolgozni – legyen szó technikai megoldásokról, módszertanokról vagy komplex biztonsági rendszerekről. [25, pp. 84-85]

Információbiztonság történeti áttekintése

A történeti áttekintés keretében röviden bemutatom az információbiztonság fejlődéstörténetét, amelynek tudományos megközelítését és feldolgozását korábban a Biztonságtudományi Szemle tudományos folyóiratban közölt publikációmban részletesen ismertettem. [25]

Hideg Háború korszaka és a 60-as évek

A hidegháború idején jelentősen megnőtt az igény a bonyolultabb és kifinomultabb feladatok elvégzésére, valamint az egyre nagyobb mennyiségű adatok tárolására és feldolgozására. Ebben az időszakban jelentek meg az első elektronikus számítógépek, amelyek kezdetben teremnyi méretű, nagyteljesítményű gépek voltak és főként katonai, tudományos, illetve állami feladatok ellátását szolgálták. E nagygépek közötti kommunikáció hatékonysága azonban korlátozott volt: a mágnesszalagos adattovábbítás és az akkoriban elérhető adatkommunikációs módszerek nem tudták kielégíteni a növekvő igényeket. Az Egyesült Államok Honvédelmi Minisztériumának Fejlett Kutatási Projektek Ügynöksége (Department of Defense's Advanced Research Projects Agency, a továbbiakban: ARPA) ezért megkezdte egy hibatűrő és közös hálózatba kapcsolt

kommunikációs rendszer megvalósíthatóságának vizsgálatát, amely képes volt támogatni a katonai információcserét. A programot 1969-ben Larry Roberts koordinálta, akit az internet egyik alapítójaként is emlegetnek. Az így létrejött ARPANET gyakorlatilag a ma ismert internet történeti előzményének tekinthető. [25, pp. 84-85]

A 70-es 80-as évek

A következő évtizedek során az ARPANET népszerűvé és széles körben elterjedté vált. Az ARPANET-ben lévő potenciál egyre erősebb kihasználása miatt a visszaélések száma is gyakoribbá vált. 1973 decemberében Robert M. "Bob" Metcalfe, - akinek nevéhez később az egyik legnépszerűbb hálózati protokoll az Ethernet fejlesztése fűződik - felismerte az ARPANET biztonságával kapcsolatos alapvető problémákat. Az rendszerben lévő egyes távoli helyszínek nem rendelkeztek elegendő kontrollal és védelemmel az adatok illetéktelen felhasználóktól történő távoli megvédésére. Egyéb problémákkal is bővelkedett a rendszer, úgymint: a jelszó szerkezetének és formátumainak sebezhetősége, a telefonos kapcsolatokhoz igazodó biztonsági eljárások és felhasználói azonosítás hiánya.

A gazdagépek és a felhasználók számának robbanásszerű növekedésével együtt járt, hogy a rendszerben használt telefonszámokat széles körben terjesztették, sőt gyakran nyilvánosan is feltüntették, például telefonfülkék falain. Nem meglepő tehát, hogy a korabeli „hackerek" viszonylag könnyen hozzáférhettek az ARPANET-hez. Ezt a súlyos információbiztonsági hiányosságot egy 1978-ban megjelent tanulmány, a Protection Analysis – Final Report tárta fel egyértelműen, amely részletesen bemutatta az ARPANET operációs rendszereinek biztonsági sebezhetőségeit. [26, pp. 3-15] A feltárt problémákra válaszul az Egyesült Államok Védelmi Minisztériuma kiadta a Rand Report R-609 jelzésű, mérföldkőnek tekinthető dokumentumot. [27, p. 11] Ez volt az első olyan hivatalos irat, amely meghatározta a többszintű számítógépes rendszerek tartalmát és amelytől kezdve számíthatjuk a számítógépes biztonság történetének kezdetét. Jelentősége abban állt, hogy lefektette azokat az alapelveket – például a jogosultsági szintek elkülönítését és a hozzáférés-szabályozás szükségességét –, amelyek a mai napig meghatározó elemei az információbiztonsági rendszereknek. [25, pp. 84-85]

Az internet megjelenése a 90-es években

A 20. század végén a személyi számítógépek használata egyre inkább elterjedt és ezzel párhuzamosan megjelent az igény arra, hogy ezek a számítógépek hálózatban kapcsolódjanak egymáshoz. Ez az igény vezetett a hálózatok globális hálózatának, az

internetnek a kialakulásához. Az internet gyakorlatilag minden számítógéphez csatlakozási lehetőséget biztosított, amely rendelkezett telefonvonalas kapcsolattal vagy helyi hálózati (angol elnevezése: Local Area Network, LAN) eléréssel.

Az internet kereskedelmi forgalomba kerülését követően a technológia rohamosan elterjedt és a világ szinte minden részébe eljutott. Az internetkapcsolatok kezdetben de facto szabályokon alapultak, amelyek alig nyújtottak védelmet az információbiztonság számára. Később, ahogy ezek az elődtechnológiák széles körben elfogadottá váltak és ipari szabványokká fejlődtek, bizonyos fokú biztonságot eredményeztek. A korai internetes telepítéseknél azonban a biztonság alacsony prioritást kapott. Ennek egyik oka az volt, hogy abban az időszakban az internet és az e-mail felhasználóinak többsége informatikus volt, így a levelezőszerverek hitelesítése és az üzenetek titkosítása nem tűnt sürgetőnek. Valójában számos olyan probléma, amely ma is sújtja a levelezőrendszereinket, már akkoriban is megjelent az interneten. Ahogy a számítógépek hálózatos összeköttetésbe kerültek, megszűnt az a védelem, amelyet a fizikai elszigeteltség jelentett és ezt követően a tárolt információk fokozottan ki voltak téve a különféle fenyegetéseknek. [25, pp. 84-85]

2000-es évek válaszai

Az internet a számítógépes hálózatok millióit kapcsolja folyamatos kommunikációba egymással. Az egyes számítógépekben tárolt adatok biztonsága nagymértékben függ minden olyan más számítógép biztonsági szintjétől, amellyel kapcsolatban állnak. A 2000-es évek elejétől kezdve egyre nagyobb tudatosság figyelhető meg az információbiztonság javításának szükségessége kapcsán, megjelennek az ajánlások és a szabványok.

A szabványosítási törekvések az információtechnológia fejlődésével párhuzamosan erősödtek. Az 1980-as évektől kezdődően a számítógépek üzleti célú alkalmazása egyre elterjedtebbé vált, az üzleti folyamatok és az adatok felhasználása pedig az egységesített gyakorlat irányába mozdult el. Egyre erőteljesebben jelentkezett az igény egy olyan átfogó keretrendszer megalkotására, amely mintegy „sorvezetőként” segíti a rendszerekben kezelt információk védelmét.

Ezt az igényt elsőként a COBIT (Control Objectives for Information and Related Technology – magyarul: Irányítási célok az információkra és a kapcsolódó technológiákra) elnevezésű keretrendszer elégítette ki. A COBIT nem minősül hivatalos szabványnak, ám a gyakorlatban gyakran szabványként alkalmazzák. Lényegében egy ajánlásgyűjtemény, amely főként az információtechnológiai auditálás céljait támogatja.

A másik irányt a tényleges szabványosítás jelentette. Erre jó példa az ISO/IEC 27001 nemzetközi szabvány, amely követelményrendszert fogalmaz meg az információbiztonság-irányítási rendszer (IBIR) kialakítására, bevezetésére, működtetésére és folyamatos fejlesztésére. A szabvány folyamatközpontú és a PDCA-ciklusra (Plan–Do–Check–Act, magyarul: Tervezés–Végrehajtás–Ellenőrzés–Beavatkozás) épül. Az így megvalósított IBIR integrálható más irányítási rendszerekkel, például a minőségirányítási (ISO 9001) vagy a környezetirányítási (ISO 14001) szabványokkal. Az információbiztonsági kutatásomhoz kapcsolódó, a szabványosítás kérdését feldolgozó publikációm a National Security Review tudományos folyóiratban jelent meg, amelyre az irodalomjegyzékben is hivatkozom. [28]

Egy adott szervezet számára stratégiai döntést jelent, hogy bevezeti-e az információbiztonság-irányítási rendszert. A kialakítást befolyásolja a szervezet célrendszere, folyamatai, mérete, felépítése, valamint a biztonsággal kapcsolatos elvárásai. [25, pp. 84-85] Az ISO/IEC 27001 megfogalmazása szerint: „Az információbiztonság-irányítási rendszer egy kockázatkezelési folyamat segítségével őrzi meg az információk bizalmasságát, sértetlenségét és rendelkezésre állását és az érdekelt felekben bizalmat kelt arra vonatkozóan, hogy a kockázatokkal kielégítő módon foglalkoznak.” [29]

1.4 A kutatás által érintett generációk információbiztonsági jellemzői

Ebben a fejezetben bemutatom a kutatásomba bevont generációk információbiztonsági sajátosságait. Fontos kiemelni, hogy egyik generáció sem tekinthető önmagában jobbnak vagy rosszabbnak a kiberbiztonság megközelítésében; eltéréseik elsősorban abból fakadnak, hogy másként használják digitális eszközeiket, így különféle mértékben vannak kitéve bizonyos fenyegetéseknek. Az értekezésben a generációk általánosan jellemző kiberbiztonsági mintázataira összpontosítok, jóllehet az egyéni sajátosságok ettől eltérhetnek. Az alábbiakban e generációk alapvető jellemzőit foglalom össze.

Az X generáció 1965-1980

Az X generációt a szakirodalom gyakran „digitális bevándorlóknak” nevezi, mivel e nemzedék tagjai a számítógépek, mobiltelefonok és a digitális technológiák elterjedése előtt születtek, így azok használatát életük későbbi szakaszában kellett elsajátítaniuk. [30] A kutatásomban a részt vevő gyermekek szüleinek többsége szintén ebbe a generációba tartozott: a válaszadók 56%-ának szülei az X generáció tagjai. Ez jól mutatja, hogy e korosztály jelentős arányban képviselteti magát a mai iskoláskorú gyermekek szülői

körében. Az X generáció számára a technológiai eszközök nem képezték természetes módon a munkavégzés részét, így alkalmazkodásra kényszerültek a digitális környezet gyors térnyerésével szemben. A kiberfenyegetésekkel kapcsolatos tapasztalataikat sokszor nem tudatos felkészülés, hanem közvetlen áldozattá válás révén szerezték, ezért saját gyakorlatokat, „trükköket" és szokásokat alakítottak ki a védekezésre. Ennek hátterében az is áll, hogy a kiberbiztonsági ismeretek és készségek nem képeztek meghatározó tényezőt, amikor e generáció tagjai a munkaerőpiacra léptek. A kommunikációs formák tekintetében az X generáció leginkább a telefonhívást és az e-mailt részesíti előnyben. Az e-mailt biztonságosabbnak és kényelmesebbnek ítélik meg az SMS-nél, továbbá jobban felkészültek arra, hogy felismerjék az elektronikus levelezésen keresztül megvalósított adathalászati kísérleteket. [31, pp. 42-48] E nemzedék rendelkezik a legnagyobb munkatapasztalattal és ők azok, akik a kezdetektől fogva tanúi lehettek a kiberfenyegetések fejlődésének, valamint a kiberbiztonsági intézkedések és szervezeti szabályozások fokozatos bevezetésének a munkahelyeken. Az X generáció tagjai a szabályok követésére az utánuk következő nemzedékeknél nagyobb hajlandóságot mutatnak: tudatosan elkülönítik a munkahelyi és a személyes e-mail-címeket és jelszavaikat rendszerint a munkahelyi előírásoknak megfelelően változtatják. Az újkori technológiák bevonodása a magánéletükbe azonban egy újabb kihívás és ez a vállalati világban is problémákhoz vezethet. Az X generációsok azok akik hajlamosabbak arra, hogy személyes információkat osszanak meg a közösségi média profiljaik, ezáltal nagyobb eséllyel vannak kitéve a social engineering támadásoknak. Mivel kevésbé ismerik ezeket a platformokat, az adathalász-támadásokat is nehezebben ismerik fel a közösségi médiában. Ezek a személyes információk, amelyeket nyíltan megosztanak a közösségi médiában, valós fenyegetést jelenthetnek a személyükre vagy akár munkaadóik számára is, hiszen ezeket az információkat egy spear phishing támadásban akár a személyes fiókhoz vagy a munkahelyi fiókjukhoz köthető biztonsági kérdések megválaszolásához és feltöréséhez is felhasználhatják.

Az Y generáció másnéven a milleniumi generáció (1980-1995)

Az ezredfordulón született, úgynevezett millenniumi vagy Y generáció technológiai szempontból sajátos helyzetben van. Nem minden tagja tekinthető teljes mértékben digitális bennszülöttnek: bár többségük gyermekkorában már rendelkezett otthoni számítógéppel, a közösségi média csak később vált életük meghatározó részévé. A munka világában azonban már egyértelműen digitális bennszülötteknek számítanak, hiszen a

számítógép a kezdetektől fogva jelen volt munkahelyi környezetükben. A kiberbiztonság számukra nem ismeretlen terület és közülük sokan részesültek formális képzésben is e témában. Kommunikációs szokásaikban nagyobb szerepet kapnak a szöveges üzenetek, mint az X generáció esetében, továbbá gyakran használnak okostelefonos alkalmazásokat mindennapi feladatok – például banki ügyintézés vagy számlafizetés – elvégzésére. [32, p. 122] Az Y generáció tagjai egyszerre hordozzák a technológiai környezetben való szocializáció és a munkahelyi tapasztalat sajátosságait. Mivel belenőttek a digitális eszközök használatába, hajlamosak úgy vélni, hogy értik azok kockázatait. Ez a magabiztosság azonban oda vezethet, hogy bizonyos kérdésekben jobban bízva saját tudásukban, olykor kevésbé támaszkodnak a munkahelyi informatikai szakemberek szakértelmére. [33, pp. 343-345] A biztonságtudatosságuk leginkább a személyes eszközeik kezelésében érhető tetten, ugyanakkor nem minden esetben ugyanolyan körültekintőek a munkahelyi eszközök használatában. [34, pp. 89-90] Gyakran szembesülnek jelszókezelési nehézségekkel, ugyanakkor ők azok, akik a legnagyobb arányban veszik igénybe az online banki szolgáltatásokat. Ez a bizalom ugyanakkor sebezhetővé is teheti őket: nagyobb valószínűséggel eshetnek áldozatul banki intézménynek álcázott adathalász kísérleteknek, mivel rendszeresen kapnak hivatalos üzeneteket és értesítéseket pénzintézetüktől. Technológiai döntéseiket gyakran a kényelem szempontja határozza meg, így általában nyitottak olyan megoldásokra, mint a jelszókezelők vagy a VPN-ek (Virtual Private Network – virtuális magánhálózatok) használata, ha azok egyszerűsítik mindennapi digitális tevékenységeiket.

Z generáció (1995-2010)

A digitális bennszülött definíciója a Z generációval kezdődik. A legtöbb esetben ennek a generációnak a tagjai nem emlékeznek olyan időszakra, amikor a digitális technológia ne lett volna az életük szerves része. A technológiával való érintkezésük nagy része az okostelefonjukon keresztül történt. [35, pp. 81-84] Az új platformokat gyorsabban fogadják el, mint más generációk, de gyakran kevésbé járatosak az asztali számítógépekben. Elsősorban a közösségi médiaplatformokon, például a Snapchat-en keresztül kommunikálnak és gyakran a felhasználónevüket cserélik ki telefonszámuk helyett, amikor új emberrel találkoznak. Kevesebb kiberbiztonsági képzésben részesültek, mint más generációk és összességében sokkal nagyobb biztonságban érzik magukat online. [36, pp. 270-274] A Z generáció munkahelyi szokásait vizsgálva már most kirajzolódnak a jellegzetes viselkedési jellemzők. [37] A Z generáció a

technológiával együtt nő fel de ez nem jelenti azt, hogy automatikusan érti is azt. Úgy tűnik, hogy ezen generáció tagjai számára talán már túlságosan is normalizálódott a digitális technika jelenléte. A Z generáció technológiai ismereteit nagyban befolyásolják az okostelefonokon lévő közösségi média alkalmazások, amelyek túlsúlyban lévő használata miatt rosszul felkészültek az e-mailben vagy akár hamisított webhelyeken keresztül történő adathalász-támadások felismerésére. Ők az a generáció, amely közül sokan az utolsó pillanatig figyelmen kívül hagyják az előírt informatikai frissítéseket és újra felhasználják a személyes és munkahelyi fiókok jelszavait. Másik oldalról fiszont jeleleg ők a legügyesebb generció a közösségi médián keresztül végrehajtott átverési kísérletek felismerésében. Ez a generáció gyorsan alkalmazkodik az új technológiai trendekhez és hajlandó betartani az ehhez kapcsolódó szabályokat ha azok fontosságát számukra érthetően elmagyarázzák.

Alfa generáció (2010 után született gyermekek generációja)

Az értekezésben vizsgált általános iskolás korosztály az Alfa generáció, vagyis azok a gyermekek, akik 2010 után születtek. Ők egyértelműen „digitális bennszülöttek”, hiszen a digitális technológia jelenlétébe, használatába és vívmányaiba beleszülettek és születésük pillanatától kezdve mindennapjaik szerves részét képezik. Ők azok akik több időt töltenek online a számítógép képernyője, okostelefonok és táblagépek előtt, mint bármely korábbi generációs csoport. [38, p. 2] Szüleiktől eltérően az „Alfák” fejlődésének középpontjában a vizuális tanulás és a digitális képeken keresztüli kommunikáció áll. Míg az idősebb generációk valószínűleg jobban hozzászoktak a halláson keresztüli tanuláshoz, számukra a vizuális kommunikáció a kulcs a megértéshez. A technikában járatos alfa-gyerekek, digitális társas világban élnek és az elektronikus eszközök számukra mindennapos játékká válnak. Mindez egyre fontosabb részét képezi a szocializációjuknak. Az alkalmazások és játékok által összekötött barátságok az Alfa generáció képviselői számára nem korlátozódnak a játszótérre. [39, pp. 6-8] Számukra az influenszerek jelenléte természetes az online játék és a social média alkalmazások használata mindennapos. A kibertámadások iránya főleg ezen platformok használatán keresztül jelentkeznek náluk, valamint a korukból adódó bizalommal társuló ismerethiányból ered. További, fontos tényezője a korosztálynak, hogy az Alfa generáció egy olyan világban nő fel, ahol a mesterséges intelligencia olyan általános, mint az internet volt a milleniumi generáció számára. Ezért a technológiáról, a magánéletről és a

biztonságról való gondolkodásuknak még fejlődnie kell. Az AI által generált kiberbiztonsági kihívások egyre jobban megjelennek náluk.

1.5 Általános iskolás korú fiatalok kiberbiztonsági fenyegetései

A számítógépek megjelenésével és gyors fejlődésével a kezelt információs adatok száma, mennyisége és tárolási kapacitása korábban nem látott mértékben növekedett [40, pp. 41-43]. A nagy koncentrációban történő adattárolás új dimenziókat nyitott az adatok feldolgozásában, miközben a fiatalok maguk is egyre inkább információforrásokká váltak: adataik birtoklása értéket képvisel, és jelentős információs erőforrást jelent [41, pp. 378-379]. A gyermekek és serdülők online térben való jelenléte ma már meghatározó társadalmi jelenség, amely egyszerre hordoz fejlődési lehetőségeket és komoly kockázatokat. Az Egészségügyi Világszervezet (WHO – World Health Organization) Europai tanulmányában 2024-ben publikált iskoláskorú gyermekek egészségmagatartását vizsgáló kutatásban amely 44 ország és régió több mint 279 000 fiataljának bevonásával készült rámutatott arra, hogy az iskolai zaklatás és az online bántalmazás széles körben érinti a 11, 13 és 15 éves korosztályt. A felmérés szerint a serdülők 15%-a, vagyis minden hatodik fiatal, már megtapasztalta a cyberbullyingot, míg 12%-uk maga is zaklatott másokat az online térben. [42] „Az információtechnológiai rendszerek és összetevők új sebezhetőségeket hordoznak, új - elsősorban információs jellegű - veszélyeztető hatások számára teremtenek lehetőségeket.” [43, p. 1] Az információk kezelőinek és használóinak óriásira nőtt a felelőssége abban, hogy ezen információk ne sérüljenek és ne torzuljanak, hogy a felhatalmazott felhasználók számára ezek az információk és kapcsolódó értékek mindig elérhetőek legyenek illetve hogy csak az arra jogosult vagy felhatalmazott személy számára legyenek elérhetőek. Ez egyfajta védelmi rendszer kiépítését igényli, illetve preventív tevékenységekre ösztönöz. Napjainkban a kiberbiztonsági kihívások minden szereplőt érinthetnek, így a gyermekek is potenciális célpontjai lehetnek a digitális térben megjelenő támadásoknak és visszaéléseknek. Mindez indokolttá teszi a kockázatok részletes feltárását és rendszerezését, hogy pontosabb képet kaphassunk a fiatal korosztály sérülékenységéről és védelmi lehetőségeiről. Áttekintés keretében jelen fejezetben bemutatom a gyermekeket érintő kiberbiztonsági kockázatokat és fenyegetéseket, valamint összegzem azok legfontosabb jellemzőit. Tanulmányomban a Quayyum és munkatársai által, a Norvég Tudományos és Technológiai Egyetemen (NTNU) végzett kiberbiztonsági kutatásban alkalmazott jegyzetcsoportosítási módszert követem. [44]

Online adatvédelem (online privacy)

Az online adatvédelem a gyermekek digitális jelenlétének egyik legkritikusabb területe, amely a személyes adatok – így például a név, lakcím, fényképek vagy helyadatok – biztonságos kezelését jelenti. A gyermekek körében tapasztalható tudatosság hiánya és a felügyelet elégtelensége miatt a személyes információk könnyen illetéktelen kezekbe kerülhetnek, növelve a visszaélések és a kiszolgáltatottság kockázatát. Ide sorolandó kockázatok:

- Adatvédelem a közösségi hálózatokon
    - Az információk megsértése és/vagy kitettség: A fogalom arra utal, amikor a gyermekek személyes adatai illetéktelen hozzáférés, nyilvánosságra kerülés vagy jogosulatlan felhasználás következtében veszélybe kerülnek.
    - Az információk túlzott mértékű megosztása: Azon jelenség, amikor a gyermekek a szükségesnél több személyes információt, képi vagy szöveges tartalmat tesznek közzé, ezáltal fokozva digitális sérülékenységüket.
    - Földrajzi címkézés (megjelölés): Olyan adatvédelmi kockázat, amely során a megosztott tartalmakhoz kapcsolódó helymeghatározási adatok a gyermekek tényleges tartózkodási helyét azonosíthatóvá teszik.
    - Közösségi média fiókok feltörése: A gyermekek közösségimédia-fiókjainak jogosulatlan hozzáférése, amely identitáslopáshoz, adatvesztéshez vagy visszaélésekhez vezethet.

Összegzés: A közösségi média használata jelentős adatvédelmi kockázatokat rejt magában, különösen a gyerekek és tinédzserek esetében. Az online megosztott személyes adatok, például a helyadatokkal ellátott fényképek, könnyen felhasználhatóak rosszindulatú célokra. [45] A helyadatok online nyilvánosságra hozatala, valamint a tinédzserek által megosztott tartalmak gyakran visszaélések célpontjai lehetnek, engedély nélküli felhasználás vagy később megbánt posztolások révén. Az ilyen „információs megsértések” lehetnek a fényképek vagy adatok engedély nélküli megosztása. Az adatvédelem kérdésköréhez tartozik a közösségi médiafiókok feltörésének problémaköre is [46, pp. 611-621] amelyhez kapcsolódik az az érzet, hogy a tinédzserek nagy számban aggódnak fiókjaik hackelésének lehetősége miatt. [47, pp. 1503-1504]

- adatvédelem (magánvédelem) az intelligens játékokban

Az internethez kapcsolódó, szenzorokkal és mikrofonokkal felszerelt intelligens játékok jelentős adatvédelmi kockázatot hordoznak, mivel folyamatosan gyűjtik és továbbítják a gyermekekről szóló információkat. Az eszközök gyenge biztonsági megoldásai miatt a személyes adatok, beszélgetések és tevékenységek illetéktelen hozzáférés tárgyává válhatnak, ami komoly magánszférabeli és pszichológiai kockázatokat eredményez. Ide sorolandó kockázatok:

- Gyenge titkosítás: Az intelligens játékokban alkalmazott elégtelen adatvédelmi algoritmusok következtében a kommunikáció könnyen feltörhető és visszafejthető.
- Audio injekciós támadás (audio sérüléses támadás): Olyan támadási forma, amelyben a készülékbe mesterséges hangparancsokat juttatnak be a működés manipulálására.
- Lehallgatás (eavesdropping): A játékok kommunikációs csatornáinak titkosítatlan vagy gyenge védelme lehetővé teszi a beszélgetések és hanganyagok illetéktelen rögzítését.
- Érzékeny információk kiszolgáltatása: A gyermekek által megadott adatok – például név, kor, helyszín – harmadik félhez kerülhetnek, sértve a magánszférát.
- Adatmegfigyelés, kémkedés: A beépített szenzorok és mikrofonok révén a felhasználói tevékenységek rejtett követése valósulhat meg.
- Gyermek reklám: A játékok adatgyűjtés útján célzott hirdetésekkel befolyásolhatják a gyermekek fogyasztói magatartását.
- Jogosulatlan távvezérlés: A hálózatra kapcsolt eszközök feletti illetéktelen irányítás lehetőséget ad a funkciók külső manipulálására.

Összegzés: Az okosjátékok, amelyek hangfelismerést vagy internetkapcsolatot használnak, komoly adatvédelmi kockázatokat hordoznak. A gyermekek gyakran adnak ki érzékeny információkat, vagy osztanak meg személyes adatokat az ilyen eszközökkel való játék során anélkül, hogy tisztában lennének a lehetséges következményekkel. Az okosjátékok technikai gyengeségei, mint a nem megfelelő titkosítás, lehetőséget biztosítanak arra, hogy illetéktelenek lehallgassák vagy módosítsák a hangfelvételeket. Emellett ezek az eszközök sok esetben adatokat gyűjtenek kereskedelmi célokra, például a gyermekek beszélgetéseiből vagy használati szokásaiból. [48]

Harmadik fél általi nyomonkövetés

- Az online szolgáltatások és alkalmazások gyakran harmadik felek – például hirdetők vagy adatbrókerek – számára is lehetővé teszik a felhasználói tevékenységek követését. Ez a gyakorlat különösen veszélyes a gyermekek számára, mivel böngészési szokásaik, érdeklődési körük és digitális interakcióik alapján részletes profilok épülhetnek róluk, amelyek célzott reklámokra, manipulációra vagy akár a magánszférájuk megsértésére adnak lehetőséget. Tipikus példa, amikor egy ingyenesen letölthető játékalkalmazás a háttérben adatokat továbbít harmadik félnek reklámcélú felhasználásra.

Összegzés: Az internetes tevékenységek nyomon követése szinte minden online tevékenységet érint, beleértve a gyerekek által használt weboldalakat és alkalmazásokat is. Eközben reklámcégek vagy elemzőplatformok azaz a „harmadik felek" adatokat gyűjtenek a felhasználók viselkedéséről, például böngészési szokásokról. A gyerekek adatvédelmi viselkedésére különböző tényezők vannak hatással, például a neveltetés, szociális normák vagy a technológiai ismeretek szintje. Ők még nincsenek tisztában azzal, hogy személyes adataikat követik és ezek az adatok hogyan kerülhet harmadik fél kezébe. Ezért fontos az adatvédelmi tudatosság növelése. [49]

Online zaklatás (online harassement)

Az online zaklatás olyan ismétlődő, ellenséges vagy sértő magatartás az online térben, amely a gyermekek pszichés, érzelmi és társas jóllétét egyaránt veszélyezteti. Ide tartoznak mindazon digitális interakciók, amelyek célja a megalázás, a megfélemlítés vagy a kiközösítés és amelyek gyakran tartós lelki terhelést eredményeznek. Tipikus példa, amikor egy gyermek közösségi médiában folyamatos gúnyolódás vagy bántó kommentek célpontjává válik. Ide sorolandó kockázatok:

- kiberbántalmazás (cyberbullying)
    - Lángolás (flaming vagy roasting): Ellenséges, durva vagy sértő üzenetek nyilvános online közzététele, amely konfliktusok kiélezésére szolgál.
    - Hínévrontás (denigration): Hamis, bántó vagy lejárató információk terjesztése a gyermekről a közösségi térben.
    - Megszemélyesítés (impersonation): Más személy online identitásának jogosulatlan felhasználása ártó vagy megtévesztő szándékkal.

- Álcázás (masquerading): Szándékos félrevezetés, amikor az elkövető hamis identitást hoz létre a gyermek becsapására vagy zaklatására.
- Outing: Bizalmas vagy érzékeny információk közzététele a gyermek beleegyezése nélkül, megalázó vagy sértő céllal.
- Csalás, trükkösködés (trickery): A gyermek megtévesztése annak érdekében, hogy érzékeny információkat osszon meg, amelyeket később visszaélésre használnak.
- Kiközösítés és kirekesztés: A gyermek szándékos kizárása online közösségekből vagy csoportokból, amely pszichés terhelést okoz.

Összegzés: A kiberbántalmazás a gyerekeket érintő kiberbiztonsági kockázatok közül az egyik leggyakoribb és legjobban kutatott terület. Ez a fajta zaklatás az internetképes technológiai eszköz (pl.: okostelefon, számítógép) használatával történik. A jelentősége és hatása rendkívül nagy mert a kiberbántalmazás súlyos pszichológiai és viselkedési problémákat idézhet elő a gyermekek és tinédzserek körében. Az elszenvedő gyermekben szorongást, depressziót és alacsony önbecsülést is indukálhat. [50, pp. 333-349]

- kiberzaklatás követéses formája (cyberstalking)
  - Lángolás (flaming): Olyan online kommunikációs forma, amelyben ismétlődő, ellenséges vagy zaklató üzenetek célzottan a gyermek megfélemlítésére irányulnak.
  - Személyazonosság-lopás (identity theft): A gyermek személyes adatainak illetéktelen megszerzése és felhasználása más identitásának megszemélyesítésére vagy bűncselekmények elkövetésére.
  - E-mail hamisítás (email forgery): Olyan technika, amely során az elkövető hamisított feladói adatokkal rendelkező elektronikus levelet küld, megtévesztve a címzettet a küldő személyazonosságáról.
  - Vírus: Kártékony szoftver, amely a gyermek eszközein futva adatvesztést, rendszerhibát vagy jogosulatlan hozzáférést eredményezhet.

Összegzés: Kiberzaklatás követéses formája a technológia (például számítógépek, okostelefonok, okoszeszközök) segítségével történő zaklatást és nem kívánt kommunikációt foglalja magában. Ez a fajta online zaklatás olyan helyzeteket idéz elő, ahol az áldozat folyamatosan veszélyben érezheti magát az ismétlődő, nem kívánt megkeresések miatt. A kiberzaklatás követéses formája az egyik leggyakoribb online

fenyegetés, amelyet a tinédzserek tapasztalhatnak. A kiberbántalmazás és a cyberstalking az online zaklatás két leggyakoribb formája, amelyek jelentős pszichológiai és érzelmi kockázatot jelentenek a gyerekek és tinédzserek számára. A kiberbántalmazás főként pszichológiai problémákhoz vezethet, míg a cyberstalking a folyamatos zaklatás és a személyes tér megsértésének érzését idézi elő. Mindkét esetben elengedhetetlen a szülők, tanárok és kiberbiztonsági szakemberek együttműködése, hogy megfelelő oktatási programokkal és támogató eszközökkel biztosítsák a gyerekek online biztonságát. [51, pp. 1-9]

Idegen veszély (stranger danger)

Az idegen veszély olyan kockázatokat foglal magában, amelyek során ismeretlen személyek megtévesztéssel vagy manipulációval próbálnak kapcsolatba lépni a gyermekkel. Ide sorolandó kockázatok:

- Kibercsalogatás (cybergrooming): Olyan manipulatív online magatartás, amelynek során egy felnőtt bizalmat épít a gyermekkel annak érdekében, hogy később kihasználja vagy szexuálisan zaklassa.
- Hamis online identitás létrehozása (catfishing): Hamis online identitás létrehozása és fenntartása a gyermek megtévesztése, érzelmi manipulációja vagy kihasználása céljából.
- Megszemélyesítés (impersonation): Más személy identitásának felhasználása abból a célból, hogy a gyermek bizalmát elnyerjék és így veszélyes helyzetbe sodorják.

Összegzés: A „stranger danger” az idegenekkel való kommunikáció során fellépő biztonsági fenyegetések gyűjtőfogalma. [52] Ezen belül a „cybergrooming” olyan online tevékenység, amely során egy felnőtt rejtett és káros szándékkal kapcsolatot épít ki egy gyermekkel az interneten keresztül, érzelmi kötődést kialakítva. A célja általában a gyermek manipulálása. Az online grooming jelentős kockázatot jelenthet, mivel a gyermekek érzelmi kötődés révén könnyen megtéveszthetőek. Ez az interakció veszélyes hosszú távú hatásokkal járhat, mind fizikailag, mind érzelmileg. A catfishing azt a fajta online környezetben történő megtévesztést jelenti, amikor valaki hamis személyazonosságot hoz létre, hogy másokat becsapjon. Gyermekek esetében ez különösen kockázatos, mivel könnyen elhitetik velük, hogy egy biztonságos kapcsolatot alakítottak ki valakivel, miközben az illetőnek rosszindulatú szándékai vannak. A

megszemélyesítés során valaki más nevében lép fel az online térben, gyakran a gyermekek manipulálásának vagy érzékeny információk megszerzésének céljával. Az ilyen típusú csalásokat gyakran kombinálják a cybergroominggal, hogy megerősítsék a gyermek bizalmát. Emellett a megszemélyesítés adatlopásra is felhasználható, például érzékeny információk eltulajdonítására vagy zsarolásra. [53]

Emberi bizalomra épülő támadások (social engeneering)

Emberi bizalomra épülő támadások (social engineering): Az ilyen típusú kockázatok az emberi pszichológia, a bizalom és a hiszékenység manipulálásán alapulnak, céljuk pedig érzékeny adatok megszerzése vagy a felhasználó megtévesztése. Ide sorolandó kockázatok:

- Adathalászat (phishing) és QR-kód alapú csalás (quishing): Olyan megtévesztő technikák, amelyek során a támadók hamis üzenetekkel vagy vizuálisan hitelesnek tűnő QR-kódokkal próbálnak jelszavakat, banki adatokat vagy más érzékeny információt kinyerni.
- Személyazonosság-lopás (identity theft): A gyermek személyes adatainak jogosulatlan megszerzése és felhasználása más identitás létrehozására, amely súlyos pénzügyi, jogi vagy reputációs következményekkel járhat.

Összegzés: A phishing, vagy adathalászat, az érzékeny információk megszerzésére irányuló csalárd tevékenység, amelyet a támadók általában megtévesztéssel érnek el. Bár ezt gyakran pénzügyi adatok ellopásával hozzák összefüggésbe a gyermekek is kiszolgáltatottak lehetnek az ilyen támadásokkal szemben hiszen a gyermekek gyakran nem tudják megkülönböztetni a hiteles és a nem hiteles weboldalakat, ezért könnyen megoszthatják érzékeny adataikat, például jelszavaikat vagy egyéb személyes információikat. [54, pp. 229-239] Az adathalászat egy speciális és talán a legfrissebb fajtája a QR kód alapú csalás (Quishing). Ebben az esetben egy ismert off-line felületre tett QR-kód matrica az adott weboldallal történő interakciót sugalja, pedig egy adathalász oldalra vezet. Az ott megadott adatok visszaélésre adnak lehetőséget.

A személyazonosság-lopás olyan kiberbiztonsági fenyegetés, amely során valaki egy másik személy adatait használja fel, gyakran az érintett tudta nélkül. A gyermekek még nem rendelkeznek kellő tudatossággal az adatvédelem terén és nem mindig értik, hogy az személyes információkat túlzott megosztása - például közösségi média platformokon vagy játékok során - milyen következményekkel járhat. Ide sorolandó kockázatok:

- Adathalászat (phishing): Olyan megtévesztő technika, amely során az elkövető e-mailben, telefonon vagy más csatornán keresztül próbál személyes adatokat megszerezni; gyermekek esetében tipikus előfordulás a hamis banki e-mail, amely jelszófrissítést kér.
- Hangalapú adathalászat (Vishing - voice phishing): Telefonhívások útján végrehajtott adathalászati forma, amely során a támadó hivatalos szereplőnek (pl. banki ügyintézőnek) adja ki magát; gyermekek körében ez leggyakrabban adatbekéréssel történő megtévesztés formájában jelenik meg.
- SMS-alapú adathalászat (smishing – SMS phishing): SMS-ben küldött megtévesztő üzenetekre épülő támadás, amely hamis linkek segítségével csalja ki a felhasználó adatait; gyermekek számára tipikus kockázat az adathalász weboldalra irányító üzenet.
- Csalogatás (baiting): Olyan manipulációs technika, amely során az áldozatot csábító ajánlattal vagy ajándékkal veszik rá érzékeny információk kiadására; gyermekek esetében tipikus példa az ingyenes zenei letöltés, amely valójában rosszindulatú programot tartalmaz.
- Előzetes kitalált történettel való megtévesztés (pretexting): Megtévesztésen alapuló támadás, ahol az elkövető egy előre felépített, hamis történettel igyekszik legitimálni adatbekérését; gyermekek körében jellemző forma, amikor valaki IT-támogatónak adja ki magát jelszó megszerzése céljából.
- Váll fölötti leskelődés (shoulder surfing): Olyan fizikai biztonsági kockázat, amikor a támadó közvetlen jelenlétben figyeli meg az áldozat képernyőjén vagy billentyűzetén bevitt adatokat; gyermekek esetében tipikus példa a PIN-kód ATM-nél történő ellesése.
- Jogosulatlan belépés követéssel (tailgating): Jogosulatlan behatolási módszer, amely során a támadó egy feljogosított személyt követve jut be védett területre; gyermekeknél ennek megfelelő kockázat lehet, ha valaki belépőkártya hiányára hivatkozva próbál áthaladni egy ellenőrzési ponton.

Tartalommal kapcsolatos kockázatok (content related risks)

Az interneten elérhető tartalmak sokrétűsége jelentős lehetőségeket kínál a tanulás és a szórakozás terén, ugyanakkor komoly veszélyeket is hordoz a gyermekek számára. Ezek a kockázatok egyrészt pszichológiai szinten jelennek meg, mivel a nem megfelelő, erőszakos vagy szexuális tartalmak torzíthatják a gyermekek világképét és érzelmi

fejlődését, másrészt jogi és társadalmi dimenzióval is bírnak, hiszen az illegális anyagokhoz való hozzáférés vagy a szerzői jogok megsértése közvetlen szabályozási és felelősségi kérdéseket vet fel. Ide sorolandó kockázatok:

- Nem megfelelő tartalom: Olyan anyagok, amelyek életkoruknál fogva káros hatással lehetnek a gyermekek fejlődésére és értékrendjére.
- Pornográfia: Szexuális jellegű tartalmak, amelyek a gyermekek számára korai és torzított képet közvetítenek az intimitásról.
- Célzott reklám: Adatgyűjtés alapján megjelenített hirdetések, amelyek befolyásolják a gyermekek fogyasztói magatartását.
- Erőszakos, káros, deviáns tartalom: Olyan vizuális vagy szöveges anyagok, amelyek erőszakot, önkárosítást vagy társadalmilag deviáns magatartást népszerűsítenek.
- Illegális tartalmak: Jogszabályba ütköző anyagok, amelyekhez való hozzáférés jogi és erkölcsi kockázatokat hordoz.
- Szerzői jog (copyright): Jogosulatlan tartalomhasználat, amely a gyermekeket jogsértő magatartásba sodorhatja.
- Spamek: Nem kívánt elektronikus üzenetek, amelyek félrevezető tartalmukkal és kártékony linkjeikkel adatvédelmi és biztonsági kockázatot jelentenek.

Összegzés: A gyermekek könnyen találkozhatnak olyan tartalmakkal, amelyek nem felelnek meg életkoruknak vagy tapasztalati szintjüknek. Ez egy gyakori kockázati tényező, amely negatívan befolyásolja fejlődésüket. [55] Az internetes pornográf tartalmakhoz való hozzáférés különösen súlyos veszélyt jelent a gyermekek számára, amellyel sok esetben akaratlanul szembesülnek. Az ilyen anyagok nemcsak érzelmi fejlődésükre hathatnak károsan, hanem hosszabb távon lelki és pszichés problémákat is okozhatnak. Ide sorolhatók a megtévesztő vagy félrevezető tartalommal bíró, gyermekeket célzó reklámok is. Különösen veszélyesek az olyan tolakodó (invazív) hirdetések, amelyek arra ösztönzik a kiskorúakat, hogy osszák meg személyes adataikat. Az erőszakos vagy káros tartalmak közé tartoznak a szélsőséges, veszélyes vagy elfajzott (deviáns) viselkedést népszerűsítő anyagok. Ezek fokozhatják az agressziót és a szorongást, valamint előfordulhat, hogy a gyermekek tiltott vagy bűncselekményekhez kapcsolódó tartalmakkal találkoznak. Ezek a kockázatok gyakran kevésbé láthatók, ám jelentős veszélyt hordoznak.

Szintén figyelmet érdemel, hogy a gyermekek tudtukon kívül jogvédett tartalmakkal kerülhetnek kapcsolatba: ilyeneket megoszthatnak vagy le is tölthetnek, amely előrevetíti a szerzői joggal összefüggő problémákat. Bár ez a fajta online viselkedés gyakran nem tudatos, mégis jogi következményekkel járhat.

A tartalommal kapcsolatos kockázatok közé tartoznak a spamek. A spamek kéretlen üzeneteket vagy tartalmakat jelentenek az online környezetben, amelyek gyakran nem megfelelő, félrevezető vagy káros anyagokat tartalmaznak és veszélyeztethetik a gyermekek biztonságát. [56]

Szexuális felbújtás (sexual solicitation) szexuális tartalmak megosztása

Az online térben a gyermekek különösen veszélyeztetettek a szexuális jellegű megközelítések és tartalmak miatt, amelyek súlyosan befolyásolhatják pszichoszexuális fejlődésüket és hosszú távú érzelmi, valamint társadalmi következményekkel járhatnak. E kockázatok nemcsak pszichológiai, hanem jogi szinten is kiemelt jelentőségűek: a gyermekpornográfia tilalma, a beleegyezési korhatárra vonatkozó szabályozások és a kiskorúak védelmét szolgáló büntetőjogi rendelkezések mind azt célozzák, hogy megakadályozzák a gyermekek szexuális kizsákmányolását és sérülékenységük kihasználását. Ide sorolandó kockázatok:

- Szexuális tartalmú üzenetküldés (sexting): Olyan gyakorlat, amikor a gyermek saját maga által készített szexuális jellegű képet vagy üzenetet oszt meg, amely később visszaélés és zsarolás tárgyává válhat.
- Kockázatos szexuális viselkedés / magatartás: Az online térben tanúsított olyan magatartásformák, amelyek szexuális kizsákmányoláshoz, pszichés sérüléshez vagy a gyermek önértékelésének torzulásához vezethetnek.
- Kiberszex: Virtuális térben zajló szexuális interakció, amely életkoruknál fogva felkészületlen gyermekeket vonhat be korai és jogilag tiltott szexuális élményekbe.

Összegzés: A sexting olyan tevékenység, amely során a gyermekek szexuális tartalmú képeket, videókat vagy üzeneteket küldenek vagy fogadnak az online térben. Ez az egyik leggyakoribb formája a szexuális zaklatásnak. Ennek tevékenységnek az a kockázata hogy a szexuális tartalmú képek, videók vagy üzenetek könnyen illetéktelen kezekbe kerülhetnek vagy visszaélésre adhatnak lehetőséget. A gyermekek nem mindig ismerik fel a következményeket és ezen online tartalmak megosztásának hosszú távú hatásait. A

kockázatos szexuális viselkedés / magatartás azt jelenti, hogy a gyermekek az online interakciók során olyan viselkedésformákba bocsátkoznak, amelyek veszélyeztetik a biztonságukat vagy érzelmi jólétüket. Az ilyen magatartás fokozhatja a gyermekek kiszolgáltatottságát és növelheti annak esélyét, hogy rosszindulatú egyének manipulálják őket. A kiberszex olyan tevékenységeket foglal magában, amelyek során a gyermekek online szexuális tevékenységekbe bonyolódnak vagy szexuális jellegű beszélgetéseket explicit tartalmakat osztanak meg. Ez érzelmi és adatvédelmi kockázatokkal jár hiszen illetéktelen kezekbe kerülve szexuális zaklatások vagy manipulációk célpontjává teszik őket melynek következményeként a gyermekek mentális egészsége és önbecsülése súlyosan károsodhat valamint személyes adatok kiszivárgásához és zsaroláshoz vezethet. [57, pp. 1205-1215]

Technológiai alapú fenyegetések

A technológiai eredetű kiberfenyegetések olyan rosszindulatú vagy visszaélésszerű műszaki mechanizmusokat jelentenek, amelyek a gyermekek digitális eszközein, hálózati kapcsolataikon vagy szolgáltatásain keresztül veszélyeztetik az adatvédelmet, az integritást és a felhasználói biztonságot. Ide sorolandó kockázatok:

- Rosszindulatú szoftver (malware): Olyan szoftverkomponensek gyűjtőfogalma, amelyek jogosulatlan működést, adatvesztést vagy rendszerteljesítmény-romlást okoznak; tipikus példa, amikor egy ingyenes játék telepítője rejtett kártevőt tartalmaz.
- Vírus: Reprodukcióra képes kártékony program, amely más fájlokhoz vagy rendszerelemekhez csatolódva terjed, adatvesztést vagy működési zavarokat idézve elő; gyermekeknél gyakran e-mail mellékletként vagy letöltött fájlok révén jelenik meg.
- Hekkelés (hacking) és QR-kód alapú csalás (quishing – QR-phishing): A hekkelés az eszközök vagy szolgáltatások jogosulatlan feltörését jelenti; a quishing esetében a gyermek egy játékhoz kapcsolódó plakáton szereplő QR-kód beolvasásával egy adathalász oldalra juthat.
- Zsarolóvírus (ransomware): Kártevő, amely titkosítja a felhasználói adatokat vagy lezárja az eszközt, majd kifizetést követel; gyermekek esetében előfordulhat, hogy egy ingyenes alkalmazás letöltése után az eszközön tárolt képek és fájlok elérhetetlenné válnak.

- Örökölt fenyegetések (legacy threats): Régebbi rendszerekben, elavult szoftverekben vagy gyenge konfigurációkban rejlő sérülékenységek; például egy régi, frissítetlen tablet biztonsági réseinek kihasználásával a gyermek adataihoz illetéktelenek férhetnek hozzá.
- Hamisítás (spoofing): A forrás vagy identitás meghamisítása (pl. feladó-cím, IP-cím vagy weboldal), amely megtévesztéssel juttatja rá a gyermeket adatszolgáltatásra; tipikus forma a hamisított közösségimédia-bejelentkezési oldal.
- Kémszoftver (spyware): Olyan rejtett programok, amelyek adatokat gyűjtenek és továbbítanak a támadó felé (pl. billentyűleütések, böngészési előzmények); előfordulhat például, hogy egy gyermek mobiljára telepített alkalmazás észrevétlenül követi a felhasználói tevékenységeket.

Összegzés: A malware a "malicious software" kifejezés rövidítése, amelyet rosszindulatú szoftverek gyűjtőfogalmaként használnak. Ezek a programok vagy kódok káros célokra készülnek és komoly kockázatot jelentenek a gyermekek online biztonságára az adatok ellopásával, rendszerek megbénításával vagy a gyermekek megtévesztésével. Ezek a szoftverek képesek érzékeny adatokat ellopni vagy károsítani az eszközök működését. A malware támadások gyakran személyes információk - például jelszavakhoz és banki adatok - megszerzésére irányulnak így súlyos következményekkel járhatnak.

A gyermekek online biztonságára hatással lévő technológiai alapú fenyegetéseknek egy másik jelentős csoportja: a számítógépes vírusok. A vírusok olyan káros programok, amelyek más fájlokat vagy rendszereket támadnak meg, gyakran észrevétlenül terjednek és adatvesztést, eszközkárosodást okoznak. A vírusok különösen akkor veszélyesek, amikor személyes adatokat próbálnak megfertőzni vagy ellopni a felhasználó tudta nélkül. A hekkelés olyan tevékenység, amely során a támadók hozzáférnek egy rendszerhez, például egy gyermek által használt eszközhöz vagy fiókhoz. A hekkerek manipulálhatják az eszközt, ellophatják a személyes adatokat vagy akár kárt is okozhatnak az informatikai rendszerekben. Az ilyen típusú támadások különösen fontosak, mivel a gyermekek gyakran nem rendelkeznek elegendő tudással ahhoz, hogy felismerjék a hekkerek próbálkozásait. [58, pp. 82-85] A zsarolóvírusok olyan típusú rosszindulatú szoftverek (malware-ek), amelyek titkosítják a felhasználó fájljait és váltságdíjat kérnek azok visszaállításáért. A gyermekek online környezetében ezek a támadások is kockázatot jelenthetnek, mivel olyan értékes információk mint például

fényképek vagy iskolai anyagok is veszélybe kerülhetnek. Az örökölt fenyegetések olyan technológiai kockázatok, amelyek a régebbi eszközök és szoftverek biztonsági gyenge pontjaiból adódnak. Az ilyen fenyegetések különösen veszélyesek lehetnek, ha a gyermekek régebbi rendszereket használnak – például olyan régebbi számítógépet vagy okoskészüléket - amelyek nem rendelkeznek a legfrissebb biztonsági frissítésekkel és védelmi mechanizmusokkal. A hamisítás (spoofing) olyan támadási forma, amikor egy kibertámadó más személynek vagy entitásnak adja ki magát, hogy megtévessze a célszemélyt. A gyermekek esetében ez gyakran azt jelenti, hogy egy másik személy - például egy barát vagy egy családtag - identitásával próbálnak kapcsolatba lépni a célzott gyermekkel. Ide tartozik még a hamisított e-mailek vagy weboldalak is amelyek gyakran alkalmazzák ezt a módszert, hogy ellopják a kiskorú felhasználók adatait. A kémszoftverek olyan programok, amelyek titokban nyomon követik a felhasználó tevékenységét, adatokat gyűjtenek és továbbítanak a kibertámadónak. A gyermekek esetében ezek a programok különösen veszélyesek, mert titokban nyerhetnek információkat a személyes használatról, beleértve a jelszavakat, böngészési előzményeket, vagy más érzékeny adatokat.

Gazdasági alapú kockázatok (economy risks)

Gazdasági alapú kockázatok: Az online térben a gyermekek nemcsak adatvédelmi, hanem pénzügyi jellegű fenyegetéseknek is ki vannak téve, amelyek a megtévesztés, a manipuláció és a jogtalan pénzszerzés különféle formáiban jelenhetnek meg. Ide sorolandó kockázatok:

- Online szerencsejáték: Digitális platformokon zajló játékok, amelyek pénzügyi kockázatot hordoznak és a gyermekeket könnyen függőségbe vagy anyagi veszteségbe sodorhatják; tipikus példa az ingyenesnek hirdetett, de valójában fizetős funkciókat kínáló játékoldal.
- Pénzügyi csalások (financial scams): Olyan megtévesztő technikák összessége, amelyek célja anyagi előnyszerzés; gyermekek esetében leggyakrabban online vásárlásokhoz, játékbeli tranzakciókhoz vagy előfizetésekhez kapcsolódva jelennek meg.
    - Személyazonosság-lopás (identity theft): A gyermek személyes adatainak jogosulatlan megszerzése és felhasználása pénzügyi

tranzakciókhoz vagy új fiókok létrehozásához; például bankkártya-adatok illetéktelen felhasználása.

- Csaló hívások (scam calls): Telefonon keresztül történő megtévesztési kísérlet, amikor az elkövető hivatalos szereplőnek (pl. szolgáltatónak) adja ki magát pénzügyi adatok megszerzése érdekében; gyermekeknél tipikus helyzet, ha ismeretlen számról érkező hívásban előfizetési adatok megadását kérik.

Tekintve hogy a fiatalok könnyen hozzáférhetnek az interneten elérhető szerencsejáték oldalakhoz, előfordulhat, hogy pénzt költenek szerencsejátékokra anélkül, hogy teljesen tisztában lennének a pénzügyi következményekkel. [59] Az ilyen típusú játékok és az online játékok egyébként nem feltétlenül kiberbiztonsági kockázatok, de a gyermekek döntéseinek következménye hosszú távon befolyásolhatja viselkedését, családi viszonyait és komoly anyagi kihatásai lehetnek. Az online játékokban való vásárlások pénzügyi kockázatokat rejthetnek hiszen a gyermekek könnyen találkozhatnak olyan helyzetekkel amikor nem tudják eldönteni, hogy a játékban elérhető extra funkciók vagy prémium szolgáltatások pénzbe kerülnek és akár véletlenül vásárolhatnak különféle termékeket. Az ilyen vásárlások esetén gyakran előfordul, hogy a szolgáltatók nem tisztázzák, hogy az alapjáték ingyenes, de további költségek merülhetnek fel a használat során. Az ilyen események során a gyermekek jelentős összegeket veszíthetnek el csaló tranzakciók következtében.

A pénzügyi csalások a gyermekek számára is komoly veszélyt jelenthetnek. A személyazonosság-lopás (identity theft) és a csaló hívások (scam calls) révén. A személyazonosság-lopás során a támadók a gyermekek személyes adatait szerzik meg – a nevüket, a címüket, jelszavaikat vagy a banki adataikat - hogy azokkal visszaéljenek. Ez gyakran phishing (adathalász) támadások révén történik meg, ahol a gyermekek hamis weboldalakon adhatják meg ezeket az érzékeny információkat. A csaló hívások során a gyermekeket vagy szüleiket telefonhívásokkal próbálják megtéveszteni. A támadók különféle technikákat alkalmaznak, hogy rávegyék őket pénz átutalására vagy személyes adataik megadására. A gyermekek esetében a gyanútlan válaszok és a könnyű manipuláció miatt ezek a támadások különösen veszélyesek. [56]

Internetfüggőség (internet addiction)

Ide sorolandó kockázatok:

- Internetfüggőség (internet addiction): Az internetfüggőség a viselkedési addikciók egyik formája, amelyben a gyermekek túlzott és kontrollálatlan internethasználata zavarokat okoz a mindennapi életük különböző területein, így például a tanulási teljesítményben, a társas kapcsolatok minőségében és a pszichés jólétben. Pszichológiai szempontból a túlhasználat fokozott szorongáshoz, alvászavarokhoz és társas izolációhoz vezethet, míg jogi és szabályozási dimenzióban a problémát az ENSZ Gyermekjogi Egyezményében rögzített egészséges fejlődéshez való jog, valamint a kiskorúak védelmét célzó nemzeti programok keretében kezelik. Tipikus előfordulási forma a közösségi média, az online játékok vagy a videómegosztó platformok túlzott használata, amelyek fokozott kockázatot jelentenek a gyermekek számára.

Az internetfüggőség önálló kiberbiztonsági kockázatként nem értelmezhető de a gyermekek és fiatalok körében az internetfüggőség növelheti a kockázatos online viselkedések előfordulásának valószínűségét és hasonló negatív fizikai és viselkedési következményekkel járhat, mint más típusú kiberbiztonsági veszélyek. [60, pp. 495-503] Azon gyermekek és fiatalok akik túlzottan elmerülnek az online térben, gyakrabban válhatnak olyan online fenyegetések áldozatává, mint a személyes adatok kiszivárgása vagy csalások.

Jelszókezelés gyakorlata (password practice and management)

Ide sorolandó kockázatok:

- A jelszókezelés gyakorlata a gyermekek digitális biztonságának egyik alapvető tényezője, amely a jelszavak létrehozásának, használatának és tárolásának módját foglalja magában. A nem megfelelő jelszóhasználat – például egyszerű, könnyen kitalálható jelszavak alkalmazása, azonos jelszó több felületen való használata vagy a jelszavak nyílt megosztása – jelentős kockázatot hordoz, mivel elősegíti a fiókok feltörését, az illetéktelen hozzáférést és a személyes adatok kiszivárgását. Gyermekek esetében különösen gyakori probléma a rövid, játékokhoz vagy kedvenc figurákhoz kapcsolódó jelszavak alkalmazása, amelyek nem nyújtanak kellő védelmet.

A megfelelő jelszóhasználat nemcsak az online fiókok védelmét szolgálja, hanem az egészséges digitális szokások kialakításához is hozzájárul, amelyek segítenek a gyermekeknek abban, hogy biztonságosan navigáljanak az online világban. A

jelszókezelés gyakorlata kulcsfontosságú tényező a gyermekek online biztonságának biztosításában. Mivel a gyermekek egyre inkább kapcsolatba kerülnek az online világgal fontos, hogy megfelelő tudással és készségekkel rendelkezzenek a jelszavak biztonságos használatára vonatkozóan. A jelszavak gyenge kezelése vagy azok helytelen használata könnyen vezethet adatlopáshoz, személyazonosság-lopáshoz és egyéb kiberfenyegetésekhez. [61, pp. 1-19]

1.6 Vonatkozó elméletek és releváns megközelítések

Az alábbiakban megvizsgálom azokat az elméleteket és teoretikus megközelítéseket, melyek a gyermekek kiberbiztonsági tudatosság növelésére irányuló kutatásokban relevánsnak bizonyultak. Ezen megközelítések és elméletek segítségével vizsgálható, hogy milyen tényezők befolyásolják a gyermekek kiberbiztonsági tudatosságát és hogy hogyan lehet ezeket a tényezőket megismerni, kezelni és felhasználni.

Adatvédelmi kalkulus elmélet

Az adatvédelmi kalkulus elmélet egy olyan kognitív modell, amely arra törekszik, hogy megmagyarázza, milyen gondolatmenetek zajlanak le az egyénekben, amikor személyes adataik megosztására kérik őket. [62, pp. 1-10] Az elmélet szerint az egyének saját értékeik és tapasztalataik alapján hozzák meg döntéseiket úgy hogy felmérik az adatmegosztással járó előnyöket (pl.: személyre szabott szolgáltatások, közösségi élmények) és hátrányokat (pl.: adatvédelmi kockázatok, identitáslopás) ezáltal egyfajta költség-haszon elemzést végeznek, mielőtt döntést hoznak.

Ha egy felhasználónak lehetősége van egy új közösségi média platformon regisztrálni, akkor az adatvédelmi kalkulus elmélete szerint a következőket mérlegeli:

- Előnyök: Új barátok szerzése, érdekes tartalmak megosztása, személyre szabott hírfolyam, stb.
- Hátrányok: Kiberbiztonsági veszélyek, adatvédelmi kockázatok (pl. személyes információk kiszivárgása, hirdetések, időpazarlás, stb.).

Az elmélet rámutat arra, hogy az emberek nem mindig hoznak racionális döntéseket és az egyének nemcsak passzív résztvevői a kibertér szabályozásainak, hanem aktív szereplői is, akik saját döntéseikkel alakítják az online környezetet és saját biztonságukat. Segít megérteni, hogy miért hajlamosak az emberek bizonyos online szolgáltatásokat használni, még akkor is, ha tudatában vannak az adatvédelmi kockázatoknak.

Vygotsky proximális fejlődési zóna elmélete

Vygotsky proximális fejlődési zóna (Vygotsky's Zone of Proximal Development, ZPD) elmélete a tanulók által önállóan és egy képzettebb partner, mentor vagy szülő irányításával elérhető eredmények közötti különbséget mutatja be. Az egyén ZPD-je a különbség aközött, amit segítség nélkül meg tud tenni és aközött, amit segítséggel képes megtenni. [63]

A ZPD folyamata: A tapasztaltabb személy felméri a tanuló jelenlegi tudásszintjét és képességeit, majd ezt követően meghatározza, hogy milyen készségeket szeretne a tanulónál fejleszteni és milyen támogatásra van szüksége ahhoz hogy ezeket a készségeket elsajátítsa. Ezt követően a tapasztaltabb személy olyan támogatást nyújt a tanulónak, amely segíti őt fejlődni. A folyamatban a támogatásnak fokozatosan csökkennie kell, ahogy a tanuló egyre önállóbbá tudjon válni.

Információbiztonság tudatosítása szempontjából Vygotsky ZPD elmélete felhasználható az oktatók számára a megfelelően támogató tanulási környezet kialakításához, szülői szempontból alkalmazható a gyermekek kiberbiztonsági fejlődésének segítésére valamint kiberbiztonsági szakemberek és mentorok számára a gyerekek fejlődésének támogatására.

Nissenbaum kontextuális integritás elmélete

Az elmélet szerint az információ az adott helyzetet szabályozó normák szerint áramlik. Ezek a normák a kulturális, etikai, erkölcsi és jogi tényezők kontextusától függően változnak. Az elmélet alkalmazásával elemezhető, hogy egy adott információáramlás sérti-e a kontextuális integritást, megfelel-e az adott kontextusban érvényes normáknak és elvárásoknak. Abban az esetben ha az információáramlás nem felel meg ezeknek a normáknak, akkor az lehetséges információbiztonsági kockázatot jelent.

A keretrendszer elemei:

- Kontextus: Az adott helyzet, amelyben az információáramlás történik.
- Attribútumok: Az információ jellemzői (tartalom, érzékenység, pontosság).
- Szereplők: általános iskolás korú gyermekek, akik részt vesznek az információáramlásban.
- Átviteli elvek: szabályok, szabályozási keretek és mechanizmusok, amelyek meghatározzák, hogy az információk hogyan áramlanak a különböző szereplők között.

Az információáramlás a kulturális, etikai és jogi normák mentén történik. Nissenbaum kontextuális integritás elmélete egy olyan keretrendszer amely segíti a hatékony adatvédelmi politika kialakítását, mert figyelembe veszi a különböző kontextusokban

érvényes normákat és elvárásokat. Segít az olyan technológiák fejlesztésében, amelyek tiszteletben tartják a gyermekek magánéletét valamint segítő szempontokat ad a gyermekek magánéletét védő jogszabályok kidolgozásához is. [64] Fontos megjegyezni azonban, hogy ez az elmélet nem ad konkrét válaszokat az adatvédelemmel kapcsolatos kérdésekre, hanem egy gondolkodási keretet biztosít a további vizsgálatokhoz. Ez az elmélet a magánélet normáira összpontosít, amelyek a helyzet kontextusától függően változik.

Piaget kognitív fejlődési elmélete

Jean Piaget svájci pszichológus kognitív fejlődési elméletében négy fő szakaszt különböztetett meg. Ezek:

- Szenzomotoros szakasz (0-2 év): A csecsemő a világ megismerését érzékszervi és szenzomotoros tapasztalatain keresztül szerzi. A tárgyállandóság kialakulása is ekkor történik meg.
- Műveletek előtti szakasz (2-7 év): A gyermek szimbolikus gondolkodásra képes lesz, de gondolkodása még egocentrikus és nem mindig képes a megmaradás elvét megérteni.
- Konkrét műveletek szakasza (7-12 év): A gyermek képes logikai műveleteket végezni konkrét tárgyakon és eseményeken. A megmaradás elvét is megérti.
- Formális műveletek szakasza (12 évtől): A serdülő képes elvont fogalmakkal gondolkodni, hipotéziseket felállítani és ellenőrizni.

Ez alapján a kognitív fejlődési elmélet azt sugallja, hogy a gyerekek a konkrét műveleti szakaszban (nagyjából 7-12 éves korukban) már képesek "megjeleníteni a dolgokat a fejükben". [65] Az elmélet 21. századi kiberbiztonsági vonatkozása az, hogy ez alapján ebben az életkorban a gyermekeknek már elég kompetensek ahhoz, hogy önállóan használják a digitális eszközöket és kockáztathatják a magánjellegű információk közlését és megosztását. Ez azonban potenciálisan kockázatot jelent a magánéletük védelme szempontjából.

ARCS motivációs modell

Az ARCS motivációs modellt John M. Keller amerikai pedagógus - pszichológus fejlesztette ki és a tanulók motivációjának fokozására szolgál. A modell négy fő komponensre épül és egyben ezen szavak betüiből áll össze az ARCS mozaikszó. Ezek:

- Figyelem (Attention): Első lépés a gyerekek érdeklődésének felkeltése és a figyelmük fenntartása. Ez olyan stratégiákkal érhető el, mint a valós példák alkalmazása, humor, vagy éppen meglepő elemek beépítése a feldolgozandó (tan)anyagba.

- Relevancia (Relevance): A gyerekeknek meg kell érteniük, hogy a tanult anyag miért fontos számukra és hogyan kapcsolódik az életükhöz. A relevancia érzékeltetése segíti a gyerekeket motiváltabbá válni.
- Önbizalom (Confidence): A gyerkeknek el kell hinniük, hogy képesek a feladatok megoldására. Az önbizalom erősítéséhez fontos a pozitív visszajelzés és a kis lépésekben történő haladás valamint a megfelelő támogatás nyújtása.
- Elégedettség (Satisfaction): A gyerekeknek elégedetteknek kell lenniük a tanulás eredményeivel. Ez sikerélmény kialakulásához vezet és a tanulás folytatásához vezető motivációt erősíti.

Az ARCS motivációs modell egy hatékony eszköz az oktatók (tanárok, szülők) kezében, amellyel a gyerekek motivációját fokozhatják és a tanulási folyamatot eredményesebbé tehetik. A modell alkalmazásával a tanulók jobban megértik az anyagot, elkötelezettebbé válnak a tanulás iránt és nagyobb valószínűséggel érik el a kitűzött céljaikat és segítségével olyan eszközöket lehet alkalmazni és szoftvereket fejleszteni, amelyek a általános iskolás korú tanulók számára érdekesebbé és motiválóbbá tehetik a kiberbiztonsági ismeretek elsajátítását. [66]

APCO makromodell

Az APCO makromodell egy olyan elméleti keretrendszer, amelyet a serdülőkorban lévő fiatalok online adatvédelmi viselkedésének megértésére dolgoztak ki. Nevét az angol Antecedents, Privacy Concerns, Outcome kifejezések kezdőbetűiből kapta, amelyek magyarul a következőképpen fordíthatók: Előzmények (Antecedents), Adatvédelmi aggodalmak (Privacy Concerns), Következmények (Outcome). [67] A modell célja annak feltárása, hogy mely alapvető folyamatok befolyásolják a fiatalok személyes adatok megosztásával kapcsolatos döntéseit.

A keretrendszer két fő szemléletet egyesít: a kockázatvállalási magatartás és a társas tanulás megközelítését. A modell értelmezése szerint a kamaszkorban lévő fiatalok hajlamosabbak a kockázatvállalásra, ami hatással lehet online adatvédelmi döntéseikre. Az adatvédelemmel kapcsolatos ismereteiket szüleiktől, barátaiktól és a médiából sajátítják el és ezek a külső társas hatások alakítják saját viselkedésüket. Az APCO modell fő elemei:

- Tudás: A fiatalok ismeretei az adatvédelemmel kapcsolatban.
- Attitűdök: A fiatalok véleménye és érzései az adatvédelemmel kapcsolatban.
- Szubjektív normák: A fiatalok azon elképzelései, hogy mások mit várnak tőlük az adatvédelem terén.
- Érzekelhető kontroll: A fiatalok azon meggyőződése, hogy képesek irányítani az online adatvédelmi helyzetüket.

Az APCO modell fontos hozzájárulás az adatvédelmi kutatásokhoz, mivel segít megérteni, hogy a fiatalok miért hoznak bizonyos döntéseket személyes adataik megosztásával kapcsolatban. A modell alkalmazásával hatékonyabb adatvédelmi oktatási programokat lehet fejleszteni, amelyek figyelembe veszik a fiatalok egyedi jellemzőit és szükségleteit.

A rugalmasság elmélete

A rugalmasság elmélete (resilience theory) arra a képességre utal, hogy az egyének, közösségek vagy rendszerek képesek alkalmazkodni, helyreállni és fejlődni nehéz helyzetekben vagy traumatikus események után. Ez az elmélet nemcsak a pszichológiában, hanem a kiberbiztonság területén is egyre nagyobb figyelmet kap, különösen a gyermekekkel kapcsolatban. A rezilienciaelmélethez kapcsolódó eredmények nem egyszerűen azt jelentik, hogy a tizenévesek ki vannak-e téve kockázatnak, hanem azt, hogy képesek-e ennek ellenére boldogulni. [68]

Hogyan kapcsolódik a „rugalmasság elmélete" a gyermekek kiberbiztonságához? A reziliens gyermekek könnyebben képesek megbirkózni az online veszélyekkel, mint azok, akik kevésbé rugalmasak. Ezek a gyermekek számos kiberbiztonsági veszélyhelyzetet másként kezelnek: kevésbé érzékenyek a negatív megjegyzésekre és hatékonyabban védekeznek az online zaklatás ellen, jobban tudják szabályozni az interneten eltöltött időt és kevésbé hajlamosak az internetfüggőségre valamint biztosabban navigálnak az online térben és könnyebben felismerik az online veszélyeket. Ezáltal tudatosabban hozzák meg döntéseiket.

Az online tér számos kihívást jelent az általános iskolás korú gyermekek számára, mint például a kiberzaklatás, a hamis információk terjedése és az online adathalászat. A rugalmas gyermekek jobban felkészültek lehetnek ezekkel a kihívásokkal szemben és egészségesebb kapcsolatot alakíthatnak ki a technológiával. A gyermekek önbizalmának erősítésével, olyan biztonságos és támogató környezet kialakításával ahol kifejezhetik érzéseiket és gondolataikat valamint problémamegoldó készségeik és digitális tudatosságuk fejlesztésével hozzá lehet járulni a gyermekek rezilienciájának fejlődéséhez.

A rugalmasság elmélete fontos eszköz a gyermekek kiberbiztonságának megértésében és fejlesztésében. A szülők, pedagógusok és a társadalom egészének felelőssége, hogy segítsék a gyermekeket rugalmasabbá válni.

Védelmi motivációs elmélet és az egészséghit-modell

A védelmi motivációs elmélet (Protection Motivation Theory - PMT) a veszélyek észlelésére és a kockázatos magatartás elkerülésére összpontosít. A védelmi motiváció

elmélet szerint az emberek két tényező alapján védik magukat: a fenyegetettség és a megküzdés értékelése alapján. A fenyegetésértékelés a helyzet súlyosságát értékeli és azt vizsgálja, hogy mennyire súlyos a helyzet, míg a megküzdési értékelés azt jelenti, hogy az ember hogyan reagál a helyzetre. [69] Az egészséghit-modell (Health Belief Model, HBM) egy pszichológiai megközelítés, amely az egyének hozzáállására és meggyőződéseire összpontosítva igyekszik értelmezni és előre jelezni az egészséges viselkedést. [70] A PMT és HBM elméletek segíthetnek megérteni, hogy az online térben a gyermekek miért döntenek egy bizonyos módon és hasznosak lehetnek a gyermekek online kockázatokkal kapcsolatos érzékelésének és viselkedésének megértésében. A gyermekek nagyobb valószínűséggel fogadnak el online biztonsági tanácsokat, ha érzik és megértik hogy az online kockázatok őket is érintik és hisznek abban, hogy a biztonsági intézkedések hatékonyak lehetnek.

A családi rendszerek elmélete

A családi rendszerek elmélete (Family Systems Theory) a családot egy összetett, dinamikus rendszerként fogja fel, amelyben a tagok kölcsönösen hatnak egymásra. Az elmélet szerint a család nem csupán az egyéni tagok összessége, hanem egy egységes rendszer, ahol mindenki másoktól függ és mindenki hatással van a rendszer egészére. [71] Az elmélet alapelvei:

- Kölcsönös függőség: A családtagok viselkedése és érzelmei egymásra hatnak; egyetlen tag változása az egész családi rendszerre kihatással lehet.
- Körkörös okság: A családon belüli ok-okozati kapcsolatok nem lineárisak, hanem kölcsönösen visszahatóak. Egy eseménynek egyszerre lehet több oka és következménye.
- Egyensúlyi törekvés (homeosztázis): A család rendszerszerűen igyekszik fenntartani a stabilitást. Ha ez felborul, a tagok olyan válaszokat adnak, amelyek a korábbi egyensúly helyreállítását szolgálják.
- Alrendszerek: A családon belül sajátos működésű alrendszerek különíthetők el (például a szülői vagy testvéri kapcsolatok), amelyek saját szabályrendszerrel és működési mechanizmusokkal rendelkeznek.

A család dinamikája jelentős hatással van a gyermekek kiberbiztonságára. Amennyiben a szülők és a gyermekek között nyílt és őszinte kommunikáció van, akkor a gyermekek nagyobb valószínűséggel beszélnek a szüleiknek az online problémáikról és így hatékonyabb védelmet kaphatnak. A családi rendszerek elmélete segíthet megérteni, hogy a gyermekek online viselkedését számos tényező befolyásolja és hogy ebben a családnak fontos szerepe van. Az elmélet alapján a szülők és a szakemberek olyan beavatkozásokat dolgozhatnak ki, amelyek erősítik a családi kapcsolatokat és támogatják a gyermekek biztonságos online jelenlétét.

Szülői közvetítés elmélete

A szülői közvetítés elmélete (Parential Mediation Theory) azt vizsgálja, hogy a szülők milyen stratégiákat alkalmaznak gyermekeik médiafogyasztásának alakítására és hogy ezek a stratégiák milyen hatással vannak a gyermekek médiával kapcsolatos tapasztalataira és viselkedésére. Az elmélet alapelvei:

- A szülők aktív szerepet játszanak gyermekeik médiahasználatának alakításában.
- A szülők különböző módszereket és stratégiákat alkalmazhatnak a média szokások kialakitásában és nevelésében mint például az egyidőben történő közös média használat, a tartalom korlátozása, a tartalomról való beszélgetés vagy a saját példamutatás.
- A szülői közvetítés hatása függ a gyermek életkorától, személyiségétől és a családi környezettől.

A szülői közvetítés fontos szerepet játszik a gyermekek online biztonságában. Azok a gyermekek, akiknek szülei aktívan részt vesznek az online tevékenységeikben, általában jobban tisztában vannak az online veszélyekkel és kevésbé hajlamosak kockázatos viselkedésre. [72] A szülői közvetítés elmélete alapján a szülők számos módszert alkalmazhatnak gyermekeik online biztonságának megőrzése érdekében. Ilyen módszer a közös internetezés is ahol a szülők és gyermekeik együtt töltenek online időt és beszélgetnek arról amit látnak és tapasztalnak. Fontos, hogy a szülők és a gyermekek között nyílt és őszinte kommunikáció legyen az online világról valamint hogy a szülők állítsanak fel világos szabályokat a gyermekek internetes használatára vonatkozóan és következetesen tartsák be azokat. A szülők legyenek példaképek gyermekeik számára és mutassák meg nekik, hogyan használják biztonságosan az internetet.

A szülői közvetítés elmélete rávilágít arra, hogy a szülőknek fontos szerepük van gyermekeik online biztonságának megőrzésében. Azáltal, hogy aktívan részt vesznek gyermekeik online életében és megfelelő stratégiákat alkalmaznak a szülők segíthetnek gyermekeiknek biztonságosan és felelősségteljesen navigálni az online világban.

1.7 Gyermekek információbiztonságával összefüggő jogszabályi keretek vizsgálata

Az adatbiztonság és információbiztonság megerősítésének egyik lehetséges módszere, hogy jogszabályokat, vonatkozó szabályozásokat, valamint ajánlásokat és irányelvek hoznak létre jogszabályalkotói hatáskörben. Az információbiztonsági incidensek előfordulása a részben a jogszabályi szabályozás hiányára vagy azok nem megfelelő betartására is visszavezethető. Ezek a jogszabályok és szabályozások általában azonosítják az információbiztonsági kockázatokat, előírják a megelőző intézkedéseket és

javasolják a válaszlépéseket az incidensek esetén. Az információbiztonsági incidensek nagyon változatosak lehetnek, így a jogszabályi szabályozásnak is széles körűnek kell lennie ahhoz, hogy hatékonyan tudjon reagálni a különféle helyzetekre. A következő táblázatban időrendi rendezés szerint összefoglalom az informatika történetének nemzetközi mérföldköveit amelyek hatással voltak információbiztonság és az adatvédelem szabályozásának kérdésére. A tudományos probléma feldolgozását korábban a National Security Review tudományos folyóiratban megjelent tanulmányomban ismertettem, amelyre az irodalomjegyzékben is hivatkozom. [73]

Évszám	Informatikai információbiztonsági események
1969	Advanced Research Projects Agency Network (ARPANET) az internet elődjének megállapítása
1971	Első e-mail elküldése
1984-1991	TRW adatlopás - Az Amerikai Szövetségi Nyomozó Iroda (FBI) nyomozása során derült ki, hogy egy amerikai kormányzati vállalkozás titkosan gyűjtött adatokat több millió amerikai állampolgárról.
1989-1991	World Wide Web (www.) megjelenése
1990	AT&T adatlopás - A Bell Labs (az AT&T kutatási egysége) több mint 300 000 személyes adatot veszített el, amikor a rendszerét feltörték.
1991	Első weboldalak megjelenése
1993	Első webböngésző (Mosaic) megjelenése (1993.04.22.)
1993-1994	Az első keresőmotorok (Archie, Veronica, Excite) megjelenése
1995	Az első online kiskereskedők (Amazon, Ebay) megjelenése
1995	Citibank adatlopás - a bank több mint 200 ezer személyes adatot veszített el, amikor kiberbűnözők támadták meg a rendszerét.
1998	Google kereső alapítása
1999	eBay adatlopás - online kereskedelmi oldal több mint 4 millió felhasználójának személyes adata került illetéktelen kezekbe.
2000	Google AdWords megjelenése - az AdWords lehetővé tette a hirdetők számára, hogy célzott reklámokat jelenítsenek meg a Google keresési eredményei között.
2001	Wikipédia indítása
2004	Facebook alapítása
2005	YouTube indulása
2007	iPhone megjelenése - az Apple által kifejlesztett okostelefon jelentős változást hozott a mobiltechnológiában és megnyitotta az utat az alkalmazások és a mobilfizetés terén.
2008	Cloud Computing elterjedése - az Amazon Web Services az első nagy felhőalapú szolgáltatás elindulása.
2009	Bitcoin indulása
2010	Mobil internet elterjedése - Az okostelefonok és táblagépek elterjedése jelentősen megnövelte a mobilinternet használatát és az internetezők többsége már mobil eszközön keresztül fér hozzá az internethez.
2010	Instagram indítása
2011	Snapchat indítása
2011	Facebook Messenger elindítása
2016	Pokémon Go - Az okostelefonokhoz kapcsolódó játék hatalmas népszerűségre tett szert és az augmented reality (AR) technológia újabb dimenziót nyitott meg az internetes játékok számára.
2020	Covid-19 pandémia hatása - az élet minden területén jelentős változásokat hozott. Az internet és a digitális technológia még fontosabbá vált a munka az oktatás a szórakozás és a kapcsolattartás terén.
2020	5G hálózatok megjelenése lehetővé teszi a nagyobb adatátviteli sebességet és a megbízhatóbb kapcsolatot, ami jelentős hatással lesz az internet használatára.
2020-2021	Blockchain technológia elterjedése - blokklánc technológia új lehetőségeket kínál az adatbiztonság, az adatvédelem terén és számos új iparág fejlődését segíti elő.
2022-2023	ChatGPT és egyéb mesterséges intelligenciák megjelenése - AI fejlődése és alkalmazása egyre fontosabbá válik a digitális technológia területén és számos új lehetőséget kínál az internetes szolgáltatásokban.

2.sz. táblázat: Informatika történetének nemzetközi mérföldkövei (saját szerkesztés)

A következőkben áttekintem azokat a jogi szabályozási mérföldköveket, amelyek az informatikai és információbiztonsági eseményekre adott válaszként jöttek létre. Ezek a szabályozások nemcsak technológiai szempontból reagálnak a gyorsan változó digitális környezet kihívásaira, hanem alapvetően befolyásolják azt is, hogy milyen jogi és

intézményi keretek között valósulhat meg a gyermekek, szülők és pedagógusok információbiztonsági védelme. [73]

Évszám	Információbiztonság és adatvédelem jogi szabályozása
1980	Gazdasági Együttműködési és Fejlesztési Szervezet – Irányelvek a magánélet védelméről és a személyes adatok határokon átívelő áramlásáról (OECD – Organisation for Economic Co-operation and Development – Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)
1981	Európa Tanács Egyezménye az Egyének Védelméről Személyes Adatok Gépi Feldolgozása Során
1983	Német alkotmánybíróság népszámlálási ítélete (Volkszahlungsurteil), mely explicit módon kimondja, hogy az egyén általános személyiségi jogának védelmével, ezen belül információs önrendelkezési jogával és a demokratikus társadalmi berendezkedéssel, valamint az ezt szolgáló jogrenddel egyaránt összeegyeztethetetlen egy olyan információs helyzet, melyben a polgár nem tudhatja, kik, mikor és milyen célból rendelkeznek róla információval"
1992	1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról [1]
1995	AZ EURÓPAI PARLAMENT ÉS A TANÁCS 95/46/EK IRÁNYELVE a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról
2005	2004. évi XC. törvény az elektronikus információszabadságról
2011	Az Európai Parlament és a Tanács 2011/93/EU irányelve a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről, valamint a 2004/68/IB tanácsi kerethatározat felváltásáról
2011	2010. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról – Magyarország
2016	AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 (GDPR) RENDELETE a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)
2016	AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/680 IRÁNYELVE a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi keret határozat hatályon kívül helyezéséről
2018	Általános Adatvédelmi Rendelet – hatályba lépés (2018) (GDPR – General Data Protection Regulation, 2018, European Union)
2021	Európai Bizottság - Az EU gyermekjogi stratégiája

[1] Ez az ún. „Adatvédelmi törvény” volt Magyarországon, amelyet később a 2010. évi CXII. törvény (Infotv.) váltott fel.

Évszám	Információbiztonság és adatvédelem jogi szabályozása
2022	Az Európai Parlament és a Tanács rendeletjavaslata a gyermekek szexuális bántalmazásának megelőzésére és az ellene folytatott küzdelemre vonatkozó szabályok megállapításáról
2022-2023	Európai Uniós Kiberbiztonsági Ügynökség és az Európai Unió Adatvédelmi Biztosa együttműködése
2022	Az Európai Parlament és a Tanács rendelete a digitális szolgáltatásokról (Digitális Szolgáltatási Rendelet) – gyermekvédelmi kötelezettségek
2024	2024. évi LXXVIII. törvény az internetes agresszió visszaszorításáról
2024	2024. évi XLIX. törvény az online pornográf tartalom korlátozásáról gyermekvédelem céljából
2024	Az 1997. évi XXXI. törvény (Gyermekvédelmi törvény) 2024. évi módosításai – az online káros tartalmak bejelentésének és eltávolításának egyszerűsítése
2025	Európai Bizottság útmutatója a kiskorúak online biztonságáról a Digitális Szolgáltatási Rendelet (DSA) keretében – nem kötelező erejű ajánlás

3. sz. táblázat: Az információvédelem és adatvédelem főbb jogi szabályozásának nemzetközi és hazai mérföldkövei. (saját szerkesztés)

A táblázatban azokat az évszámokat emeltem ki, amelyek közvetlenül a gyermekek és fiatalkorúak helyzetének szabályozásához kapcsolódnak. Ugyanakkor fontos megjegyezni, hogy számos olyan információbiztonsági jogszabály is született, amely általánosságban minden felhasználóra vonatkozik, de rendelkezései a gyermekekre és fiatalkorúakra is kihatással vannak.

A gyermekek digitális térben való jelenléte különösen érzékeny adatvédelmi és információbiztonsági kérdéseket vet fel, mivel e korosztály fokozottan sérülékeny az online kockázatokkal szemben. [74] Az őket érintő információk védelme nem csupán technológiai, hanem szabályozási kihívás is, amelyre az állami és nemzetközi jogalkotás egyaránt igyekszik választ adni. E védelmi mechanizmusok megértéséhez elengedhetetlen az információbiztonságra vonatkozó jogszabályi környezet áttekintése, amely mind Magyarországon, mind az Európai Unió szintjén egyre komplexebb formát ölt. A jelenleg hatályos gyermekeket érintő jogszabályokat azonosítottam és az irodalomjegyzékben tüntetem fel. [75] [76] [77] [78] [79] [80] [81] [82] [83] [84]

„A digitális biztonsághoz való jog mindenkit megillet. A jog egyszerre segít és véd minket, akár még önmagunktól is” – mondja Baracsi Katalin internetjogász aki hangsúlyozza, hogy a tudatos internethasználat elterjesztése kulcsfontosságú, különösen a gyermekek és fiatalkorúak esetében, akik egyre korábban lépnek be az online térbe. [85]

Az általános iskolás korú gyermekek információbiztonságának védelme érdekében számos jogszabály és intézkedés létezik, amelyek célja a személyes adatok védelme, az online biztonság elősegítése és az illetéktelen hozzáférések megakadályozása. Az informatika fejlődése által generált információbiztonsági incidensekre és hatásokra folyamatosan keresik azokat a jogi szabályozási kereteket, amelyek választ adhatnak a jelen digitális kor kihívásaira.

Gyerekekre és fiatalkorúakra vonatkozó szabályozás specifikumai - WHO ajánlások

Az Egészségügyi Világszervezet (WHO – World Health Organization) és az Egyesült Nemzetek Szervezete (ENSZ – United Nations) több ajánlást fogalmazott meg a gyermekek és fiatalkorúak védelmére vonatkozóan. Ezek az ajánlások és szabályozások célja, hogy biztosítsák a gyermekek és fiatalkorúak egészséges fejlődését és védelmét a különböző kockázatokkal szemben. Ezek közül a kutatásom szempontjából kettőt emelek ki.

- Erőszak és bántalmazás elleni védelem: A WHO iránymutatásokat adott ki az egészségügyi szektor számára a gyermekbántalmazás kezelésére, hangsúlyozva a gyermekekkel foglalkozó szakemberek szerepét a bántalmazás felismerésében és az elsődleges támogatás nyújtásában. [86]
- A Gyermek jogairól szóló egyezményt 1989-ben fogadták el az ENSZ tagállamai, ezzel történelmi elköteleződést vállalva a gyermekek jogainak védelmére. Az egyezmény a világ legszélesebb körben ratifikált emberi jogi dokumentumává vált, és jelentősen hozzájárult a gyermekek életének javításához világszerte. [87] Magánélet védelme: Az ENSZ Gyermekjogi Egyezménye kimondja, hogy minden gyermeknek joga van a magánélethez. A törvénynek (jogszabályoknak) védenie kell a gyermekek magánéletét, családját, otthonát, kommunikációját és jó hírnevét minden támadástól. [88]

1.8 Digitális kultúra oktatásának vizsgálata

„Az informatikai rendszerre vonatkozó információk tartalmazzák az adott rendszer felépítésére, működésére vonatkozó adatokat és a rendszerhez csatlakozó eszközök jellemzőit. Nem létezett és nem létezik tökéletes biztonság. A fejlődéssel párhuzamosan folyamatosan jelennek meg újabb és újabb támadási módszerek, biztonsági rések, ennek következtében minden kockázatra kiterjedő védelemről sem beszélhetünk.” [89]

A Központi Statisztikai Hivatal (a továbbiakban: KSH) oldalán elérhető legfrissebb oktatási adatai szerint Magyarországon a 2023/2024-as tanévben 1 millió 462 ezer fiatal vesz részt a köznevelés, a szakképzés és a felsőoktatás valamilyen szintű képzéseiben. Közülük közel 714 ezren általános iskolában tanulnak. [90] Szintén a KSH oldalán fellelhető adatok alapján a magyar háztartások 91,4 százalékában van internet elérés [91]. Ez azt jelenti, hogy ezen korosztály internettel és azok információbiztonsági kihívásaival való találkozása gyakorlatilag elkerülhetetlen.

A kiberbűnözés gazdasági hatásai világszerte folyamatosan növekvő tendenciát mutatnak. Az Európai Unióban 2020-ban a kiberbűnözés becsült éves költsége a globális gazdaság számára 5,5 milliárd eurót tett ki [92]. Az Egyesült Államok Szövetségi Nyomozóirodája (FBI) ugyanebben az időszakban közzétett beszámolója 16,6 milliárd USD éves kárt állapított meg [93]. Ezzel párhuzamosan a Cybersecurity Ventures előrejelzése szerint a kiberbűnözés globális költsége 2024-ben elérte a 9,5 billió USD-t évente és a költségek éves szinten várhatóan 15%-os növekedést mutatnak, amely 2025-re akár 10,5 billió USD értéket is elérhet. A kalkulációk széles körű tényezőket tartalmaznak, többek között adatvesztést, termelékenység-csökkenést, szellemi tulajdon eltulajdonítását, valamint jogi és helyreállítási költségeket. Ezzel párhuzamosan a 2023-ban publikált Cybersecurity Ventures előrejelzés szerint a kiberbűnözés globális költsége 2024-ben elérhette a 9,5 billió USD-t évente és a költségek éves szinten várhatóan 15%-os növekedést mutatnak, amely 2025-re akár 10,5 billió USD értéket is elérhet. A kalkulációk széles körű tényezőket tartalmaznak, többek között adatvesztést, termelékenység-csökkenést, szellemi tulajdon eltulajdonítását, valamint jogi és helyreállítási költségeket. [94]

Látható, hogy világszinten mennyire komoly ez a probléma. Ha ebből a szempontból vizsgáljuk a fiatalkorúak információbiztonsági tudatosságának a kérdését, akkor elmondható, hogy a téma hosszútávon gazdasági és nemzetbiztonsági kérdéseket is felvet. Amennyiben, mint elöljáró korosztály nem gondoskodunk a fiatalok információbiztonsági védelméről, „elengedjük a kezüket” és hagyjuk, hogy ismeretek és védelem hiányában járják végig a maguk útját, óriási veszélynek tesszük ki őket illetve hosszútávon közvetve hatással lehet a honvédelem területére is.

Digitális kultúra tantárgy tananyagainak vizsgálata

Az informatikai eszközök folyamatos fejlődése egyre újabb lehetőségeket teremt, amelyekkel a korábbi generációk még nem szembesülhettek. Ezért a tanulók digitális

kompetenciájának fejlesztése nem korlátozódhat pusztán az informatikai ismeretek átadására, hanem a digitális kultúra tudatos és sokoldalú fejlesztését is magában kell foglalnia. Bár ez valamennyi tanulási területen megjelenik, a szükséges szakmai és módszertani keretet, valamint az egységes szemléletet elsősorban a Digitális kultúra tantárgy biztosítja – amint azt a kerettanterv magyarázatának első oldala is hangsúlyoz. [95] A Digitális kultúra tantárgy tananyagainak tudományos vizsgálatát részletesebben a National Security Review tudományos folyóiratban megjelent tanulmányomban fejtettem ki. [96] Az általános iskolás korú fiatalok számára kiadott Digitális Kultúra tankönyv megjelenésének alap adatait az alábbi táblázatban foglalom össze:

Évfolyam	Kiadás éve	Engedély időtartama
3	2021	2027. 08. 31-ig
4	2022	2027. 08. 31-ig
5	2020	2025. 08. 31-ig
6	2020	2027. 08. 31-ig
7	2022	2027. 08. 31-ig
8	2023	2027. 08. 31-ig

4. sz. táblázat – Digitális kultúra tantárgy tankönyveinek kiadása (saját szerkesztés)

Az általános iskolás korú fiatalok esetében a gyerekek első alkalommal harmadik osztályban találkoznak a Digitális kultúra tantárggyal. Megvizsgáltam, hogy egyes tananyagokban milyen hivatkozások és milyen ismereti anyagok állnak rendelkezésre az információbiztonság és adatvédelem kérdéskörében tágabb értelemben a kiberbiztonság tudatosítása kapcsán.

- A harmadikos tankönyv [97] tisztázza, hogy „sok olyan adat, információ létezik, ami személyes dolgokat árul el rólad.” Meg is nevezi ezeket: név, a születési idő, a lakcím, a diákigazolvány szám, illetve oktatási azonosító. Azaz „minden olyan adat, amely alapján tudják, ki vagy, vagyis azonosíthatnak téged.” A tankönyvben jelzik a gyerekeknek, hogy a személyes adatok mellett a fotó, a videó készítéséhez a szülők beleegyezése szükséges. Felhívja a figyelmet, hogy fizikai veszélyeken kívül más veszélyekre is figyelniük kell a gyerekeknek. A veszélyek azonban okos használattal és felnőtt segítség mellett elkerülhetőek. A tananyag kiemeli, hogy az interneten nem csak olyan információk és adatok találhatók meg, amelyek minden esetben helyesek.
- Az általános iskolás korú fiatalok esetében második alkalommal negyedik osztályban találkoznak [98] ahol az információvédelem területéről leginkább az álhírek kezelése és az arra való reakció van legbővebben kifejtve, amellyel több oldalon keresztül foglalkozik a tankönyv. Ezen kívül a korosztályhoz igazodva itt már játékos feladatokkal demonstrálják egy-egy elveszett jelszó esetén a tennivalókat, illetve a befolyásolásra vonatkozó információk kezelését.

- Az ötödik osztályban [99] a tantárgy keretében az adatvédelem és az információvédelmi megközelítés kissé visszaszorul és a korosztályos ismeretátadás más területeinek fókuszai kerülnek előtérbe pl.: robotika, programozás vagy a prezentációkészítés.
- A hatodik osztályban [100] az adatvédelem és adatbiztonság fogalmak már konkrétan megjelennek. Az adatvédelmet úgy magyarázza, hogy az adatainkat megvédjük az illetéktelenek ellen. Felhívja a figyelmüket arra, hogy adataikat a saját nevükkel és saját jelszavukkal érhetik el. Emellett elkülöníti az adatbiztonság fogalmát, ami adataik megóvása attól, hogy megsérüljenek vagy megsemmisüljenek és amelyre a mentés és biztonsági másolat készítését javasolja. Ennél a korosztálynál kerül bevezetésre az „Etikus és egészséges eszközhasználat a felhőben és a földön” címszó alatt az internet etikusságára vonatkozó ismeretanyagok ismertetése, valamint az internetfüggőség és játékfüggőség fogalmak magyarázata is.
- Hetedik osztályban [101] egy teljes fejezetet szentelnek az adatvédelem területének. A tankönyv javaslatot tesz arra, hogy a fiatalok hogyan kezeljék adataikat az internet használat közben és meghatározza mit tekintünk személyes adatnak. Külön érdekessége az ez évi tananyagnak, hogy átbeszélésre kerül az, hogy milyen szabály vonatkozik a tizennégy év alattiak és a tizennyolc év alattiak weboldalakra történő regisztrációjára. Egyébként a tantárgy esetében a fő fókusz a szövegszerkesztésre és a prezentációra esik.
- A vizsgált tananyagok legutolsó darabja a nyolcadikos [102], ami egyben a legfrissebb is. A tankönyv 2023-ban került kiadásra. Ebben egy külön fejezet a „Az e-világ és az online kommunikáció” foglalkozik az információbiztonság és az adatvédelem területével. Nyolcadik osztályban a legnagyobb tartalmi mondanivaló a táblázatszerkesztés módjaival foglalkozik, a 113 oldalas tankönyv 27 oldalán keresztül, igen részletesen. A nyolcadikosok számára szerkesztett tankönyv a vizsgált könyvek közül a legtöbb oldalból áll. A tankönyv végén találhatunk egy összefoglaló fogalomgyűjteményt is, illetve a számítógép kialakulásáról is tartalmaz egy három oldalas összefoglaló fejezetet.

A digitális kultúra tantárgy általános iskola harmadik osztályától kezdve nyolcadik osztályig része a tantervnek. A tantárgy, a metodika és a tananyag nagyon új. De a mai világunkban az „új” fogalma relatív. A digitális korban az egyre gyorsuló információkból egyre többet kell feldolgoznunk ezért a tananyag pár éven belül várhatóan frissítésre szorul majd.

1.9 Kutatás során áttekintett hazai és nemzetközi projektek és szakpolitikai kutatások

Az alábbiakban egy táblázatban összefoglalva bemutatom, mely projekteket és szakpolitikai kutatásokat vizsgáltam a szakirodalmi áttekintés keretében:

ssz.	Kutatás / projekt	Rövid leírás	
1	DIGIKID kutatás	A 8-15 éves iskolás korosztály okostelefonhasználatát és online viselkedését vizsgálta kérdőíves és szoftveres adatgyűjtéssel.	[103]
2	Magyar Fiatalok 2020 Kutatás	A 15-29 éves magyar fiatalok társadalmi helyzetét, digitalizációs szokásait és jövőképét elemezte.	[104]
3	Az EU Kids Online magyarországi kutatásáról	Európai szintű kutatás, amely a gyermekek és fiatalkorúak internethasználati és információbiztonsági szokásait vizsgálta.	[105]
4	Magyar Tinik a Neten 2021	A magyar tinédzserek internethasználati és közösségimédia-fogyasztási szokásait elemezte.	[106]
5	Magyar Tinik a Neten 2023	Újabb kutatás a magyar tinik digitális térben való jelenlétéről és információbiztonsági kihívásairól.	[107]
6	Ifjúság 2020 kutatás	A magyar fiatalok életmódját, oktatási és munkaerőpiaci helyzetét vizsgálta.	[104]
7	Kulcsocska - NAIH kutatása (2018)	A Nemzeti Adatvédelmi és Információszabadság Hatóság kutatása a gyermekek adatvédelmi tudatosságáról.	[2]
8	OFCOM - Online Nation	Az Egyesült Királyság területén az internethasználatát és digitális tudatosságot vizsgáló riportok.	[108]
10	SANGO projekt	A Nemzetközi Távközlési Egyesület (ITU) által támogatott gyermekeknek szóló kibervédelmi kiadvány és kutatás.	[109]
11	DQ Institute gyermek online biztonsági index	30 ország gyermekfelmérésére épülő kutatás a digitális intelligencia és információbiztonság területén.	[110]
12	France, portrait social – Insee Références – Édition 2022 tanulmánya	A Francia Nemzeti Statisztikai és Gazdasági Tanulmányok Intézete (Insee) tanulmánya a gyermekek képernyő elött eltöltött idejéről	[111]
13	BornSocial #2023 kutatás	Franciaországi gyermekek internethasználatát és digitális tudatosságát vizsgáló kutatás.	[112]

ssz.	Kutatás / projekt	Rövid leírás	
14	Pew Research Center „Teens and Cyberbullying” - Amerikai Egyesült Államok	Amerikai kutatás a tinédzserek és az internetes zaklatás összefüggéseiről	[113]
15	Kék Vonal Gyermekkrízis Alapítvány	Gyermekvédelmi szervezet akik névtelen, anonim és ingyenes szolgáltatásaival segíti a gyerekeket az online zaklatás és a digitális biztonság területén is.	[114]
16	Saferinternet.hu kutatásai, projektjei és szakanyagai	A gyermekek internetes veszélyekkel kapcsolatos tudatosságának vizsgálata és prevenciós programok ismertetése	[115]
17	Médiatudatosságot fejlesztő óratervek és feladatok tanórai felhasználáshoz	Bűvösvölgy - Médiaértés-oktató Központ A gyermekek és fiatalok tudatos médiafogyasztásának és internethasználatának fejlesztésére irányuló oktatási programja	[116]
18	A digitális világ veszélyei	A 9-18 éves fiatalok internethasználatával kapcsolatos önkormányzati kutatás	[117]
19	Gyermekek a neten és digitális szülőség	Internet Hotline (IH) a Nemzeti Média- és Hírközlési Hatóság (NMHH) által készített felmérés	[118]
20	Biztonsagosinternet.hu hotline beszámoló	Nemzetközi Gyermekmentő Szolgálat Magyar Egyesület beszámolója	[119]
21	Útmutató szülők és gondviselők számára	Internet Watch Foundation kiadványa a gyermekekkel szembeni visszaélésekről a biztonsagosinternet.hu publikálásában	[120]
22	Kiberbiztonság a sérülékeny csoportok számára, Írország	Munster Műszaki Egyetem, Cork projektje	[121]

5. sz. táblázat – Projektek és szakpolitikai kutatások (saját szerkesztés)

1.10 Részkövetkeztetések

Kutatásomban kevert módszertani megközelítéssel éltem, ahol egymásra épülő kvalitatív és kvantitatív módszereket alkalmaztam, amelyeket a trianguláció módszerével egészítettem ki annak érdekében, hogy az eredmények megbízhatóságát és érvényességét növeljem. A kutatás elméleti és kontextuális megalapozásának célja volt, hogy megvizsgáljam a téma elméleti hátterét. Ezt követően a második szakaszban feltártam a legfontosabb problématerületeket, míg a harmadik szakaszban szélesebb körű adatokkal támasztottam alá a vizsgálatomat és biztosítottam saját eredményeim visszamérését és

pontosítását. A trianguláció módszerének alkalmazása lehetővé tette, hogy többféle forrásból és nézőpontból vizsgáljam a kutatási kérdéseket, ezáltal csökkentve az esetleges torzításokat, valamint biztosítva, hogy az adatok kiegészítsék és megerősítsék egymást. Az eltérő megközelítések kombinálása nemcsak az eredmények hitelességét növelte, hanem segített a vizsgált jelenségek objektív értelmezésében is.

Munkám során nagy hangsúlyt fektettem a tudományos kutatás alapelveire és azokra a tényezőkre, amelyek befolyásolhatják a kutatási eredményeimet. Figyelembe vettem a történeti és jogi hátteret, valamint a digitális környezet gyors fejlődését, amely folyamatosan alakítja az általános iskolás gyermekek információbiztonsági kihívásait. A kutatási módszerek és az elemzési keretek összehangolásával célom az volt, hogy részletes képet adjak a gyermekek online biztonságát érintő problémákról, valamint azokról az igényekről, amelyek a szülők és pedagógusok oldalán megjelennek. A továbbiakban az információbiztonsággal kapcsolatos alapfogalmakat, történeti előzményeket, generációs különbségeket, valamint a jogi és oktatási kereteket mutattam be, különös tekintettel az általános iskolás korú gyermekek digitális biztonságára. A kutatási koncepcióm szerint ez az elméleti alapozás nem csupán a fogalmi tisztázást szolgálta, hanem megalapozta a későbbi empirikus vizsgálati szakaszokat is. Ebben a fejezetben tisztáztam az információbiztonság, a kiberbiztonság, az adatvédelem és a gyermekekre vonatkozó adatvédelem fogalmait, valamint ezek viszonyrendszerét. Ezen fogalmi háttér ismerete elengedhetetlennek bizonyult a kutatásom szempontjából a releváns keretek kijelöléséhez. A történeti áttekintés során bemutattam, hogyan fejlődött az információbiztonság, különös tekintettel arra, miként vált a kezdetben ipari célokat szolgáló hálózati infrastruktúra mára a mindennapok szerves részévé, amelynek kihívásai különösen a gyermekeket érintik.

Kutatásomban kiemelt szerepet kapott a generációs megközelítés. Az alfa generációba tartozó gyermekek mellett a szülői és pedagógusi szerepköröket betöltő X, Y és Z generációk információbiztonsági attitűdjeit is vizsgáltam. A fejezetben bemutatott elméleti és empirikus előzmények alapján világossá vált számomra, hogy ezek a generációk eltérő szintű tudatossággal rendelkeznek, ami közvetlenül hat a gyermekek védettségére is a digitális térben.

Itt mutattam be részletesen azokat a kiberbiztonsági fenyegetéseket, amelyek a legnagyobb veszélyt jelenthetik az általános iskolás korosztály számára. A fenyegetéseket

szakirodalmi alapokon nyugvó, kutatásom során kiegészített csoportosítás szerint rendszereztem, ezzel megalapozva a kutatási kérdéseim és hipotéziseim értelmezhetőségét.

Fontosnak tartottam a gyermekeket érintő jogi szabályozási környezet bemutatását is. Ismertettem a legfontosabb magyar és uniós jogszabályokat – különösen a GDPR-t és a 2013. évi L. törvényt –, amelyek irányt mutatnak a gyermekek adatainak kezelésére. Kutatásom eredményei alapján azonban úgy látom, hogy a jogi szabályozás önmagában nem elegendő: az érintettek – gyermekek, szülők és pedagógusok – tudatossága és gyakorlati felkészültsége elengedhetetlen a védelem érvényesítéséhez.

A digitális kultúra oktatásának vizsgálatakor áttekintettem az iskolai tananyagokat és pedagógiai módszereket, különös figyelmet fordítva arra, milyen mértékben jelenik meg az információbiztonság a köznevelés rendszerében. Bár a „Digitális kultúra" tantárgy önmagában üdvözlendő, kutatásom rámutatott arra, hogy a tartalmak aktualitása és mélysége sok esetben nem elegendő ahhoz, hogy a diákok valós élethelyzetekben is alkalmazható ismeretekhez jussanak. Kiemelten fontosnak tartom a pedagógusok módszertani támogatását, továbbképzését is, hiszen ez alapfeltétele annak, hogy a fiatal generáció tudatosan és biztonságosan tudjon mozogni a digitális térben.

A fejezet végén bemutattam azokat a hazai és nemzetközi szakpolitikai kutatásokat, valamint jó gyakorlatokat, amelyek inspirációul szolgáltak saját kérdőíves kutatásom kérdéseinek és nyelvezetének kialakításához. Ezek a példák segítettek abban, hogy kutatásom valós társadalmi és oktatási igényekre reflektáljon.

Összegzésként bizonyítottam, hogy az információbiztonság nem csupán műszaki-technikai vagy jogi kihívás, hanem összetett társadalmi és oktatási kérdés is. Úgy vélem, hogy a jogi szabályozás, a tudatosság növelése és az oktatás csak együttesen lehet képes arra, hogy valódi védelmet biztosítson a gyermekek számára a digitális térben. E komplex szemléletmód meghatározta a további kutatásaim irányát és célkitűzéseit.

2 A „DIGIÓ” KUTATÁS ÉS AZ EREDMÉNYEK VIZSGÁLATA

A következő fejezetben a „DigiÓ” kutatás teljes folyamatát mutatom be, amely magában foglalja a kvalitatív megfigyelések és interjúk eredményeit, a kvantitatív kérdőíves felmérést, valamint az ezekre épülő visszamérést. Az elemzés középpontjában a hipotézisek vizsgálata és az azokból levont részkövetkeztetések állnak, amelyek hozzájárulnak a gyermekek információbiztonságával kapcsolatos helyzetkép pontosabb megértéséhez.

2.1 A kutatás lebonyolításának folyamata

A kutatási célok és hipotézisek megfogalmazása szorosan összefügg a kvalitatív vizsgálati szakaszban kialakult kutatási fókuszcsoportokkal amelyek megalapozták a további vizsgálatok irányát. A kutatásomat, a disszertációm első fejezetében jelzett triangulatív megközelítésben a kvalitatív eredményeim felhasználásával kvantitatív kérdőíves megkérdezéssel folytattam.

A kvantitatív adatgyűjtésre épülő „DigiÓ” kutatásom célja az volt, hogy képet kapjak az általános iskolás gyermekek, szüleik és nevelő pedagógusaik információbiztonsághoz kapcsolódó ismereteiről, attitűdjeiről és viselkedési mintáiról. A kutatás lebonyolítása több egymásra épülő lépésen keresztül valósult meg, amely során törekedtem az etikai (lásd. 0 Tudományos kutatási alapelvek beépítése), adminisztratív és módszertani szempontok összehangolására.

A folyamat következő lépéseként egyetemi támogató levelet szereztem be[2], amely igazolta a kutatásom hitelességét, szakmai hátterét és tudományos célját. Ezt követően ezzel a dokumentummal kerestem meg az illetékes tankerületet, akiktől hivatalos engedélyt kértem az adatgyűjtés lefolytatására.[3] Az engedély birtokában került sor a kapcsolatfelvételre az iskolákkal, amelynek során az intézményvezetőkkel egyeztettük a részvétel feltételeit, illetve a kérdőívek technikai kiküldésének módját és időzítését.

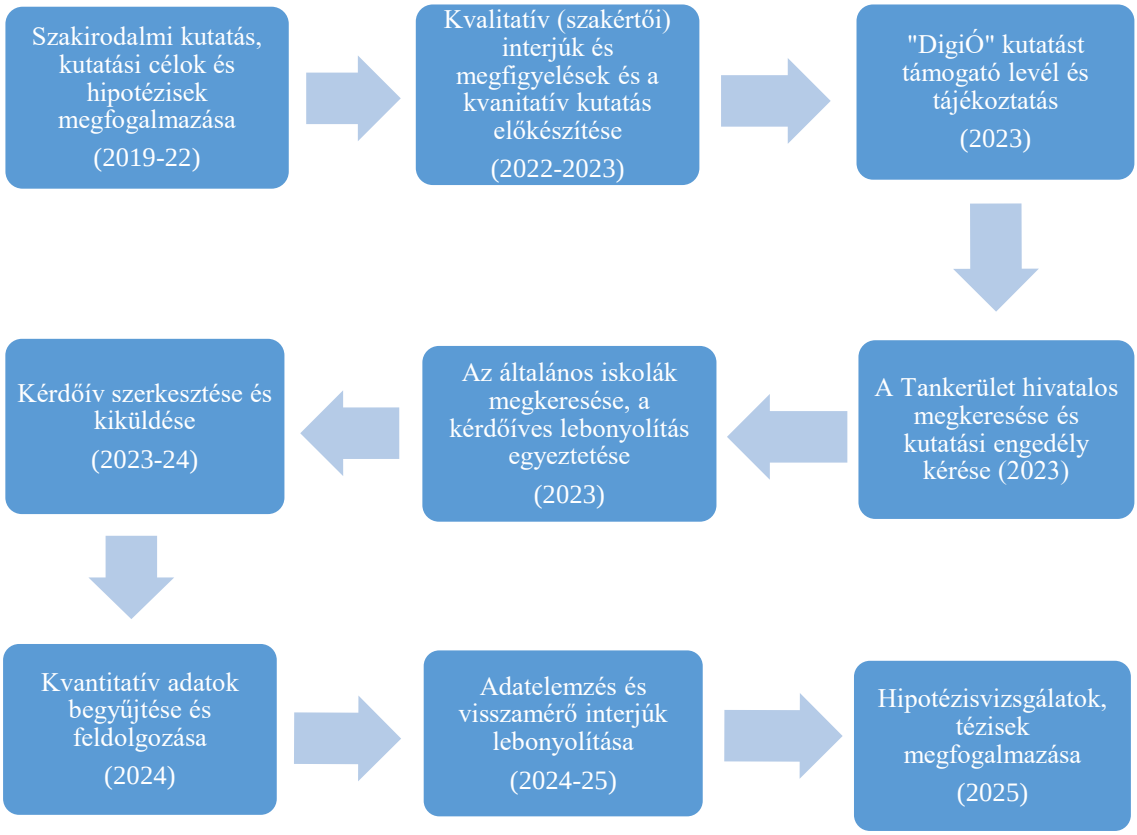
A kérdőívek online formában kerültek továbbításra az iskolák által preferált módon – jellemzően az iskolaigazgatók közreműködésével - a pedagógusok és a szülők felé. Tekintettel arra, hogy az általános iskolás korú gyermekekre szigorú kiskorúakat védő

[2] Az Óbudai Egyetem által adott támogató levél másolata a disszertációm mellékletében található
[3] A tankerület képviselője által írt kutatást visszaigazoló e-mail, a disszertációm mellékletében található.

szabályozás vonatkozik, őket közvetlenül nem volt lehetőségem megszólítani. A releváns gyermekválaszok gyűjtését úgy oldottam meg, hogy a gyermekeknek szóló kérdőív kizárólag a szülői kérdőíven keresztül volt elérhető. Ezáltal a gyermekek részvétele minden esetben a szülői beleegyezéshez kötötten, annak tudtával és engedélyével történt, megfelelve az etikai és jogi elvárásoknak.

A kérdőíveket minden célcsoport számára külön, az adott célcsoport nyelvezetére és kontextusára szabott bevezető szöveggel láttam el, kiemelve a részvétel önkéntességét, névtelenségét és a kutatás célját. A gyerekek, szülők és pedagógusok számára készített kérdőívek más-más szempontok szerint épültek fel, de mindegyikük fókuszában a kvalitatív szakaszban körülírt témakörök - úgymint az információbiztonsági tudatosság, az eszközhasználati szokások és a védelmi stratégiák és attitűdök vizsgálata - álltak.

A kérdőívek kitöltését követően az adatok begyűjtése és rendszerezése történt meg, majd az adatállomány tisztítása után sor került a kvantitatív elemzésre, amely során JASP statisztikai elemző program használatával vizsgáltam a válaszok jellemzőit, összefüggéseit és azonosítottam a legmarkánsabb mintázatokat. A kutatási folyamat ezen szakasza kulcsszerepet játszott abban, hogy a kvalitatív szakaszban feltárt fókuszpontokat nagyobb elemszámú adathalmaz alapján megerősítsem, pontosítsam, illetve kontextusba helyezzem. Ezt követően került sor az eredmények szakértői interjúk általi visszamérésére, majd a hipotézis vizsgálatokra. Ezt a fentebb szövegesen leírt kutatási folyamatot, az alábbi folyamatábrán összefoglalva is bemutatom.



1. sz. ábra – DigiÓ kutatás folyamata (saját szerkesztés)

2.2 Kvalitatív kutatás bemutatása

Kutatásom első kvalitatív szakaszában, az általam elkészített interjúk és a megfigyeléseim rávilágítanak arra, hogy az információbiztonsági kihívások összetett hatással vannak a szülőkre, pedagógusokra és a gyermekekre egyaránt. Az állami szerepvállalás kérdése, a pedagógusok digitális kompetenciáinak bizonytalanságai és az okoseszközök használatának szabályozása olyan kérdések, amelyek együttesen befolyásolják a jövő generációjának viselkedését. Az interjúk alapján összeállítottam azon kérdőívet, amelynek segítségével továbbléptem a kutatási kérdéseim megválaszolásában.

Szakértői interjúk módszertana

Jelen fejezetben bemutatom a kutatásom első kvalitatív szakaszában lebonyolított interjúk és megfigyelések [5] módszertanát és eredményét. Az interjú kérdések a disszertációm végén a függelékben találhatóak meg.

Kutatásmódszertani szempontból a félig strukturált interjú módszere mellett döntöttem. Ez lehetőséget adott nekem az interjú alanyokat ne szorítsam be egy adott kérdéskör

válasz-falai közé, hanem azon szakértői szempontok is be tudjanak épülni a kutatásomba, amire esetleg én magam nem gondoltam. Ez a módszer lehetőséget adott arra is, hogy a kutatási kérdéseim főbb témái ne maradjanak ki és egy fajta vezérvonalként vezessenek engem.

A megvalósítás során olyan tapasztalt és a területen jártas szakembereket kerestem meg akik a kutatási kérdéseimmel összefüggésben válaszokat, támpontokat és iránymutatásokat tudnak adni az általános-iskolás korú gyermekek információbiztonság kihívásaival kapcsolatban. Az elmúlt évek kutatómunkája során számos – a területen működő és szaktekintélynek tartott - szakemberrel ismerkedtem meg akik közül választottam ki az interjú alanyokat. Az interjúkat többségében személyesen kevesebb alkalommal online bonyolítottam le. Az interjúk megszervezésekor és lebonyolításakor komoly kihívást jelentett az interjú-időpontok egyeztetése az interjúalanyok elfoglaltsága miatt valamint az interjú alanyok rendelkezésre állásának időbeli korlátja. A következő táblázatban összefoglaltam, az általam megkeresett és interjúba bevont szakemberek adatait.

Név	Interjú lebonyolítása	Szervezet	Pozició	Kutatási relevancia
Dr. Baracsi Katalin	személyes	önálló szakértő	LL.M családjogi szakjogász, LL.M infokommunikációs szakjogász internetjogász, közösségi média tréner	A terület elismert és tapasztalt jogi szakértője, A SANGO projekt magyarországi koordinátora
Forgács Mariann	Online	Be Social magyarországi digitális ügynökség	Alapító, ügyvezető	Az ifjúsággal foglalkozó Magyar Tinik a Neten 2021 és Magyar Tinik a Neten 2023 kutatások menedzsere
Fülöp Hajnalka	személyes	Kütyüjogsi - Tudatos digitális szülő	Alapító, előadó, tréner	Tapasztalt iskolai és szülői tréner, előadó
Dr. Péterfalvi Attila	személyes	Nemzeti Adatvédelmi és Információszabadság Hatóság	elnök	Gyermekek információbiztonsági jogi szabályozása
Dr. Ságvári Bence	online	Indiana University, Bloomington	ifjúságkutató, data scientist	Digikid kutatás - kutatásvezetője A 8-15 éves, iskolás korosztály okostelefonhasználatát és

Név	Interjú lebonyolítása	Szervezet	Pozició	Kutatási relevancia
				online viselkedését vizsgálta
Dr. Király Borbála	személyes	Nemzetközi Gyermekmentő Szolgálat	Safer Internet Center (SIC) projektmenedzser	Gyermekek biztonságos internethasználatával foglalkozó szervezet szakértője
Dr. Pokó Diána	személyes	Gazdálkodási és Tudományos Társaságok Szövetsége Gazdasági és Külgazdasági Tagozat	társelnök Európa jogi szakjogász LL.M Mesterséges Intelligencia (AI) és Technológiai szakjogász LL.M	szakértő
Orosz Péter Pál	Online	Nemzetbiztonsági Szakszolgálat, Mesterséges Intelligencia Nemzeti Labor	NBSZ kutatásért felelős munkacsoportjának tagja, operatív szakmai vezető	szakértő

6. sz. táblázat – Kvalitatív kutatási szakasz interjúalanyok (saját szerkesztés)

Az interjúkat a keretelemzés és a tematikus elemzés kvalítatív elemzési módszereivel végeztem el. Tematikus elemzéssel az alábbi témaköröket azonosítottam:

- Gyermekek digitális kockázatai, technológia fejlődésének hatása
- Szülői attitűdök és felelősség
- Pedagógusok és oktatás
- Állami szerepvállalás
- Okostelefon használat és életkor összefüggései

Ezt követően elvégeztem a keretelemzést amelyben azt vizsgáltam, hogy az egyes kutatási kérdésekhez kapcsolódó témák milyen gyakran fordulnak elő a az interjúk során. Ez alapján az alábbi megállapításokat tettem:

- Gyermekek információbiztonsági kockázatainak kérdésköre a legdominánsabb téma, amely azt mutatta számomra, hogy a szakembereket erősen foglalkoztatja az általános iskolás korú fiatalokat érintő digitális veszélyek és a gyermekek online biztonsága.

- Szülők állami segítség iránti igénye szintén jelentős hangsúlyt kapott, ami arra utal, hogy az interjúalanyokat foglalkoztatja a szabályozás, a jogi környezet és az állami szerepvállalás kérdése.
- Pedagógusok felkészültsége és a hozzá kapcsolódó kérdéskör a harmadik leggyakoribb téma volt az interjúkban. Ez számomra azt mutatta meg, hogy a tanárok és az iskolarendszer digitális biztonsági oktatásra való felkészültségének kérdését tovább kell elemezni.
- A pedagógusok által igényelt téma feldolgozáshoz szükséges támogatások kérdésköre, a digitális kultúra oktatása, amely az előző témát egészíti ki, szintén megjelent az interjúkban.
- Az gyermekek okostelefon használata azzal összefüggésben, hogy hány éves korban kellene a gyermekek kezébe adni az okoseszközöket.

2.2.1 Megfigyelések és további kutatást kiegészítő kvalítatív módszerek alkalmazása

Módszertani megközelítésből a „résztvevői megfigyelést” végeztem az általános iskolákban, ahol közvetlenül találkoztam gyermekekkel és jómagam is kérdéseket tehetem fel nekik. Mivel a kutatási megfigyelés személyes jelenlétet igényel, minden esetben engedélyt kértem az intézmény igazgatójától az iskolába való belépésre. A Kolozsvár Utcai Általános Iskolában élő megfigyeléseket végeztem egy az osztályfőnöki óra keretében megtartott „internetbiztonsági foglalkozáson”. Az alkalmon Fülöp Hajnalka, Safer Internet oktatót kísértem el és mint kutató aktívan részt vettem a felvilágosító tevékenységben. A „nem részt vevő megfigyelés” módszerét is alkalmaztam, amikor lehetőségem volt – egyfajta külső szemlélőként - megfigyelni a Magyar Máltai Szeretetszolgálat ifjúsági képzőinek képzését amelyet Baracsi Katalin internetjogász, tréner tartott a gyerekek információbiztonsága témában. Mindegyik esetben „nyílt megfigyelés” módszerével éltem. Ez azt jelentette hogy mind a gyerekek, mind pedig a képzési csoport tagjai tudták, hogy kutatási célból vagyok jelen. A megfigyelési eredményeimet kézi jegyzeteléssel rögzítettem.

2.2.2 Részkövetkeztetések

A digitális világ rohamos fejlődésével párhuzamosan a gyermekek egyre fiatalabb korban válnak az internet aktív használóivá. Ez számos információbiztonsági kihívást vet fel, amelyeket az interjúalanyok megerősítettek. "Az online tér, az olyan mint a fizikai tér. Ugyanúgy meg kell tanítani a gyerekeket tájékozódni." Mondja Dr. Király Borbála

Nemzetközi Gyermekmentő Szolgálat Safer Internet Center projektmenedzsere. A leggyakoribb problémák közé tartoznak az online visszaélések, az internetes zaklatás és a túlzott információmegosztás veszélyei. Gyakran előfordul, hogy a fiatalok nem mérik fel megfelelően a személyes adatok közzétételének hosszú távú következményeit, ami kiszolgáltatottá teszi őket különböző online fenyegetésekkel szemben. "Az adatvédelem jogi környezetének megértése mellett az információvédelem és adatbiztonság is fontos és a gyerekeknek meg kell érteniük, miért ne osszanak meg minden adatot magukról." – ezt már Dr. Péterfalvi Attila a Nemzeti Adatvédelmi és Információszabadság Hatóság Elnöke mondja ki.

Lényegi kérdésként jelent meg az interjúkban, hogy a gyermekek milyen életkorban kapják meg az első okoseszközüket, hiszen ennek komoly hatása van az információbiztonsági szocializációjukra. Ez a kérdés megosztja a szülőket. "A gyerekeket már a leges-legelejétől fel kell készíteni az okostelefon használatára. A szülőknek ezt végig kell gondolni, hogy mikor és hogyan szeretnének eszközt adni a gyerek kezébe és hogyha már odaadják azt az eszközt, akkor igenis meg kell tanítani arra, hogyan kell használni." – mondja Baracsi Katalin internetes jogász. Az interjúk tanúsága szerint eltérő vélemények vannak arról, hogy milyen életkorban lenne ideális a gyermekek számára az okoseszközök használata. Míg egyes szülők úgy vélik, hogy minél később kapják meg a gyerekek az első telefonjukat, annál biztonságosabb lesz a fejlődésük, a valóság gyakran azt mutatja, hogy ez sokkal hamarabb megtörténik, mint ahogy azt a szülők ideálisnak tartanák. Ennek több oka lehet: a kortárs nyomás, az iskolai elvárások vagy éppen a szülői biztonsági megfontolások, amelyek miatt egyre fiatalabb korban válik a gyermek aktív digitális felhasználóvá.

A szülők és pedagógusok különböző módon reagálnak ezekre a kihívásokra és eltérő megközelítések figyelhetők meg. Egyesek szigorú tiltásokkal próbálják kontrollálni a gyermekek internetes tevékenységét, míg mások inkább az edukációra és a nyílt párbeszédre helyezik a hangsúlyt, bízva abban, hogy a gyermekek idővel megtanulják a helyes online viselkedést. Ez utóbbit erősítette meg Fülöp Hajnalka is aki szerint "A kapcsolódás fontosabb, mint a kontroll. Ne azt próbáljuk keresni, hogy hogyan tudjuk kontrollálni gyermekünk online életét, mit tudunk letölteni, blokkolni, utánanézni a gyereknek, ellenőrizni, eltiltani, hanem figyeljünk arra, amit csinál ő és legyünk vele jelen az online térben is, töltsünk vele időt."

A pedagógusok szerepe kulcsfontosságú a gyerekek információbiztonságával való foglalkozás területén. Bár az oktatási rendszerben megjelenő új digitális kultúra tantárgy lehetőséget biztosít a diákok számára, hogy megismerkedjenek a biztonságos internethasználat alapjaival, ugyanakkor sok pedagógus még mindig nem érzi magát kellően felkészültnek arra, hogy hatékonyan tudjon beszélgetni a gyerekekkel témáról. Azok a pedagógusok, akik kevésbé magabiztosak ebben a témában, nagyobb hajlandóságot mutatnak arra, hogy külső szakértőkre támaszkodjanak és szívesebben fogadnának el külső támogatást, például képzéseket vagy segédanyagokat. Az interjúk alapján világossá vált, hogy szükség van témában jártas emberi közreműködésre és további oktatási segédanyagokra valamint célzott képzésekre annak érdekében, hogy a tanárok magabiztosan tudják átadni az információbiztonságra vonatkozó ismereteket. Mindez azt jelzi, hogy a digitális kompetencia fejlesztése nem csupán a tanulók, hanem a tanárok számára is nagyon fontos.

A generációk közötti eltérések szintén meghatározó szerepet játszanak abban, hogy ki hogyan viszonyul az információbiztonsági kérdésekhez. Az X és Y generáció tagjai akik a jelen kor általános iskolás korú gyermekeinek többségét nevelik és akik felnőttként találkoztak először a digitális világgal, jellemzően óvatosabbak és inkább hajlanak a kontrolláló megoldásokra. Ilyenek például a szülői felügyeleti alkalmazások használata vagy az internet-hozzáférés korlátozása. Ezzel szemben a Z generációs szülők és Alfa generációs gyermekek már digitális bennszülöttként nőttek fel, így sokkal magabiztosabban mozognak az online térben és gyakran kevésbé érzik veszélyesnek a személyes adatok megosztását. Ők sokkal nagyobb hajlandóságot mutatnak az új technológiák gyors elfogadására is. Ezek a generációs különbségek új kihívások elé állítják a szülőket és a pedagógusokat, akiknek viszont egyensúlyt kell találniuk a digitális szabadság és a megfelelő biztonsági intézkedések között.

Többen hangsúlyozták, hogy az információbiztonsági tudatosításban az államnak jelentősebb szerepet kellene vállalnia, különösen az iskolai tananyagok kialakításában és a gyermekek internetes tudatosságának fejlesztésében. Az állami segítség iránti igények megítélését befolyásolja a családban lévő gyermekek személyes érintettsége az internetes fenyegetésekben.

A kvalitatív szakasz vizsgálatának eredményei alapján, az alábbi témacsoportok további vizsgálatát jelöltem meg:

- Az információbiztonsági eseménnyel való érintettség és az állami segítség igénye;
- A szülők digitális eszközhasználathoz való hozzáállása és a közösségi média korlátozásának szerepe;
- A gyermekek információbiztonsági védettsége és kontrollképessége az iskolai osztályok előrehaladtával;
- Az okostelefonok átadásának ideje és a generációs különbségek;
- Pedagógusok információbiztonsági felkészültsége és támogatási igényeik.

Ezen témacsoportok szolgáltak kiindulópontként a kutatásom kvantitatív szakaszához.

2.3 Kvantitatív kérdőíves kutatás és kvalitatív visszamérés

A vizsgálat irányai a kvalitatív szakasz eredményei alapján kerültek meghatározásra, melyeket a „Kvalitatív kutatás bemutatása" fejezetben részleteztem. A kvantitatív szakaszban a témacsoportok mentén megfogalmazott hipotéziseket kérdőíves adatfelvétel segítségével vizsgáltam, majd az eredményeket szakértői interjúk révén validáltam.

Általános információk a kérdőívvel kapcsolatban

A gyermekekre vonatkozó adatvédelmi előírások miatt a kérdőívek csak anoním és azonosítás mentes módon kerülhettek kitöltésre. A gyermekek maguk, csak szülői hozzájárulással tudták kitölteni a kérdőívet. Az iskolák nem voltak néven nevezve, hanem az azonosítás egyetlen jelölése az iskolák kódja volt, amelyet minden intézményvezetőnek külön küldtem meg.

Fontos megemlítenem, hogy a kérdőíves adatfelvétel a vizsgált témát jóval szélesebb körben öleli fel, mint amelyet jelen disszertáció keretei lefednek. Az értekezés fókuszát tudatosan szűkítettem annak érdekében, hogy az interjúk során azonosított főbb problématerületekre koncentrálva egy átláthatóbb, koherens elemzési irányt alakítsak ki. Ez a tematizálás lehetővé tette, hogy a kvalitatív eredmények mélyebb értelmezést nyerjenek, miközben a kérdőíves kutatás további dimenzióinak feldolgozása a jövőbeli publikációk és kutatási irányok számára nyitva marad. A választott megközelítéssel nem szűkítettem le az adatfelvétel jelentőségét, csupán egy első, tudatosan kijelölt tudományos lépést tettem annak feltárásában. [122]

Szintén fontos része a kutatásomnak, az eredmények visszacsatolása az érintett iskolák felé, támogatva a helyi intézmények tudatosabb információbiztonsági nevelési gyakorlatainak kialakítását és megerősítését.

Kitöltésre vonatkozó összesített adatok

Az alábbi táblázatban összesítem az újpesti DigiÓ kvantitatív kutatás kitöltőinek számát.

DigiÓ felmérés kitöltőinek száma	
szülők	530
általános iskolás gyerekek	276
pedagógusok	138
Összesen:	944

7. sz. táblázat - DigiÓ felmérés kitöltőinek száma (saját szerkesztés)

Tankerületi és pedagógus adatok

Kutatásom elsősorban az Észak-Budapesti Tankerületi Központ (EBTK) újpesti területén zajlott le. Személyes kutatási kapcsolatok révén további két iskolából kaptam adatokat amelyek az Észak-Pesti Tankerületi Központ területén helyezkednek el. Az alábbi táblázatban összefoglaltam a DigiÓ kutatás tankerületi személyi kapcsolatait.

Tankerület	Kapcsolat
Észak-Budapesti Tankerületi Központ	Márk Attila Olivér szakmai igazgatóhelyettes
Észak-Budapesti Tankerületi Központ	Dr. Szántó Attila osztályvezető, kamarai jogtanácsos

8. sz. táblázat – Tankerületi kapcsolatok (saját szerkesztés)

A következő táblázatban összefoglalom az általam megkeresett tankerületi iskolák 2023/24 tanévi tanulói és pedagógusi létszámát (Forrás: Észak-Budapesti Tankerületi Központ) valamint a DigiÓ kutatás kitöltőinek számosságát.

Iskola neve	Pedagógusok száma	Tanulók száma
Újpesti Karinthy Frigyes Magyar-Angol Két Tanítási Nyelvű Általános Iskola	49	613
Bajza József Általános Iskola	33	372
Csokonai Vitéz Mihály Általános Iskola és Gimnázium (csak ált.isk. rész)	39	499
Homoktövis Általános Iskola	52	627
Károlyi István Általános Iskola és Gimnázium (csak ált.isk. rész)	44	566
Lázár Ervin Általános Iskola	55	487
Megyeri Úti Általános Iskola	57	496
Szigeti József Utcai Általános Iskola	35	374
Szűcs Sándor Általános Iskola	54	593
Összesen	418	4,627
Minta	138	276
Kitöltési arány	33.0%	6.0%

9.sz. táblázat – DigiÓ kutatásban megkeresett általános iskolák és a tanulói / pedagógusi létszáma és a válaszadók száma (saját szerkesztés)

Az adatok alapján szeretném külön kiemelni, hogy az Észak-Budapesti Tankerületi Központ – újpesti területi pedagógusai körében minden harmadik megkeresett személy visszajelzett és kitöltötte a kérdőívet. Ez az arány különösen jelentős, mivel a pedagógusokra vonatkozó elemzések esetében ez a minta kellően reprezentatív alapot biztosított a kvalitatív megállapítások kvantitatív megerősítéséhez. Ezen válaszok hozzájárultak ahhoz, hogy a pedagógusok információbiztonsági felkészültségére, attitűdjeire és támogatási igényeire vonatkozó következtetéseim megalapozottabbak és hitelesebbek legyenek.

Szülői adatok

A kutatás során alkalmazott triangulatív módszertani megközelítés egyik pillérét a szülői visszajelzések képezték, mint harmadik – a gyermekek és pedagógusok mellett – releváns célcsoport.

Az alábbi táblázatban összefoglaltam a szülői kérdőíves adatfelvétel főbb szociográfiai adatait.

Változó	Kategória	N	%
nem	férfi	116	21.887
	nő	414	78.113
korcsoport	1965 és 1980 között	299	56.415
	1981 és 1995 között	223	42.075
	1996 és 2010 között	8	1.509
lakóhely	Község/Falu	11	2.075
	Város	41	7.736
	Vármegye-székhely	1	0.189
	Főváros	477	90.000
végzettség	főiskola / egyetem (felsőfokú)	311	58.679
	érettségi (középfokú)	176	33.208
	általános Iskola illetve szakma (alapfokú)	43	8.113

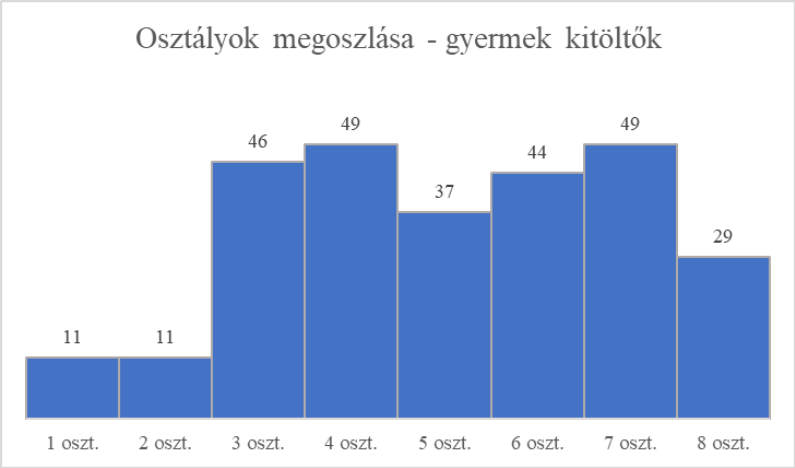
10.sz. táblázat – DigiÓ kutatásban résztvevő szülői kitöltések (saját szerkesztés)

A szülői válaszok értelmezésének egy szempontja, hogy a válaszadók melyik évfolyamos gyermekükre vonatkozóan töltötték ki a DigiÓ kérdőívet. Ez azért is fontos, mert a gyermek életkora és iskolai évfolyama jelentős hatással van a digitális eszközhasználati szokásaira, valamint az információbiztonsági kockázatokkal való találkozás gyakoriságára is. Az alábbi ábra azt mutatja be, hogy a szülők hányadik osztályos gyermekükre vonatkozóan válaszoltak a kérdőív vonatkozó kérdéseire.

2. sz. ábra - Melyik évfolyamos gyermekükre vonatkozóan töltötték ki a szülők a kérdőívet (saját szerkesztés)

Gyermek adatok

A kérdőívet kitöltő általános iskolás tanulók száma összesen 276 fő volt. Ez a válaszadói létszám biztosított mintát számomra a tanulók információbiztonsági tudatosságának, eszközhasználati szokásainak és az online térben való viselkedésmintáinak vizsgálatához a kérdőív alapján. A válaszok mennyisége és sokszínűsége lehetővé tette a kvantitatív elemzések vizsgálatát. A lenti ábra a kitöltők számát és osztályát mutatja be.



3. sz. ábra – Gyermek kitöltők osztályok szerinti megoszlása (saját szerkesztés)

A 2023/24 tanévben az általános iskolai nappali oktatásban részesülő iskoláskorú tanulók száma: 712 394 fő [123]. A kutatásom időpontjában az Észak-Budapesti Tankerületi Központ – újpesti területen tanuló gyermekek létszáma 5911 fő volt (forrás: EBTK). Ez azt jelenti, hogy a tankerületi gyermekek 4,7%-a töltötte ki a kérdőívemet.

Területi áttekintés - Újpest

Kutatásomat – személyes érintettség révén – újpesten és környékén bonyolítottam le, ezért röviden, pár mondatban kitérek a település bemutatására.

Budapest IV. kerülete, Újpest, a főváros északi részén található. A kerületben található lakónépesség száma a 2022.10.01. (népszámlálási) adatok alapján 95 075 fő, területnagysága 1882 hektár [124].

Újpest modern kori fejlődése gróf Károlyi István nevéhez fűződik, aki 1831-ben lehetővé tette, hogy a rákospalotai pusztájához tartozó István-hegyen bárki telket bérelhessen szőlőültetés céljából. Ez a kezdeményezés vezetett az Újmegyer hegyközség megalakulásához, amely Újpest magjának is tekinthető. A 19. század végére a település jelentős ipari központtá nőtte ki magát, több gyár és üzem létesült itt, különösen a Váci

út mentén. Az iparosodás és Pest közelsége hozzájárult a lakosság gyors növekedéséhez: míg 1848-ban 638 fő élt itt, addig 1910-re már több mint 55 000-en lakták a települést. 1950 január 1-jén Újpestet Budapesthez csatolták, létrehozva Nagy-Budapestet. Újpest azóta is Budapest szerves részeként fejlődik [125] [126].

DigiÓ" kutatás specifikuma

A kutatási módszereim megválasztásakor a vizsgált általános iskolába járó korosztályra vonatkozóan speciális körülményeket kellett figyelembe venni. Egyfelől a 18 éven aluli gyermekek megszólítása és kutatási folyamatba való bevonása csak szülői felügyelet mellett volt lehetséges, másfelöl komoly kihívást jelentett számomra hogy a kérdőívek nyelvezete és bonyolultsága befogadható legyen a korosztályos fiatalok számára, hiszen a kérdőív kitöltésére vonatkozó hajlandóság erősen befolyásolja a kérdőívek kitöltésének darabszámát (n). A kutatás során össze kellett egyeztetni az elvárt tudományos igényességet és azt a fajta nyelvezetet amely az általános iskolás korú gyerekek számára is értelmezhető. Áttekintve a fiatalokat érintő hazai és nemzetközi kutatások nyelvezetét és stílusát [lásd. 1.9 Kutatás során áttekintett hazai és nemzetközi projektek és szakpolitikai kutatások fejezet] úgy döntöttem, hogy kutatásomban a fiatalok számára befogadható nyelvezetet illetve kapcsolódó nyelvi megfogalmazásokat használom.

A kvantitatív kutatási eredményeim visszamérése

Módszertani szempontból a kvantitatív kérdőíves adatfelvételt követően a kutatási eredményeim értelmezését és megerősítését egy kvalitatív ellenőrző lépcsővel egészítettem ki. A kvantitatív kutatási eredményeimet kvalitatív szakértői interjúk alkalmazásával visszamértem. Ennek keretében további félig strukturált interjúkat készítettem olyan szakértőkkel, akik napi szinten foglalkoznak gyermekekkel vagy digitális neveléssel vagy információbiztonsági kérdésekkel. A szakértők között pedagógus, internetjogász, digitális oktatási szakember, valamint információbiztonsági szakértő és a Nemzeti Kibervédelmi Intézet munkatársa is szerepelt.

Az interjúk célja az volt, hogy visszamérjék és értelmezzék a kvantitatív kutatási fázisban pontosított és megállapított téziseimet. A beszélgetések során nemcsak az eredmények megerősítésére, hanem azok árnyalására, kontextusba helyezésére is törekedtem. A szakértői véleményeket minden releváns kvantitatív eredmény után, a témához kapcsolódóan illesztettem be a disszertáció szövegébe, így a kutatásom hárompilléres triangulatív (gyermek–szülő–pedagógus) szemlélete mellé negyedik dimenzióként

szakértői reflexió is társul és ez nemcsak módszertani gazdagítást jelentet, hanem növelte a kutatási megállapításaim érvényességét és megbízhatóságát is.

A szakértők kiválasztásában szempont volt, hogy legyen köztük olyan szakember, aki az első kutatási szakaszban részt vett, így ezáltal egy kutatási előzményeket ismerő és az elért eredmények feldolgozására jobban rálátó szakértői véleményezést tudok kapni, amely lehet megerősítő vagy további kérdéseket felvető irányú is. Másrészről a kutatásom ezen befejező szakaszában megkerestem olyan szakembereket is, akiket a korábbi szakaszokban nem vontam be, ugyanakkor elismert szakértői a területnek. Ez Az alkalmazott kétféle megközelítési mód nagyban segítette a kutatásom hipotéziseinek kritikai vizsgálatát és garantálta az újszerű rálátást az eredményeim elemzésére.

Az interjúkat - egy kivétellel - minden esetben online bonyolítottam le. Az online lebonyolítás során az interjú rögzítésére és jegyzetelésére az MS Teams program „transcript" funkciót használtam fel.

Az interjú során. Az interjúk során a hipotéziseim és a kvantatív kutatási eredmények megállapításainak ismertetését követően az interjúalanyok kifejtették szakértői véleményüket az öt tématerületen. A szakértőkkel együtt megvizsgáltam a megállapításaimat, hogy igazak-e vagy sem. A szakértők kiegészítéseket javasolhattak, valamint magyarázatokat adhattak a kutatási megállapításaimhoz. A téziseket ezt követően véglegesítettem.

A megszólított általános iskolás korú gyermekek információbiztonságával foglalkozó releváns szakemberek felsorolását az alábbi táblázatban foglalom össze:

Név	Szervezet	Pozíció	Kutatási relevancia
Dr. Baracsi Katalin	Internetes jogász	LL.M családjogi szakjogász, LL.M infokommunikációs szakjogász, tréner	A terület elismert és tapasztalt jogi szakértője, A SANGO projekt magyarországi koordinátora
Jerabek György	Hétpecsét Információbiztonsági Egyesület	titkár, információbiztonsági felelős	Általános iskolában és civil szervezetben is dolgozik, elismert információbiztonsági szakértő
Fülöp Hajnalka	Kütyüjogsi - Tudatos digitális szülő, Safer Internet oktató	Alapító, előadó, tréner, szülői edukátor	Tapasztalt iskolai és szülői tréner, előadó
Hirmann László	Újpesti Károlyi István Általános Iskola és Gimnázium	Iskolaigazgató, gyakorló pedagógus	DigiÓ kérdőíves kutatásban résztvevő intézmény pedagógiai szakembere
Kiss Tamás László	Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NKI)	főosztályvezető, prevenciós előadó	Nemzeti Kibervédelmi Intézet témában elismert szakembere

11. sz. Táblázat – IV. kutatási fázis, szakértői visszamérő interjúk alanyai (saját szerkesztés)

Kutatást kiegészítő tapasztalatok

A téma feldolgozását segítette, hogy könyvtárelemzés keretében vonatkozó szakirodalmi feltárást végezhettem az Óbudai Egyetem partner egyetemén az ausztriai KREMS IMC Egyetemen. Az osztrák környezetben további értékes visszajelzéseket kaptam, amelyek megerősítették a kutatási irányomat. Az ott abban az időben zajló osztrák-litván-német nemzetközi projektben való közreműködésem révén sikerült nemzetközi tapasztalatokat is szereznem. További szakirányú kutatási tapasztalatokat szereztem az írországi Münsteri Műszaki Egyetem – Kiberbiztonsági Tanszéken (MTU – Munster Technological University – Chair of Cybersecurity) ahol nemzetközi kutatási projektben vettem részt. Ezen nemzetközi kutatási tapasztalatoktról szóló igazolások a disszertációm függelékében találhatóak.

Szintén segítette a kutatási folyamatot, hogy rendszeresen részt vettem a gyermekek információbiztonságát tárgyaló konferenciákon és ott is kerestem a kapcsolatot a témával foglalkozó kutatókkal és szakemberekkel, ezáltal több specifikus tartalomhoz (pl.: szakirodalom, podcast, prezentáció, stb.) fértem hozzá.

2.3.1 Eredmények és hipotézis vizsgálatok

Első kutatási fókusz: Az információbiztonsági eseménnyel való érintettség és az állami segítség igénye

Vonatkozó hipotézis (H1): Feltételezem, hogy azon szülők esetében ahol gyermekük valamilyen információbiztonsági eseménnyel érintett volt, ott nagyobb arányban várják az államtól a segítséget illetve az állam feladatának is tekintik a felvilágosítás vagy megelőzést.

A hipotézis-vizsgálat megalapozásához első lépésben változók meghatározása történt meg.

Kockázat-kontroll változók létrehozása

A vizsgálatok elvégzéséhez kutatásomban szükséges volt a változók meghatározása, ezért első lépésként azt tekintettem át, hogy milyen jellegű (lásd. 1.5 Általános iskolás korú fiatalok kiberbiztonsági fenyegetései fejezet) és mértékű információbiztonsági kockázati kitettség érinti az általános iskolás korú gyermekeket. E kitettség értékelését két szempontból végeztem el: egyrészt a gyermekek önbevallásos válaszai, másrészt a szülők által észlelt tapasztalatok alapján. E kettős megközelítés lehetővé tette, hogy az észlelt és valós kockázatok közötti esetleges eltérések is azonosíthatók legyenek.

A gyermekek szempontjából nemcsak a kockázatok jelenlétét vizsgáltam, hanem azt is, hogy milyen mértékű kontrollt képesek gyakorolni saját online jelenlétük felett. A kutatás során ennek mérésére két összetett indikátort alakítottam ki: egy „kockázati változót” és egy „kontroll-változót”. A kockázati-változó nyolc, binárisan (igen/nem) kódolt kérdés összesítésével jött létre. Ezek a kérdések olyan információbiztonsági eseményekre vonatkoztak, amelyek a gyermekeket az online térben érhetik (pl. idegenekkel való kapcsolatfelvétel, adatokkal való visszaélés, online zaklatás stb.). A kontroll-változó hat, szintén binárisan kódolt kérdésből épült fel, amelyek azt vizsgálták, hogy a gyermekek milyen tudatos lépéseket tesznek a saját digitális biztonságuk érdekében (pl. jelszóhasználat, adatmegosztás korlátozása, ismeretlenek elkerülése, stb.). E két változó

alkalmazása lehetővé tette a kockázat és a kontroll közötti viszony kvantitatív elemzését, valamint annak vizsgálatát, hogy a magasabb kockázati kitettség összefügg-e az alacsonyabb szintű kontrollal vagy éppen fordítva. A változók összetételét a következő táblázatban foglalom össze.

Kockázati változó	Kontroll változó
Törték már fel közösségi média fiókomat.	Egy évben egyszer-kétszer lecserélem a jelszavaimat.
Törték már fel e-mail fiókomat.	Beállítottam kétlépcsős azonosítást a fiókjaimhoz.
Kattintottam már 18+ felüli tartalomra	Ellenőriztem már a biztonsági beállításaimat
Volt már úgy, hogy az interneten csúfoltak / bántottak.	Ellenőriztem már, kik láthatják a posztjaimat.
Kaptál már üzenetet olyan személytől akit személyesen nem ismersz és aki kért tőled valamit? (pl.: küldj képet magadról, adj meg kódot, email fiók belépést stb.)	Kitől hallott az online védelem lehetőségéről? - magam jártam utána
Biztonsági beállítás – nincs	Rászoktál-e keresni magadra az interneten?
Találtál-e már valami olyasmit az interneten amire nem emlékeztél hogy azt te csináltad, vagy nem tudtad hogy azt valaki megcsinálta veled?	
A profiljaim nyilvánosak, bárki láthatja őket.	

12.sz. táblázat: Kockázat és kontroll változók (saját szerkesztés)

Érintettség változók

A gyerekek szülők által is ismert érintettségét adó változót három kérdés alapján hoztam létre. Ezeket az alábbi táblázatban foglalom össze:

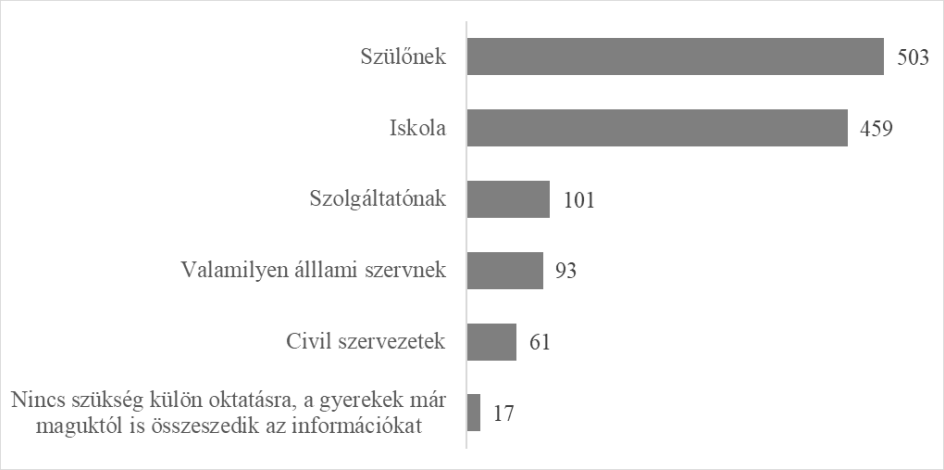
Érintettség változó
Volt-e már valaha problémája gyermekének abból, hogy valamilyen tartalmat megosztott?
Zaklatták-e már gyermekét a közösségi médián keresztül?
Került-e már gyermekéről olyan adat az internetre, amit nem szeretett volna vagy nem járult hozzá vagy nem tudott róla?

13.sz. táblázat: Érintettség változók (saját szerkesztés)

Ez alapján az „érintettséget” úgy definiáltam, hogy fenti három tényezőből legalább egy megtörtént. A kérdőíves felmérés eredményei alapján a megkérdezett szülők 14,34%-a nyilatkozott úgy, hogy gyermekét már érte valamilyen internetes atrocitás vagy

információbiztonsági incidens. A válaszok megoszlása a következőképpen alakult: a szülők 11%-a legalább egy ilyen típusú kockázatról számolt be, míg 3%-uk két különböző negatív esemény előfordulását is jelezte. Ezen túlmenően a válaszadók 0,4%-a – azaz két szülő – arról számolt be, hogy gyermekük már legalább három eltérő információbiztonsági kockázattal találkozott.

A kockázati kitettség vizsgálatát követően azt vizsgáltam, hogy a szülők mit gondolnak arról, hogy „kinek a feladata a gyermekek információbiztonsági tudatosságának fejlesztése, oktatása?” A véleményüket több válasz közül választhatták ki vagy több válasz közül jelölhették, melynek eredményét az alábbi ábra eredménye szemlélteti.



4. sz. ábra: „Kinek a feladata...” vizsgálat - szülők (saját szerkesztés)

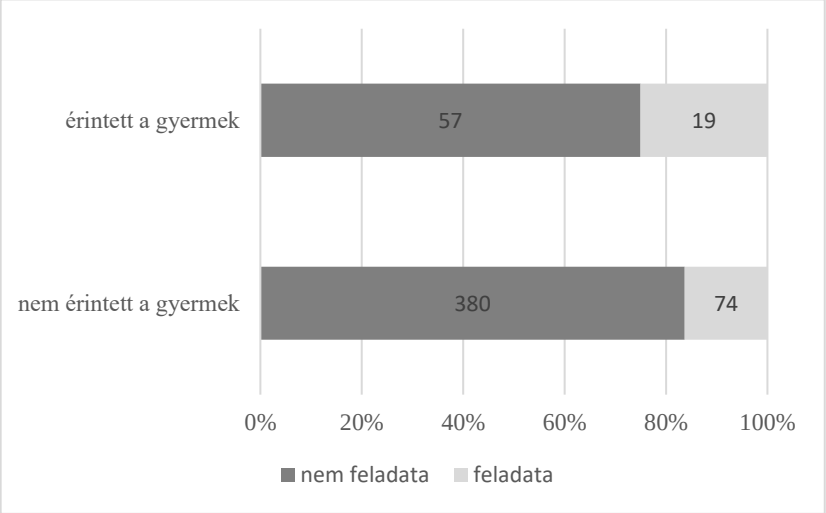
A téma jogi kereteit az állami szabályozás adja meg. Az általános iskolás korú gyermekeket körülvevő jogi keretek vizsgálata során vizsgáltam azt is, hogy a szülők szerint alkalmas-e a jogrendszerünk arra, hogy a gyermekeket megvédje. A kérdés: „Ön szerint a jogrendszerünk alkalmas arra, hogy megvédje a gyermekét az online felület használata során esetlegesen elszenvedett negatív következményektől?” Ennek eredményét a lenti táblázatban foglaltam össze.

Ön szerint a jogrendszerünk alkalmas arra, hogy megvédje a gyermekét az online felület használata során esetlegesen elszenvedett negatív következményektől?	n	%
Nem, vagy csak részben, mert le van maradva a jogrendszerünk az online kihívásokra adandó válaszokkal.	181	34.2
Sajnos, nem tudom megítélni.	126	23.8
Határozottan nem. Újra kéne definiálni a vonatkozó jogszabályokat.	111	20.9
Valószínüleg igen, de nem tudom pontosan a részleteket.	89	16.8
Határozottan igen. Van szabályozás, csak ismerni és használni kell!	23	4.3
Összesen:	530	100.0

14.sz. táblázat: „Jogrendszerünk alkalmas...” vizsgálat (saját szerkesztés)

Tekintve, hogy a jogszabályok alkotása állami feladat, ezért megvizsgáltam, hogy azon szülők esetében akik a „kinek a feladata a gyermekek információbiztonsági tudatosságának fejlesztése, oktatása?” kérdésre válaszként a „valamilyen állami szervnek” választ jelölték meg, van-e érintettség (lásd. Érintettség vizsgálat - szülők)?

Ezt a 5. sz. ábra mutatja be.



5. sz. ábra „Kinek a feladata...” és a „valamilyen állami szervnek” vizsgálat válaszadó szülői érintettség tükrében. (100% halmozott diagram) (saját szerkesztés)

Az eredmények elemzéséhez a khi-négyzet próbát (Chi-squared test) alkalmaztam [127, pp. 55-56], amely egy nemparaméteres számítási módszer. Lényege, hogy azt vizsgálja vajon két vagy több kategóriaváltozó között fennáll-e statisztikailag szignifikáns kapcsolat. [128, pp. 66-82] A próbát azért választottam, mert a vizsgálatban szereplő változók (például: gyermek érintettsége információbiztonsági eseményben, illetve az állam feladatának megítélése) nominális skálán mérhetők és így nem felelnek meg a paraméteres eljárások előfeltételeinek.

A khi-négyzet próba értéke az alábbi képlettel számítható:

$$\chi^2 = \sum \frac{(O_{ij} - E_{ij})^2}{E_{ij}}$$

Ahol O_{ij} az adott cellában megfigyelt gyakoriság, E_{ij} pedig a várt gyakoriság, amelyet a marginális eloszlások alapján számítunk. A próba szignifikanciáját a szabadságfok és a *p*-érték alapján értékeljük.

Az elemzés során a khi-négyzet érték ($\chi^2(1) = 3{,}41$; $p = 0{,}065$) azt mutatta, hogy 5%-os szignifikanciaszinten nem áll fenn összefüggés a szülők által ismert érintettség és az állami szervek feladatainak megítélése között. Ugyanakkor 10%-os szignifikanciaszinten az összefüggés szignifikánsnak bizonyult. Ez arra utal, hogy azon szülők, akiknek gyermekei érintettek voltak információbiztonsági eseményben, nagyobb arányban várják el az állami szervektől a segítségnyújtást, illetve az állam feladatának tekintik a felvilágosítást és a megelőzést.

Szakértői vélemények a (H1) hipotézissel kapcsolatos megállapításokkal kapcsolatban

A szakértők egyértelműen megerősítették, hogy a gyermek érintettsége növeli az állami szerepvállalás iránti igényt és mindannyian egyetértettek abban, hogy az államnak nagyobb hangsúlyt kell fektetnie erre a területre, azaz a gyermekek védelmére az online térben. Ugyanakkor az interjúkban kiegészítő véleményként megjelent, hogy az állami beavatkozást önmagában nem tartják elegendőnek. Fontos, hogy e mellett a szülői és pedagógusi felelősség kérdésköre is. Baracsi Katalin az igényeket így fogalmazta meg: „Nem elég az állami fellépés, ha a gyerekek maguk nincsenek tisztában azzal, hogy hogyan védhetik meg magukat. A digitális tudatosságot ugyanúgy tanítani kell, mint a matematikát.”

Mindegyik interjúalanyom egyetértett az alábbiakban:

- az államnak szerepet kell vállalnia a gyerekek információbiztonsági nevelésében és védelmében;
- Az állami intézkedések és oktatási programok kulcsfontosságúak, mivel a szülők és pedagógusok nem mindig rendelkeznek megfelelő tudással és eszközökkel
- A gyermek érintettsége növeli a szülői igényt. Kiemelték, hogy ha egy gyermek már áldozattá vált egy online fenyegetés vagy zaklatás következtében, a szülők hajlamosabbak sürgetni az állami beavatkozást és támogatást.
- Több interjúalany hangsúlyozta, hogy nemcsak a beavatkozás, hanem a megelőzés is fontos. Ehhez szükség van iskolai oktatásra, tudatosító kampányokra és szülői tájékoztatásra.

A szakértők pozitívan értékelték a meglévő állami és civil programokat, de ezek még nem elég hatékonyak vagy nem jutnak el minden érintetthez megfelelő mélységben. Ezt hangsúlyozta a Kiss Tamás László a Nemzetbiztonsági Szakszolgálat, Nemzeti

Kibervédelmi Intézet (továbbiakban: NKI) főosztályvezetője is, aki szerint: „A gyermekek online védelmében nem egyetlen szereplőre hárul a felelősség; a megelőzés és beavatkozás hatékonysága több, egymással együttműködő intézmény és szereplő (állami szervek, iskolák, civil kezdeményezések, szakmai programok és szülők) összehangolt tevékenységén múlik.”

Második kutatási fókusz: A szülők digitális eszközhasználathoz való hozzáállása és a közösségi média korlátozásának szerepe

Vonatkozó hipotézis (H2): Feltételezem, hogy a szülők digitális eszközhasználathoz való hozzáállása hatással van arra, hogy a gyermekek milyen mértékben válnak érintetté digitális események által. Különösen jelentősek azok a szülői magatartásformák, mint a gyermekkel való információbiztonsági kommunikáció, az első saját okostelefon átadásának életkora, a közösségi médiához való hozzáférés engedélyezése, az e-mailek kontrollálása, valamint a gyermek saját digitális eszközeinek száma.

A következőkben azt vizsgáltam, hogy a gyermekeket ért zaklatás összefüggésben áll-e a szülők hozzáállásával. A gyermek érintettségét befolyásolja, a szülő hozzáállása a digitális eszközhasználathoz. Ezt egy logisztikus regresszió alkalmazásával vizsgáltam, ahol a

Függő változó:

- az érintettség (0 = nem érintett, 1 = legalább 1 esemény által érintett)

Magyarázó változók:

- beszél-e a gyerekével információbiztonságról,
- hány évesen adott telefont a gyerek kezébe,
- kiengedi-e gyermekét a közösségi médiába,
- kontrollálja-e gyermekének e-mail fiókját,
- hány digitális eszköze van a gyereknek.

Megjegyzés: Ennél az elemzésnél kiszűrtem azokat a szülőket, akik még nem adtak telefont a gyerekek kezébe. Ez azért történt mert az ő esetükben nem tudtam definiálni a „mikor adott telefont a gyermekek kezébe?” változót.

A logisztikus regresszió alkalmazása a kutatásban

A logisztikus regresszió olyan statisztikai eljárás, amelyet dichotóm (bináris) kimeneti változók előrejelzésére alkalmaznak. [129, pp. 110-112] Elsődleges célja annak vizsgálata, hogy a független változók milyen irányban és milyen mértékben befolyásolják egy adott esemény bekövetkezésének valószínűségét. A lineáris regresszióval szemben a logisztikus regresszió nem egy folytonos kimeneti értéket becsül, hanem annak valószínűségét modellezi, hogy az adott jelenség bekövetkezik (pl. online zaklatás áldozatává válik = 1), illetve nem következik be (nem válik áldozattá = 0).

A módszer matematikai alapja a logit-transzformáció, amely a valószínűségi értékeket [0;1] intervallumról a valós számok tartományára vetíti:

$$\text{logit}(p) = \ln\left(\frac{p}{1-p}\right) = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \cdots + \beta_k X_k$$

ahol p az esemény bekövetkezésének valószínűsége a β_i a regressziós együtthatók X_i a magyarázó változók értékei. Az együtthatók exponenciálásával kapott odds ratio (OR) az értelmezés szempontjából kiemelt mutató:

OR > 1 esetén az adott változó növeli a vizsgált esemény bekövetkezésének esélyét,

OR < 1 esetén csökkenti azt,

OR = 1 esetén nincs hatása.

A statisztikai szignifikancia (p-érték) megmutatja, hogy az adott kapcsolat mennyiben tekinthető megbízhatóan kimutathatónak.

Az elemzést követően az alábbi megállapításokat tettem:

- A okostelefon-használat megkezdésének időpontja és az online zaklatás kockázata között pozitív összefüggés mutatható ki. Minél később kezdi meg egy gyermek a saját okostelefon használatát, annál nagyobb valószínűséggel válik online zaklatás áldozatává. A logisztikus regressziós elemzés alapján a mobilhasználat későbbi megkezdése szignifikáns pozitív kapcsolatot mutat a zaklatás bekövetkezésének esélyével (B = 0,143; OR = 1,153; p = 0,022). Ez azt jelenti, hogy a saját okostelefonhoz való hozzáférés egy évvel történő késleltetése 15,3%-kal növeli annak az esélyét, hogy a gyermek online zaklatás áldozatává válik.

- A szülők rendszeres – napi vagy heti szintű – információbiztonsági kommunikációja a gyermekkel paradox módon a zaklatásról való beszámolás magasabb arányával korrelál. Azoknál a gyermekeknél, akik esetében a szülők rendszeresen – naponta vagy hetente – beszélgetnek az információbiztonságról, szignifikánsan nagyobb az esélye annak, hogy online zaklatás áldozataivá válnak, mint azoknál, ahol ez a kommunikáció csak alkalmanként történik. A logisztikus regressziós modell szerint a rendszeres biztonságról való szülői kommunikáció növeli a zaklatás bekövetkezésének esélyét (B = 0,606; OR = 1,834; p = 0,032). Az odds ratio értelmében ez 83,4%-kal magasabb kockázatot jelent a rendszeresen tájékoztatott gyermekek körében. Ez arra utal, hogy az ilyen típusú kommunikáció növeli a gyermek tudatosságát, de paradox módon a veszélyek előfordulása is gyakoribb lehet ezekben az esetekben. A tudatos, tájékozott gyermekek nagyobb eséllyel ismerik fel és azonosítják a zaklatás különböző formáit és így valószínűbb, hogy beszámolnak ezekről a tapasztalatokról.
- A közösségi média használatának szülői tiltása védőfaktorként működik. Azok a szülők, akik nem engedélyezik gyermekük számára a közösségi médiában való részvételt, szignifikánsan csökkentik az online zaklatás bekövetkezésének esélyét. A logisztikus regressziós modell szerint a közösségimédia-használat tiltása negatív irányú összefüggést mutat a zaklatás kockázatával (B = –0,683; OR = 0,505; p = 0,014). Ez azt jelenti, hogy a közösségi médiából való tudatos távolmaradás 49,5%-kal kisebb esélyt jelent arra, hogy a gyermek zaklatás áldozatává váljon. Ez az összefüggés arra utal, hogy a közösségi média használatának szülői korlátozása hatékony védőfaktorként működhet az online zaklatással szemben, különösen az általános iskolás korosztály esetében, akik még nem rendelkeznek kellő kockázatfelismerő és elhárító készségekkel.
- Egyéb vizsgált tényezők – így a saját e-mail fiók megléte és az egyidejűleg használt digitális eszközök száma – nem mutattak statisztikailag szignifikáns kapcsolatot az online zaklatás kockázatával. A vizsgálat során elemzett tényezők – az, hogy a gyermek rendelkezik-e saját e-mail fiókkal (B = –0,023; p = 0,944), valamint az általa használt digitális eszközök száma (B = 0,078; p = 0,460) – nem mutattak statisztikailag szignifikáns kapcsolatot az online zaklatás bekövetkezésének esélyével. Ez azt jelzi, hogy ezek a változók nem befolyásolják érdemben a zaklatás esélyét.

Szakértői vélemények a (H2) hipotézissel kapcsolatos megállapításokkal kapcsolatban

A szakértők egyetértettek abban, hogy a szülői kommunikáció minősége számít, nem pedig a puszta mennyisége. A közösségi média korlátozása valóban hatásos lépésnek tartották. Azt mindenki kiemelte, hogy az oktatás, a példamutatás és a megfelelő kommunikáció fontosabb tényezők annál, mint az hogy a szülő hányszor beszél erről.

Mindegyik interjúalanyom egyetértett az alábbiakban:

- A kommunikáció önmagában nem elég. Az hogy hogyan történik ez meg, legalább ennyire fontos, hiszen ha rosszul csinálják, akár nagyobb kockázatot is jelenthet.
- A közösségi média használatának korlátozása valóban csökkenti az online zaklatás esélyét, de ezzel együtt más tényezőket is figyelembe kell venni (pl. hogyan reagál a gyermek, ha mégis veszélybe kerül).
- A gyermek életkorának megfelelő tájékoztatás szükséges. Ha túl korán vagy túl erőszakosan beszélünk neki veszélyekről, az kontraproduktív lehet.

A megállapításokkal kapcsolatban Jerabek György az alábbiakat jegyezte meg: „Ha egy csomó olyan információval kínálom meg a gyereket, amire még nem érett vagy egyszerűen nincs szüksége, azzal felkelthetem az érdeklődését olyan dolgok iránt, amelyekkel egyébként nem is találkozna.” Egy nagyon érdekes és érthető párhuzamot vont a szexuális felvilágosítással. Szerinte ez a hasonló jelenség figyelhető meg, mint amikor egy gyereket életkorának nem megfelelő mélységben tájékoztatnak érzékeny témákról. Baracsi Katalin szerint „A gyerekeknek nem félelemre van szükségük, hanem útmutatásra. Ha úgy érzik, hogy a szülő túlságosan tilt és kontrollál, akkor nem hozzá fognak fordulni, ha baj van, hanem máshol keresnek megoldást – sokszor rossz helyen.”

Harmadik kutatási fókusz: A gyermekek információbiztonsági védettsége és kontrollképessége az iskolai osztályok előrehaladtával

Vonatkozó hipotézis (H3): Feltételezem, hogy az általános iskolás korú gyermekek információbiztonsági kockázatokkal szembeni védettsége és kontroll-képessége összefügg az iskolai osztályukkal.

Kockázat

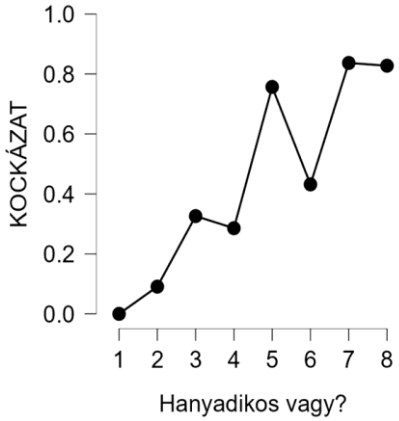
A következő elemzés célja annak feltárása volt, hogy van-e összefüggés a tanulók életkora – pontosabban az iskolai évfolyamuk – és az általuk észlelt információbiztonsági kockázatok mértéke között. A vizsgálathoz a Spearman-féle rangkorrelációs eljárást alkalmaztam, amely lehetővé tette nem paraméteres adatok közötti összefüggések vizsgálatát.

A Spearman-féle rangkorreláció (ρ, „rho") egy nemparaméteres statisztikai mutató, amely két ordinális vagy folytonos változó közötti kapcsolat erősségét és irányát méri. [130] A módszer előnye, hogy nem feltételezi a változók normális eloszlását, így különösen alkalmas olyan adatok elemzésére, amelyek sorrendi skálán mérhetők, vagy amelyek nem felelnek meg a paraméteres eljárások előfeltételeinek. A Spearman-korreláció képlete a következő:

$$\rho = 1 - \frac{6 \sum d_i^2}{n(n^2 - 1)},$$

ahol d_i az egyes megfigyelések rangkülönbsége, n pedig a megfigyelések száma. Az érték -1 és +1 között mozog: a +1 tökéletes pozitív, a -1 tökéletes negatív kapcsolatot jelez, míg a 0 kapcsolat hiányát mutatja.

Az elemzés során a tanulók évfolyama (mint ordinális változó) és a korábban kialakított „kockázati változó" közötti kapcsolatot vizsgáltam. Az eredmények alapján megállapítható, hogy létezik statisztikailag szignifikáns összefüggés a gyermekek évfolyama és a tapasztalt információbiztonsági kockázatok között, ami arra utal, hogy a magasabb évfolyamba járó tanulók nagyobb valószínűséggel találkoznak kockázatos digitális helyzetekkel. A kapcsolódó eredmények és értékek az alábbi Spearman-féle korrelációs ábrán láthatók, amely a kockázati és kontrollváltozók függvényében ábrázolja az összefüggéseket.



6. sz. ábra: Kockázat (átlag) és a kor összefüggése (saját szerkesztés)

A korrelációs elemzés mellett fontosnak tartottam annak feltárását is, hogy az egyes évfolyamok között kimutathatók-e szignifikáns eltérések a kockázati értékek tekintetében. Ezért a Spearman-féle rangkorrelációt követően a Kruskal–Wallis-próbát is alkalmaztam, amely lehetőséget adott a különböző évfolyamok közvetlen összehasonlítására. A Kruskal–Wallis-próba [131] egy nemparaméteres statisztikai eljárás, amely három vagy több független csoport középértékeinek összehasonlítására szolgál. A Kruskal–Wallis statisztika képlete a következő:

$$H = \frac{12}{N(N+1)} \sum_{i=1}^{k} \frac{R_i^2}{n_i} - 3(N+1),$$

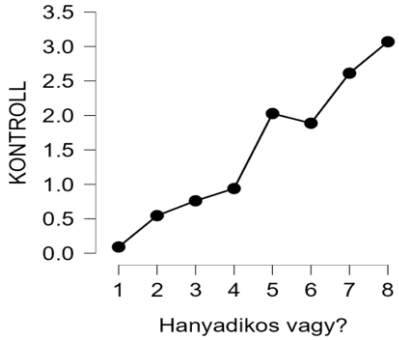
ahol N a teljes minta elemszáma, k a csoportok száma, n_i az i-edik csoport elemszáma, míg R_i az adott csoporthoz tartozó rangösszeg.

A Kruskal–Wallis-próba eredménye alapján megállapítható, hogy az információbiztonsági kockázati értékek szignifikáns különbséget mutatnak az egyes iskolai évfolyamok között ($H(7) = 34{,}94$; $p < 0{,}001$). Ez azt jelzi, hogy a kockázati kitettség mértéke nem egyenletesen oszlik meg a különböző évfolyamok tanulói között. Az ábra jól szemlélteti, hogy az idősebb korcsoportokhoz tartozó gyermekek esetében magasabb kockázati értékek jelennek meg.

Megállapítottam, hogy a tanulók életkorának növekedése fokozza az információbiztonsági kockázatokkal való találkozás esélyét.

Kontroll

A kontrollváltozó elemzése alapján megállapítottam, hogy az iskolai évfolyam emelkedésével párhuzamosan a tanulók egyre tudatosabban képesek szabályozni saját online tevékenységüket. A lenti ábra szemlélteti, hogy az idősebb korcsoportok esetében a kontroll mértéke szignifikánsan magasabb, ami arra utal, hogy a gyermekek életkorának előrehaladtával nemcsak a kockázatokkal való találkozás gyakoribb, hanem ezzel együtt fejlődik a kockázatkezelési képességük is.



7.sz. ábra: Kontroll (átlaga) és a kor vizsgálata (saját szerkesztés)

A Kruskal–Wallis-próba alapján megállapítható, hogy az információbiztonsági kockázati értékek szignifikánsan eltérnek az egyes iskolai évfolyamok mentén ($H(7) = 77{,}82$; $p < 0{,}001$). Az eredmények azt mutatják, hogy az idősebb tanulók magasabb kockázati kitettséggel rendelkeznek, ami összhangban áll azzal, hogy az életkor előrehaladtával egyre szélesebb körű és intenzívebb digitális eszközhasználat jellemzi őket. Ugyanakkor az alábbi ábra szemlélteti, hogy az életkor növekedésével párhuzamosan a kontroll-változó értéke is emelkedik.

- Megállapítottam, hogy, az idősebb korcsoportokba tartozó gyermekek nemcsak több kockázattal találkoznak, hanem egyúttal fejlettebb kontrollal (önvédelmi stratégiákkal) is rendelkeznek, így tudatosabban képesek szabályozni saját online jelenlétüket.

Szakértői vélemények a (H3) hipotézissel kapcsolatos megállapításokkal kapcsolatban

Az interjúalanyok egyetértett abban, hogy a magasabb évfolyamokban tanuló gyerekek nagyobb digitális kockázatokkal szembesülnek. Azonban eltértek a véleményük abban,

hogy mennyire képesek a gyerekek ezeket a kockázatokat kezelni. Úgy vélték, hogy a kontrollképesség az életkor előrehaladtával valóban javul, de hangsúlyozták, hogy ennek minőségét befolyásolja a megfelelő oktatás és szülői támogatás mértéke.

Mindegyik interjúalanyom egyetértett az alábbiakban:

- A digitális kockázatok valóban növekednek az iskolai évfolyamok előrehaladtával. „A kamaszok hajlamosak azt hinni, hogy mindent tudnak az internetről, de sokkal könnyebben esnek áldozatul manipulációnak vagy online zaklatásnak, mint a kisebbek.” – mondja Fülöp Hajnalka.
- A kontrollképesség fejlődése nem automatikus. Egyikük sem gondolta, hogy önmagában az életkorral együtt jár a nagyobb védekezési képesség. „Nem törvényszerű, hogy a nagyobb gyerekek jobban kontrollálják a digitális kockázatokat – ha senki nem tanítja meg nekik, akkor csak nagyobb veszélynek lesznek kitéve, de nem tudnak hatékonyabban védekezni.” Ezt már Jerabek György fűzte hozzá.
- Az oktatás és a családi háttér döntő szerepet játszik. A gyerekek digitális tudatossága nemcsak az életkorukon múlik, hanem azon is, hogy milyen információkat kapnak az iskolában és otthon. Baracsi Katalin szerint: „Azt feltételezni, hogy a nagyobb gyerekek automatikusan jobban kezelik az online veszélyeket, olyan, mintha azt mondanánk, hogy egy 17 éves jobban vezet, mint egy 30 éves, csak mert több időt tölt autóban.”
- Kiss Tamás László az NKI szakértője érdekes jelenségre hívta fel a figyelmet: „…a tapasztalatok azt mutatják, hogy már a 8–9. évfolyamban is megjelennek olyan esetek, amikor a fiatalok nemcsak érintettként, hanem elkövetőként is szerepet kaphatnak.”

Negyedik kutatási fókusz: Az okostelefonok átadásának ideje és a generációs különbségek

Vonatkozó hipotézis (H4): Feltételezem, hogy a szülők által ideálisnak tartott életkor, amikor a gyermekek okostelefont kapnak, eltér attól az életkortól, amikor valójában megkapják azt és ez a különbség a szülők generációja szerint változik.

A következő elemzési szakaszban azt vizsgáltam, hogy a szülők miként viszonyulnak gyermekük első okostelefonhoz vagy más okoseszközhöz való hozzáférésének időpontjához. A vizsgálat célja az volt, hogy feltárjam az ideálisnak tartott életkor és a

tényleges gyakorlat között fennálló különbségeket. Ehhez az ismételt méréses ANOVA (Repeated Measures ANOVA) statisztikai eljárást alkalmaztam, mivel ugyanazon szülők két, eltérő típusú válaszát – az ideális és a valós életkort – hasonlítottam össze.

Az ANOVA (varianciaelemzés / ANalysis Of VAriance) egy olyan statisztikai eljárás, amely több csoport átlagainak összehasonlítására szolgál. [128] Lényege, hogy megvizsgálja, vajon a csoportok közötti különbségek nagyobbak-e annál, mint ami a véletlen ingadozásból adódna. Az ismételt méréses ANOVA különösen akkor alkalmazható, ha ugyanazon vizsgálati személy több feltételhez kapcsolódó választ ad és ezek átlagai közötti eltérést kívánjuk kimutatni.

Az ANOVA alapképlete a varianciák hányadosán alapul:

$$F = \frac{MS_{\text{csoportok közötti}}}{MS_{\text{csoporton belüli}}}$$

ahol

$MS_{csoportok\ közötti}$ = a csoportok átlagai közötti átlagos négyzetösszeg

$MS_{csoporton\ belüli}$ = a csoportokon belüli átlagos négyzetösszeg

A kapott *F*-értékhez tartozó szignifikancia szint alapján dönthető el, hogy a csoportok közötti eltérések statisztikailag igazolhatóak-e.

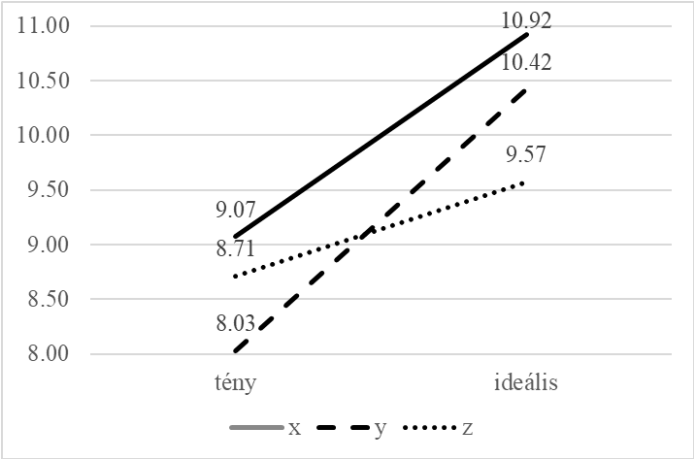
A vizsgálatban csoportképző ismérvként a szülők generációs hovatartozását (X, Y, Z generáció) vettem még figyelembe. Ennek célja, hogy feltárjam van-e eltérés a különböző generációk elvárásai és tényleges gyakorlatuk között. Az eredményeket az alábbi táblázatban foglaltam össze, szemléltetve a generációs különbségeket az eszközhasználat bevezetésének életkori megítélésében.

Köztényezős hatások - ANOVA (varianciaanalízis) kimeneti táblázata						
Eset	Négyzetösszeg	df (Szabadságfok)	Átlagos négyzet	F	p	ω^2
SZ_Mikor született?	136.411	2	68.206	7.027	< .001	0.009
Residuals	4445.699	458	9.707			

Leíró statisztikák						
RM Factor 1 (Ismételt mérés faktor)	SZ_Mikor született?	N	Mean átlag	SD szórás	SE sztenderd hiba	Variációs együttható
tény	x	264	9.072	2.072	0.128	0.228
	y	190	8.026	2.531	0.184	0.315
	z	7	8.714	2.870	1.085	0.329
ideális	x	264	10.924	2.739	0.169	0.251
	y	190	10.421	2.923	0.212	0.280
	z	7	9.571	1.902	0.719	0.199

15. sz. táblázat: Ismételt méréses ANOVA vizsgálat (saját szerkesztés)

Az elemzés során csak azokat a családokat vettem figyelembe, ahol a szülői válaszok alapján a gyermek már rendelkezett saját okostelefonnal. Azokban az esetekben, ahol a gyermek még nem kapott ilyen eszközt, az összevetés az ideális és a tényleges életkor között nem volt elvégezhető. Ezek az adatok az elemzésből kizárásra kerültek. Az ismételt méréses ANOVA vizsgálat eredményei alapján megállapítható, hogy a szülők által megjelölt valós és ideális életkor között statisztikailag szignifikáns különbség mutatható ki ($F(1, 458) = 25{,}29$; $p < 0{,}001$). Ez arra utal, hogy a szülők utólag jellemzően későbbi életkort tartanak ideálisnak gyermekük első okostelefonhoz való hozzáférése szempontjából, mint ahogy azt a valóságban ténylegesen lehetővé tették. Emellett a generációs hovatartozás is szignifikáns csoporthatással bírt az értékelésekre ($F(2, 458) = 3{,}157$; $p = 0{,}043$), vagyis az X, Y és Z generációs szülők eltérő mértékben korrigálták visszamenőleg az „ideális” életkorra vonatkozó válaszaikat a tényleges döntésükhöz képest. Ez a generációk közötti gondolkodásbeli különbségeket tükrözi az okoseszköz-használat bevezetésének megítélésében. A következő ábra vizuálisan is bemutatja, hogy a különböző generációhoz tartozó szülők mikor adták gyermekük kezébe az első mobiltelefont és ehhez képest milyen életkort tartanának ideálisnak.



8.sz. ábra: „Mikor adnék okostelefont a gyermekem kezébe?” vizsgálat (szülők)
Forrás: saját szerkesztés.

Az ismételt méréses ANOVA elemzést követően post hoc teszteket alkalmaztam annak vizsgálatára, hogy a válaszadó szülők generációs hovatartozása hogyan befolyásolja egyrészt azt, hogy ténylegesen mikor adták gyermekük kezébe az első okostelefont, másrészt azt, hogy milyen életkort tartanának ideálisnak erre a lépésre. A post hoc tesztek segítségével lehetővé vált az egyes generációk közötti összehasonlítás, amely alapján az alábbi megállapításokat tettem:

- Az X generációs szülő szignifikánsan (t=4,811, p<0,001) később (M=9,072, SD=2,072) adott telefont a gyereke kezébe, mint az Y generációs szülő (M=8,026, SD=2,531).
- Az X generációs szülő szignifikánsan (t=-11,558, p<0,001) később adnák már oda az okostelelefont ideálisan (M=10,924, SD=2,739), mint ahogy a valóságban (M=9,072, SD=2,072) tették.
- Az Y generációs szülő szignifikánsan (t=-12,677, p<0,001) később adnák már oda az okostelelefont ideálisan (M=10,421, SD=2,923), mint ahogy tették (M=8,026, SD=2,531).
- Az X generációs szülő (M=10,924, SD=2,739) és az Y generációs szülő (M=10,421, SD=2,923) nem alkotnak szignifikánsan eltérő véleményt abban a tekintetben, hogy mi az ideális kor a gyermek számára az első okostelefon odaadására (t=1,884, p=0,495)
- A Z generációs szülők esetében a valós (M = 8,714, SD=2,739) és az ideális (M = 9,571, SD=1,902) időpont között az okoseszköz odaadására nincs szignifikáns különbség (t=-0,871, p=1,000).

Összefoglalva bizonyítottam, hogy az Y generációs szülők szignifikánsan korábban adták gyermekeik kezébe az első okostelefont, mint az X generációhoz tartozó szülők. Mind az X, mind az Y generációs válaszadók a kérdőíves válaszok alapján utólagos korrekciót hajtottak végre saját döntésük megítélésében: a valóságban választottnál későbbi életkort tartottak volna ideálisnak az eszközhasználat bevezetésére. Ez a fajta tudatos újraértékelés azonban a Z generációs szülők esetében nem volt kimutatható. Az ideális életkor megítélésében ugyanakkor már nem mutatkozott szignifikáns különbség az X és Y generációs szülők között.

Szakértői vélemények a (H4) hipotézissel kapcsolatos megállapításokkal kapcsolatban

Az interjúalanyok egyetértett abban, hogy a szülők általában később tervezik odaadni a telefont, mint ahogy azt a valóságban megteszik. Abban is közös volt a véleményük, hogy az Y generációs szülők hamarabb adnak telefont a gyereküknek, mint az X generációsok és ennek egyik fő oka az életmódbeli változás és a digitális technológiák erőteljesebb beágyazódása a mindennapokba.

Mindegyik kutatási interjúalanyom egyetértett az alábbiakban:

- A szülők által kívánatosnak tartott életkor valóban későbbi, mint amikor ténylegesen odaadnák a telefont vagyis sokan utólag megbánják a döntésüket.
- Az Y generációs szülők valóban korábban adják oda a telefont, mint az X generációs szülők és ennek fő oka a technológiai fejlődés és a társadalmi normák változása.
- Fontos, hogy milyen szabályokkal és tudatossággal történik meg az okostelefon átadásának ideje.

A gyermekek által érzékelt közösségi nyomásról beszél Jerabek György „Ha egy osztályban mindenki telefonon kommunikál, de egy gyerek nem kap készüléket, az kirekesztettség érzéséhez vezethet. A szülők gyakran ezért adják oda korábban a mobilt.”

Baracsi Katalin egy másik generációs apektusra hívta fel a figyelmet: „A mai szülők egy része maga is tinédzserként kapta meg az első mobilját, így nem tudja, milyen hatással van egy 6-8 éves gyerekre a folyamatos online jelenlét.”

A kutatásom megállapítását erősítette meg Hirmann László igazgató, aki szerint: "Úgy gondolom, hogy az alsó tagozatot lehetőség szerint okostelefon nélkül kellene megúszni,

mivel a felső tagozatra való belépés lehet az ideális időpont az eszköz használatának megkezdésére. Tapasztalataim szerint az alsó tagozatban hihetetlen nyomás nehezedik a gyerekekre, mert amikor a tanítók és a szülők erről beszélnek a szülői értekezleteken, a szülők azt mondják, hogy a gyerekek mesélik, hogy már mindenkinek van okostelefonja, csak nekik nincs. Ez pszichés nyomást gyakorol a szülőkre, amit a gyerekek könyörgéssel és érzelmi hatásokkal érnek el. Szerintem a legkorábbi időpont, amikor okostelefont kellene adni a gyerekeknek, az az ötödik osztály." Kiss Tamás László az NKI szakértője a covid világjárvány időszakát is megemlíti: „A koronavírus-járvány jelentős hatást gyakorolt a gyermekek digitális eszközhasználatára. A lezárások és a távoktatás miatt sok család kényszerült arra, hogy már egészen fiatal korban – akár 6 évesen – biztosítson laptopot gyermekének, noha normál körülmények között az oktatás ezt nem indokolta volna. Ez a helyzet felgyorsította a digitális eszközökhöz való hozzáférést és megváltoztatta a tanulási környezetet is."

Ötödik kutatási fókusz: Pedagógusok információbiztonsági felkészültsége és támogatási igényeik

Vonatkozó hipotézis (H5): Feltételezem, hogy azok a pedagógusok, akik kevésbé érzik magukat felkészültnek az információbiztonsági oktatásra, nagyobb mértékben igénylik a jogi segítségnyújtást és az állandó, belső támogatást nyújtó szakemberek jelenlétét, mint a magabiztosabb pedagógusok.

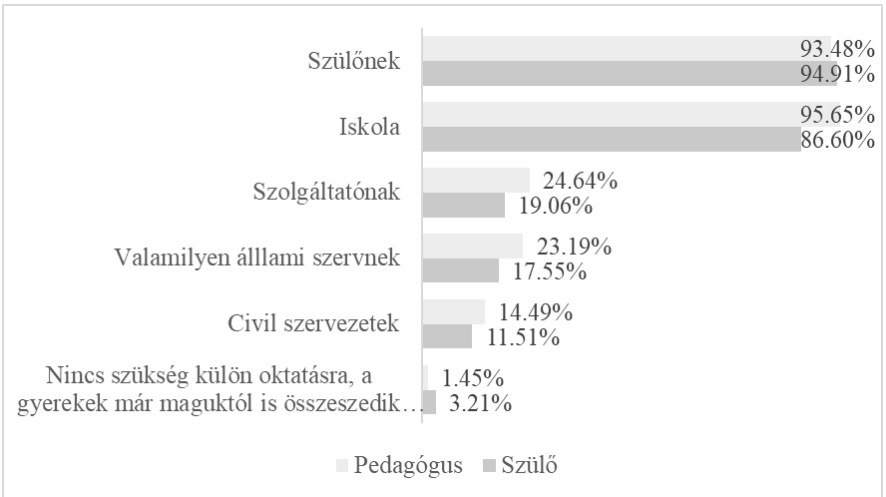
A téma vizsgálata nem lehet teljes a gyermekekkel napi szinten foglalkozó pedagógusok véleményének figyelembevétele nélkül, ezért a kutatás hárompilléres megközelítésébe a pedagógusok nézőpontját is bevontam. Ennek célja az volt, hogy feltárjam, miként érzékelik és értelmezik az oktatási intézmények szereplői a jelenlegi gyakorlati kereteket. Ezt egy több lépcsős folyamat keretében vizsgáltam. A indulásnál az információbiztonsággal kapcsolatos tudás megszerzésének forrásaira fókuszáltam. Elemzésem azt vizsgálta, hogy a gyermekek egyáltalán hozzájutnak-e az eszközeik biztonságos használatával kapcsolatos ismeretekhez és ha igen, akkor milyen forrásból – szülőktől, iskolai oktatásból, kortársaktól vagy az internetről – szerzik meg ezeket az információkat.

Kitől tanultál legtöbbet az eszközeid védelméről? (több válasz is lehetséges)		
	n	%
egyéb	5	1.81%
nem hallottam még	8	2.90%
külön internetes felvilágosító foglalkozás	21	7.61%
magam jártam utána	45	16.30%
testvér	55	19.93%
barát/osztálytárs	63	22.83%
iskolai óra keretében / tanár	157	56.88%
szülő	252	91.30%

16.sz. táblázat: „Kitől tanultál...” vizsgálat - gyerekek(saját szerkesztés)

A következő elemzési szakaszban a szülői és pedagógusi válaszokat összevontan vizsgáltam annak érdekében, hogy képet kapjak arról, hogyan ítélik meg a digitális tudatosság fejlesztéséhez kapcsolódó felelősségi köröket. A vizsgált kérdés így hangzott: „Kinek a feladata a gyermekek digitális tudatosságának fejlesztése, oktatása?”

A következő ábra szemlélteti a válaszadók megoszlását, rávilágítva arra, hogy a két csoport milyen arányban tartja ezt elsősorban a család, az iskola, az állam vagy egyéb szereplők feladatának.



17. sz. táblázat - Kinek a feladata a gyermekek digitális tudatosságának fejlesztése, oktatása táblázat (saját szerkesztés)

Az ábra eredményei alapján jól látható, hogy a válaszadók többsége a digitális tudatosság fejlesztésének felelősségét elsősorban a szülőkre és az iskolára ruházza. A pedagógusok válaszaiból kiderül, hogy komoly felelősséget éreznek a gyermekek információbiztonsági felkészítésében: a szülők szerepének megjelölése mellett közel azonos arányban saját

magukat – illetve az iskolát – is felelősnek tartják. A szülők esetében szintén az önreflexív felelősségérzet dominál, hiszen döntő többségük elsősorban saját magukat jelölte meg elsődleges szereplőként, míg második helyen kiemelkedően az iskolát nevezték meg. Ez a párhuzamos mintázat azt mutatja, hogy a két legfontosabb szocializációs közeg – a család és az iskola – kölcsönösen elismeri saját és egymás szerepét is a gyermekek digitális kompetenciáinak fejlesztésében.

A vizsgálat harmadik lépcsőjeként a pedagógusok szemszögéből elemeztem, mennyire érzik magukat felkészültnek arra, hogy az információbiztonság témáját megosszák és feldolgozzák a tanulókkal. Emellett feltérképeztem azt is, hogy milyen típusú támogatásra lenne szükségük annak érdekében, hogy ezt a nevelési feladatot hatékonyabban el tudják látni. Az elemzés célja annak feltárása volt, hogy a pedagógusok mit érzékelnek hiányosságnak – legyen az módszertani, tartalmi vagy intézményi jellegű – az információbiztonság iskolai megjelenítésében.

A pedagógusok válaszait a következő táblázatban foglaltam össze.

Értékek	igen	nem	Végösszeg	Felkészültnek érzi magát%	Nem tartja felkészültnek magát%
Tankönyv (n=44)	29	15	44	65.9%	34.1%
Kiadványok, brossurák (n=43)	28	15	43	65.1%	34.9%
Rendszeres előadások az iskolában (n=84	53	31	84	63.1%	36.9%
Pedagógus továbbképzések (n=61)	37	24	61	60.7%	39.3%
"Külsős" szakértő (n=81)	47	34	81	58.0%	42.0%
Internet jogász (n=28)	14	14	28	50.0%	50.0%
Jártas kolléga jelenléte (n=43)	20	23	43	46.5%	53.5%

18. sz. táblázat: „Felkészülnek tartja-e magát...” – pedagógus (saját szerkesztés)

Ez a vizsgálat tükrözi azon adatokat, amelyek szerint az "Információbiztonságban járatos ifjúsággal foglalkozó 'külsős' szakértő bevonása" és a "jogász meghívása" alacsonyabb preferenciát kapott összességében, de az adott célcsoportban - tehát azon pedagógusok között akik nem tartják magukat felkészültnek - jelentős igény mutatkozhat.

Szakértői vélemények a (H5) hipotézissel kapcsolatos megállapításokkal kapcsolatban

Az interjúalanyok egyetértettek abban, hogy a pedagógusok információbiztonsági felkészültsége jelentős eltéréseket mutat és ez meghatározza, hogy milyen típusú támogatásra van igényük. Az interjúk alapján a kevésbé felkészült pedagógusok hajlamosabbak külső segítségre és jogi támogatásra támaszkodni, míg a magabiztosabb tanárok inkább önállóan szeretnének fejlődni tanfolyamok és szakmai anyagok

segítségével. Ugyanakkor feltették a kérdést, hogy a magabiztosabb pedagógusok valóban megfelelő tudással rendelkeznek-e? A magabiztosság ugyanis nem mindig jelent valódi hozzáértést is.

Mindegyik interjúalanyom egyetértett az alábbiakban:

- A pedagógusok információbiztonsági tudása nagyon eltérő és sokan nem érzik magukat felkészültnek.
- A kevésbé felkészült pedagógusok hajlamosabbak külső segítséget (jogi támogatást, szakértői jelenlétet) igényelni, míg a magabiztosabbak inkább önálló tanulásra támaszkodnak.
- A jogi segítségnyújtás fontos lenne az iskolák számára, mert sok esetben a pedagógusok nem tudják, milyen felelősségük van egy digitális incidens során.
- A tanári továbbképzések szükségesek, de önmagukban nem elégségesek – állandó szakértői támogatásra is szükség lenne az iskolákban.

A magabiztosság nem mindig jár együtt valódi tudással – egyes tanárok túlértékelik a digitális kompetenciájukat, ami veszélyeket rejt magában. Jerabek György egy élő példát hozott elő saját praxisából: „Ha egy pedagógus még a saját iskolai fiókjához sem állít be többfaktoros hitelesítést, hogyan várjuk el tőle, hogy hatékonyan tanítsa az információbiztonságot?” Hirmann László iskolaigazgató szerint egy generációs kérdés húzódhat a válaszok mögött. „Ezt olvasva nekem az volt az érzésem, hogy az 1. csoportba jellemzően az idősebb pedagógusok tartozhatnak, akik szinte minden tekintetben az "old school" módszertanokat és viszonyulásokat képviselik. Az idősebb kollégák megszokták, hogy jogkövető magatartást tanúsítanak és egyértelmű jogszabályokra támaszkodnak. Kiss Tamás László az NKI szakértője is megerősítette: „A gyorsan változó digitális környezetben a pedagógusok olyan kihívásokkal is szembesülhetnek, amelyek meghaladják saját ismereteiket, ezért nélkülözhetetlen a külső szakemberek bevonása és a folyamatos támogatás biztosítása. A tudatosítás folyamatában az őszinteség és a reális elvárások megfogalmazása legalább olyan fontos, mint a módszertani eszközök bővítése.”

2.3.2 Részkövetkeztetések

Ebben a fejezetben bemutattam a „DigiÓ” kutatásom kvantitatív adatfelvétel módszertani hátterét, a kutatás lebonyolításának folyamatát, valamint a szülői, pedagógusi és gyermek válaszadók körét. A kérdőíves adatfelvétel célja az volt, hogy feltárjam az általános

iskolás korú gyermekek információbiztonsági kockázatait, valamint a szülők és pedagógusok szerepét, felkészültségét és hozzáállását e kockázatok kezelésében.

Az adatok elemzése során kiemelt figyelmet fordítottam a gyermekek online jelenlétének intenzitására, a zaklatás előfordulására, valamint az információbiztonsági tudatosság és a kontrollképesség szintjére. Vizsgáltam továbbá a szülői nevelési mintákat, kommunikációs gyakorlatokat, a közösségi médiához való hozzáférés szabályozását és azt, hogy mindezek milyen hatással lehetnek a gyermekek biztonságára. [132]

Az elemzések rávilágítottak arra, hogy a gyermek érintettsége fokozza az arra való igényt, hogy az állam is aktív szerepet vállaljon abban, hogy a fiatalokat az információbiztonsági kihívásokkal szemben megvédje és felkészítse. Megállapítható volt, hogy azok a szülők, akik rendszeresen (naponta vagy hetente) beszélgetnek gyermekükkel az információbiztonságról, nagyobb arányban számoltak be információbiztonsági incidensekről, mint azok, akik csak alkalmanként tárgyalják ezt a témát. Ezzel szemben a közösségi média használatának szülői korlátozása csökkenti az online zaklatás esélyét.

A tanulók életkora szintén meghatározó tényezőnek bizonyult: minél magasabb általános iskolai évfolyamba jár egy gyermek, annál nagyobb információbiztonsági kockázatoknak van kitéve, ugyanakkor annál nagyobb mértékű kontrollt képes gyakorolni ezen kockázatok felett. A generációs szülői mintázatok alapján elmondható, hogy az Y generációs szülők szignifikánsan korábban adják gyermekeik kezébe az okostelefont, mint az X generáció tagjai. Érdekesség, hogy míg az X és Y generációs szülők utólag inkább későbbi életkort tartanának ideálisnak, addig ez a reflexív korrekció a Z generációs szülőknél nem figyelhető meg. Ugyanakkor az ideális életkor tekintetében az X és Y generációs válaszadók között már nem mutatható ki szignifikáns különbség.

A pedagógusok válaszai alapján az is láthatóvá vált, hogy az információbiztonsági felkészüléshez kapcsolódó igények nagymértékben eltérnek attól függően, mennyire érzik magukat felkészültnek a témában. Azok, akik kevésbé magabiztosak, inkább jogi háttértámogatásra és állandóan elérhető szakértő jelenlétére tartanának igényt. Ezzel szemben azok a pedagógusok, akik magasabb szintű felkészültségről számoltak be, inkább tanfolyamokat, kiadványokat és más önállóan használható oktatási eszközöket részesítenének előnyben.

A kvantitatív elemzéseket követően a DigiÓ kutatás eredményeit tovább pontosítottam szakértői visszamérés segítségével. Mindez hozzájárult gyakorlati következtetéseim levonásához és a téziseim megerősítéséhez.

ÖSSZEGZETT KÖVETKEZTETÉSEK

A ma általános iskolás korú korosztály megközelítőleg 10-15 év múlva lép a munkaerő piacra. Akkor, amikor legnépesebb ma élő 40-50 éves munkaképes korosztály a 60-as éveiket tapossák majd. A jövőnk szorosan összefügg ezen korosztály szocializációjával. Felelősséggel tartozunk feléjük, hogy aztán amikor eljön az idő ők is felelősséggel tartozzanak irántunk. A felelősségünk része, hogy a digitális technológia által generált kihívásokra megfelelő válaszokat tudjunk közvetíteni feléjük. Kutatásom célja az volt, hogy képet alkossak az általános iskolás korú gyermekek információbiztonsági kihívásairól és feltárjam azokat a tényezőket, amelyek befolyásolják az általános iskolás korú gyermekek biztonságos digitális jelenlétét. Ennek érdekében megvizsgáltam az információbiztonság mint fogalom kérdéskörét, történeti fejlődését. Összeállítottam és rendszerbe foglalva bemutattam, hogy milyen típusú információbiztonsági kockázatokkal találkoznak a gyermekek a digitális térben, valamint hogy ezekre a kihívásokra hogyan reagálnak a közvetlen környezetükben lévő felnőttek – különösen a szülők és pedagógusok – tudatosságuk és felkészültségüktől függően. A kutatásom másik „hozott" fókuszterülete a generációs attitűdök áttekintő feltérképezése. Célom volt az X, Y, Z és Alfa generációk információbiztonsági jellemzőinek megvizsgálása, különös tekintettel a viselkedési minták, eszközhasználati szokások és attitűdök közötti különbségekre. További célként tűztem ki a releváns jogi és szabályozási környezet vizsgálatát, amely keretet biztosít a gyermekek online védelméhez. Ennek keretében vizsgáltam a szülők és pedagógusok véleményét is arról, mennyire tartják megfelelőnek a jelenlegi szabályozási környezetet az információbiztonsági kihívások kezelésére. Végül a kutatás céljaim közé tartozott a pedagógusok információbiztonsági tudatosságának és felkészültségének vizsgálata, valamint az iskolai környezetben elérhető tananyagok és oktatási környezet vizsgálata is. Az általam lebonyolított kutatási folyamat összegzését az alábbiakban foglalom össze:

1. A kvalitatív interjú fázis eredményei alapján világosan kirajzolódott számomra, hogy a gyermekek digitális térben való jelenléte egyre fiatalabb életkorban kezdődik. Ezzel párhuzamosan bizonyítottam, hogy a biztonságos

internethasználathoz szükséges információbiztonsági készségek és ismeretek sok esetben hiányosak. A megkérdezett szakértők egyetértettek abban, hogy az „1.5 Általános iskolás korú fiatalok kiberbiztonsági fenyegetései” fejezetben azonosított a digitális kockázatok komoly veszélyt jelentenek a fiatalok számára és erre a szülőknek és a pedagógusoknak fel kell készülniük.

2. A kvantitatív szakaszban lefolytatott „DigiÓ” kérdőíves kutatás alátámasztotta a kvalitatív felismeréseimet. A válaszok elemzése alapján bizonyítottam, hogy a gyermekek jelentős része nem rendelkezik megfelelő információbiztonsági tudással és sok esetben nincsenek tisztában az online viselkedés következményeivel vagy az információbiztonsággal összefüggő jogaikkal. A szülők bár fontos szerepet játszanak a digitális nevelésben, gyakran bizonytalanok a teendőiket illetően. A pedagógusok többsége pedig saját bevallása szerint nem rendelkezik elegendő módszertani és tartalmi eszközzel ahhoz, hogy magabiztosan foglalkozzon az információbiztonság kérdéskörével.
3. Végül a szakértői validálás megerősítette, hogy a téziseim relevánsak és a gyakorlatban is érvényes megállapításokat tükröznek. A visszajelzések rámutattak arra, hogy az információbiztonsági tudatosságának fejlesztésének az állam segítő funkcióiban, a családi otthonokban és az iskolai nevelés területén is van létjogosultsága.

A tudományos eredményeimet nemzetközi szinten publikáltam a Interdisciplinary Description of Complex Systems: INDECS folyóiratban [122]a „Smart Sustainable and Safe Cities Conference” konferencia keretében valamint a Munster Műszaki Egyetem Kiberbiztonsági tanszékén publikáltam.

Új tudományos eredmények

Értekezésemben öt hipotézist vizsgáltam különböző szempontok és módszerek alkalmazásával. Az újpesti „DigiÓ” kutatás eredményeire támaszkodva, valamint az általános iskolás korú fiatalok információbiztonsági kihívásainak feltárását követően az alábbi téziseket (T1–T5) fogalmaztam meg:

T1: Bizonyítottam, hogy a gyermek érintettsége fokozza az arra való igényt, hogy az állam is vállaljon szerepet abban, hogy a gyerekeket az információbiztonsági kihívásokkal szemben segítsen megvédeni és azokra felkészíteni.

T2: A kutatási eredményeimben kimutattam, hogy azokban a családokban, ahol a szülők rendszeresen beszélgetnek gyermekeikkel az online biztonságról, a gyermekek nagyobb arányban számolnak be információbiztonsági incidensekről, mint azokban a családokban, ahol ez a kommunikáció csak alkalmanként történik. Bizonyítottam továbbá, hogy a közösségimédia-használat szülői korlátozása szignifikánsan csökkenti az online zaklatás esélyét valamint, hogy a tudatosság és a kontroll együttes jelenléte a hatékony eszközök a gyermekek védelmében.

T3: Bizonyítottam, hogy a gyermekek életkorának és iskolai évfolyamának emelkedésével párhuzamosan nő az információbiztonsági kockázatokkal való találkozás esélye.

T4: Igazoltam, hogy a szülői generációk között különbségek vannak a telefon kézbeadásának kérdésében. Az Y generációs szülők statisztikailag szignifikánsan korábban adnak okostelefont gyermekeik kezébe, mint az X generációs szülők. Az „ideális életkor” megítélésében az X és Y generációs szülők között nem mutatkozik szignifikáns különbség.

T5: Bizonyítottam, hogy az információbiztonsági felkészüléshez kapcsolódó pedagógusi igények különböznek a pedagógusok saját felkészültségük megítélésétől.

A következő táblázat áttekinthető módon szemlélteti, hogyan vezetett a kutatási célkitűzéseim mentén haladó elemzési folyamat a tudományos tézisek megfogalmazásához, bemutatva a kutatási célok / kérdések, hipotézisek és tézisek közötti logikai összefüggéseket és a teljes kutatási rendszer belső koherenciáját. A táblázat strukturálja és értelmezi a kutatás menetét és a mögötte húzódó gondolkodási ívet.

Kutatási célkitűzés (C)		Hipotézis (H)		Tézis (T)	
C1	Megvizsgálni, hogy befolyásolja-e a gyermek érintettsége a szülők állami segítség iránti igényét az információbiztonsági kihívásokkal kapcsolatban?	H1	Feltételezem, hogy azon szülők esetében, ahol gyermekük valamilyen információbiztonsági eseménnyel érintett volt ott nagyobb arányban várják az államtól a segítséget, illetve az állam feladatának is tekintik a felvilágosítás vagy megelőzést.	T1	Bizonyítottam, hogy a gyermek érintettsége fokozza az arra való igényt, hogy az állam is vállaljon szerepet abban, hogy a gyerekeket az információbiztonsági kihívásokkal szemben segítsen megvédeni és azokra felkészíteni.
C2	Megvizsgálni, hogy befolyásolja-e a szülők rendszeres biztonságról való kommunikációja a gyermekek információbiztonsági tudatosságát és védelmét illeteve van-e valamilyen hatással a szülők általi közösségi média használat korlátozás valamint az első saját digitális mobiltelefon átadásának időpontja, a gyermekek digitális események általi érintettségében?	H2	Feltételezem, hogy a szülők digitális eszközhasználathoz való hozzáállása hatással van arra, hogy a gyermekek milyen mértékben válnak érintetté digitális események által.	T2	A kutatási eredményeimben kimutattam, hogy azokban a családokban, ahol a szülők rendszeresen beszélgetnek gyermekeikkel az online biztonságról, a gyermekek nagyobb arányban számolnak be információbiztonsági incidensekről, mint azokban a családokban, ahol ez a kommunikáció csak alkalmanként történik. Megállapítottam hogy a közösségimédia-használat szülői korlátozása szignifikánsan csökkenti az online zaklatás esélyét valamint, hogy a tudatosság és a kontroll együttes jelenléte a hatékony eszközök a gyermekek védelmében.
C3	Megvizsgálni, hogy milyen összefüggés van a gyermekek iskolai osztálya és az információbiztonsági kockázatok mértéke között és hogyan változik a gyermekek kontrollképessége az információbiztonsági kockázatokkal szemben az iskolai osztályok előrehaladtával?	H3	Feltételezem, hogy az általános iskolás korú gyermekek információbiztonsági kockázatokkal szembeni védettsége és kontroll-képessége összefügg az iskolai osztályukkal.	T3	Bizonyítottam, hogy a gyermekek életkorának és iskolai évfolyamának emelkedésével párhuzamosan nő az információbiztonsági kockázatokkal való találkozás esélye.
C4	Megvizsgálni hogy mit gondolnak a különböző generációjú szülők arról, hogy mikor van az ideális életkor arra, hogy a gyermekek okostelefont kapjanak és hogyan viszonyul ez a valóságban történt időponthoz képest?	H4	Feltételezem, hogy a szülők által ideálisnak tartott életkor, amikor a gyermekek mobiltelefont kapnak, eltér attól az életkortól, amikor valójában megkapják azt és ez a különbség a szülők generációja szerint változik.	T4	Igazoltam, hogy a szülői generációk között különbségek vannak a telefon kézbeadásának kérdésében. Az Y generációs szülők statisztikailag szignifikánsan korábban adnak okostelefont gyermekeik kezébe, mint az X generációs szülők. Az „ideális életkor" megítélésében az X és Y generációs szülők között nem mutatkozik szignifikáns különbség.
C5	Megvizsgálni a pedagógusok felkészültnek tartják-e magukat az internetbiztonságról való tudásátadásra és befolyásolja-e a pedagógusok saját információbiztonsági felkészültségének megítélése a felkészüléshez és oktatáshoz szükséges támogatási igényeiket? Milyen támogatási formákat tartanak szükségesnek azok a pedagógusok, akik úgy érzik, hogy nem elég felkészültek az internetbiztonsági oktatásra?	H5	Feltételezem, hogy azok a pedagógusok, akik kevésbé érzik magukat felkészültnek az internetbiztonsági oktatásra, nagyobb mértékben igénylik a jogi segítségnyújtást és az állandó, belső támogatást nyújtó szakemberek jelenlétét, mint a magabiztosabb pedagógusok.	T5	Bizonyítottam, hogy az internetbiztonsági felkészüléshez kapcsolódó pedagógusi igények különböznek a pedagógusok saját felkészültségük megítélésétől.

19. sz. táblázat – Kutatási céloktól a tézisekig összefoglaló táblázat (saját szerkesztés)

Ajánlások

A kutatásom során feltárt összefüggések és hiányterületek alapján az alábbi jövőbeli kutatási irányokat tartom relevánsnak és tudományosan megalapozottnak:

- Longitudinális vizsgálatok lefolytatása annak feltárására, hogyan fejlődik a gyermekek információbiztonsági tudatossága az iskolai évek során.
- A mesterséges intelligencia által generált kockázatok vizsgálata gyermekek körében (pl. deepfake, algoritmusvezérelt tartalmak, AI-chatbotok).
- Digitális önvédelem oktathatóságának vizsgálata különféle pedagógiai módszerek alkalmazásával (pl. játékosítás, projektalapú tanulás, drámapedagógia).
- A digitális tudatosság és a mentális jóllét közötti kapcsolat feltárása – különösen a szorongás, a kontrollérzet és a társas kapcsolatok mentén.
- Szülők és pedagógusok mélyinterjús vizsgálata a digitális neveléssel kapcsolatos dilemmákról, attitűdökről és gyakorlatokról.
- A digitális kultúra tantárgy hatásvizsgálata az információbiztonsági tudás fejlődésére – tantárgyi tartalmak és gyakorlati alkalmazás összevetése.
- Jogi tudatosság és szabályozási ismeretek feltérképezése gyermekek és szülők körében, különös tekintettel az adatvédelemre és a jogérvényesítés lehetőségeire.
- Digitális szülőség generációs összehasonlítása, azaz az X, Y és Z generációs szülők eltérő nevelési stratégiáinak és technológiai attitűdjeinek vizsgálata.

A szerző témában megjelent publikációi

Kiss, Sándor; Záhonyi, Lajos

Examination ofthe history of information security -the beginnings

National Security Review : Periodical Of The Military National Security Service 5: 2 pp. 86-99., 14 p. (2019) [23]

Záhonyi, Lajos; Szűcs, Endre

Examining information security educational tool systems, in the light of juvenile cyber security risks

National Security Review : Periodical Of The Military National Security Service: 2 pp. 134-144., 11 p. (2023) [96]

Záhonyi, Lajos; Szűcs, Endre

Examining the relationships and legal regulation of information security and data protection, with particular regard to the communication habits of young people

National Security Review : Periodical Of The Military National Security Service: 1 pp. 180-194., 15 p. (2023) [73]

Endre, Szűcs; Lajos, Záhonyi

Információbiztonság fejlődés-történeti vizsgálata – Mérföldkövek, események és válaszok

Biztonságtudományi Szemle 3: 3 pp. 81-91., 11 p. (2021) [25]

Babos, Tibor; Záhonyi, Lajos

Az információbiztonság fejlődéstörténeti vizsgálata – az ERP rendszerek fejlődése

Biztonságtudományi Szemle 2: 3 pp. 55-66., 12 p. (2020) [15]

Lajos, Záhonyi

Conflicts and Information Security Challenges in the IT Bidding Process

In: Aniko, Kelemen-Erdos; Pal, Feher-Polgar; Anett, Popovics (szerk.)

FIKUSZ 2020 XV. International Conference Proceedings

Budapest, Magyarország, Óbuda University Keleti Károly Faculty of Business and Management (2021) 342 p. pp. 200-207., 8 p.

Közlemény: 31917271 Forrás Idéző Könyvrészlet (Konferenciaközlemény) Tudományos

Lajos, Záhonyi

Examination of the history of information security -The first ones

In: Nyikes, Zoltán szerk. (szerk.)

ICCECIP 2019 Absract book

Budapest, Magyarország: Óbudai Egyetem (2019) 52 p. p. 19, 1 p.

Lajos, Záhonyi

Conflicts and Information Security Challenges in the IT Bidding Process

In: Aniko, Kelemen-Erdos; Anett, Popovics; Pal, Feher-Polgar (szerk.)

XV. FIKUSZ 2020 International Conference Abstract Book

Budapest, Magyarország: Óbudai Egyetem, Keleti Károly Gazdasági Kar (2020) 72 p. p. 1, 1 p.

Kerti, András; Záhonyi, Lajos

A study of the history of information security – incidents, methods, standards and trends

National Security Review : Periodical Of The Military National Security Service 2020: 2 pp. 176-189., 14 p. (2020) [28]

Záhonyi, Lajos

Conflicts and information security challenges in the IT bidding process

In: Aniko, Kelemen-Erdos; Anett, Popovics; Pal, Feher-Polgar (szerk.)

XV. FIKUSZ 2020 International Conference Abstract Book

Budapest, Magyarország: Óbudai Egyetem, Keleti Károly Gazdasági Kar (2020) 72 p. pp. 42-42., 1 p.

Lajos Záhonyi, Endre Sűcs

Examining the Information Security Attitudes among Primary School-Aged Children

https://doi.org/10.7906/INDECS.23.3.12

URL: https://hrcak.srce.hr/332942

Interdisciplinary Description of Complex Systems: INDECS 2025.06.30

Kötet: 23, szám: 3 Oldal: 309-315

Kiadó: Hrvatsko interdisciplinarno društvo [122]

IRODALOMJEGYZÉK

[1] UNICEF, „Protecting the rights of every child in the digital environment: Public and Private Partnerships to Support Child Rights in a Digital Age and Bridge the Digital Divide," UNICEF, 12 07 2022. [Online]. Available: https://hlpf.un.org/2022/programme/protecting-the-rights-of-every-child-in-the-digital-environment-public-and-private. [Hozzáférés dátuma: 20 04 2023].

[2] NAIH, „Kulcsocska a net világához," Nemzeti Adatvédelmi és Információszabadság Hatóság, Budapest, 2017.

[3] G. Király, I. Dén-Nagy, Z. Géring és B. Nagy, „Kevert módszertani megközelítések. Elméleti és módszertani alapok," *Kultúra és Közösség IV. folyam V. évfolyam 2014/II. szám,* pp. 95-96, 2014.

[4] L. Berek, Biztonságtechnika, Budapest: Nemzeti Közszolgálati Egyetem, 2014, p. 6.

[5] L. Berek, L. Berek és Z. Rajnai, „A tudományos kutatás folyamata és módszerei," *Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar,* pp. 37-38, 2018.

[6] GJ, „Minuszos," 2020. [Online]. Available: https://www.minuszos.hu/tomegek-olvassak-a-gyerekaneten-hu-t/. [Hozzáférés dátuma: 14 11 2023].

[7] L. Berek, L. Berek és Z. Rajnai, A tudományos kutatásfolyamata és módszerei, Budapest: ÓE-BGK 3073, 2018.

[8] B., Nagy; G., Király; I., Dén-Nagy; Zs., Géring;, „Kevert módszertani megközelítések elméleti és módszertani alapok," *Kultúra és Közösség IV. folyam V. évfolyam 2014/II. szám,* pp. 96-98, 2014.

[9] „A magyar nyelv értelmező szótára (1959-62)," [Online]. Available: https://www.arcanum.com/hu/online-kiadvanyok/Lexikonok-a-magyar-nyelv-ertelmezo-szotara-1BE8B/b-1EF8E/biztonsag-2119D/?list=eyJmaWx0ZXJzIjogeyJNVSI6IFsiTkZPX0xFWF9MZXhpa29ub2

tfMUJFOEIiXX0sICJxdWVyeSI6ICJiaXp0b25zXHUwMGUxZyJ9. [Hozzáférés dátuma: 16 10 2024].

[10] L. Berek, T. Berek és L. Berek, Személy- és vagyonbiztonság, ÓE-BGK 3071, 2016, p. 6.

[11] „A társadalmi normák jellemzői," Oktatási Hivatal - Sulinet Tudásbázis, [Online]. Available: https://tudasbazis.sulinet.hu/hu/szakkepzes/rendeszet/tarsadalomismeret-eletmod/a-tarsadalmi-normak-jellemzoi-ismervei/a-tarsadalmi-normak-jellemzoi. [Hozzáférés dátuma: 28 04 2024].

[12] „European Data Protection Supervisor," [Online]. Available: https://www.edps.europa.eu/data-protection/our-work/subjects/information-security_en. [Hozzáférés dátuma: 19 11 2023].

[13] „Electropedia," International Electrotechnical Commission, [Online]. Available: https://electropedia.org/iev/iev.nsf/display?openform&ievref=831-02-06. [Hozzáférés dátuma: 14 04 2025].

[14] „Electropedia," International Electrotechnical Commission, [Online]. Available: https://electropedia.org/iev/iev.nsf/display?openform&ievref=871-04-16. [Hozzáférés dátuma: 14 04 2025].

[15] T. Babos és L. Záhonyi, „Az információbiztonság fejlődéstörténeti vizsgálata - az ERP rendszerek fejlődése," *Biztonságtudományi Szemle II. évf. 3. szám,* p. 64, 2020.

[16] Microsoft, „What is information security (InfoSec)?," Microsoft, [Online]. Available: https://www.microsoft.com/en-us/security/business/security-101/what-is-information-security-infosec. [Hozzáférés dátuma: 17 11 2024].

[17] *Az Európai Parlament és a Tanács (EU) 2019/881 rendelete az ENISA-ról (Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről,* 2019. április 17..

[18] ENISA, „Overview of cybersecurity and related terminology,” september 2017. [Online]. Available: https://www.enisa.europa.eu/sites/default/files/all_files/2017-09-07-ENISAoverviewOfCybersecurityAndRelatedTechnology.pdf. [Hozzáférés dátuma: 17 11 2024].

[19] Microsoft, „Terméktámogatás,” Microsoft Support, [Online]. Available: https://support.microsoft.com/hu-hu/topic/mi-az-a-kiberbiztons%C3%A1g-8b6efd59-41ff-4743-87c8-0850a352a390. [Hozzáférés dátuma: 17 11 2024].

[20] SAP, „What is cybersecurity?,” SAP SE., [Online]. Available: https://www.sap.com/products/financial-management/what-is-cybersecurity.html. [Hozzáférés dátuma: 17 11 2024].

[21] Nemzeti Adatvédelmi és Információszabadság Hatóság, [Online]. Available: https://www.naih.hu/adatvedelmi-szotar. [Hozzáférés dátuma: 07 06 2023].

[22] S. Kiss, „A biztonságtechnika kialakulásának történetéről,” *Hadmérnök, X. Évfolyam, 4. szám,* pp. 26-28, 2015.

[23] S. Kiss és L. Záhonyi, „Examination of the History of Information Security,” *National Security Review 2019/2.,* p. 88, 2019.

[24] E. Szűcs, „Az ősember "biztonságtechnikai" eszköze,” *Hadmérnök, XI. Évfolyam, 4. szám,* pp. 216-221, 2016.

[25] E. Szűcs és L. Záhonyi, „Információbiztonság fejlődéstörténeti vizsgálata - Mérföldkövek, események és válaszok,” *Biztonságtudományi Szemle, III. évf., 3. szám,* pp. 84-85, 2021.

[26] R. Bisbey és D. Hollingworth, „Protection Analysis - Final report, ARPA order No. 2223,” pp. 3-15., 1978.

[27] W. H. Ware, „R-609-1 - Security Controls for Computer Systems - Report of Defense Science Board Task Force on Computer Security,” Rand, Santa Monica, 1979.

[28] L. Záhonyi és A. Kerti, „A study of the history of information security – incidents, methods, standards and trends,” *National Security Review,* pp. 176-189, 2020.

[29] Testület, Magyar Szabványügyi, MSZ SO/IEC 27001:2014, ISO (the International Organization for Standardization), 2014, p. p6.

[30] „https://generaciok.com,” Steigervald Krisztián generációs oldala, 2024. [Online]. Available: https://generaciok.com/generaciok/. [Hozzáférés dátuma: 22 03 2025].

[31] Á. Nagy és A. Fazekas, „A fiatalok szabadidõs tereinek és médiahasználatának átalakulása,” *Médiaelméleti folyóirat, XVI. évf. 2. szám,* pp. 42-48, 2016.

[32] A. Kolnhofer-Derecskei, R. Reicher és Á. Szeghegyi, „The X and Y Generations’ Characteristics Comparison,” *Acta Polytechnica Hungarica, 2017. 14 évf. 8. szám,* p. 122.

[33] A. Schüller, „Az Y generáció és az információbiztonság,” *Hadmérnök, VI. Évfolyam 2. szám,* pp. 343-345, 2011.

[34] G. Bak és A. Kelemen-Erdős, „Információbiztonság-tudatosság az Y generáció szemszögéből, kvalitatív megközelítés alapján,” *Hadmérnök, 2022. 17. évfolyam 3. szám,* pp. 89-90.

[35] S. Zoltán, „A magyar ifjúság generációs sajátosságai és a biztonsághoz való viszonyulása,” *Honvédségi Szemle, 149 évf. 3. szám,* pp. 81-84, 2021.

[36] Á. Csiszárik-Kocsir, Vállalkozásfejlesztés a XXI. században - Újszerű meglátások és hagyományos megoldások napjaink gazdasági és társadalmi problémáinak kezelésében, Budapest: Óbudai Egyetem, Keleti Károly Gazdasági Kar, 2024, pp. 270-274.

[37] Nemzeti Média- és Hírközlési Hatóság, 16 09 2024. [Online]. Available: https://nmhh.hu/cikk/248473/A_1316_eves_korosztaly_kozossegimediahasznalati_szokasait_felmero_kutatas_eredmenyei. [Hozzáférés dátuma: 02 02 2025].

[38] Jha, Amrit Kumar, „Understanding Generation Alpha," p. 2, 2020.

[39] McCrindle, Mark; Fell, Ashley, Understanding Generation Alpha, Solent Circuit, Australia: McCrindle Research Pty Ltd, 2020, pp. 6-8.

[40] Yuliana, „The importance of cybersecurity awareness for children," *Lampung Journal of International Law (LaJIL), Volume 4 Issue 1,* pp. 41-43, 2022.

[41] Rahman, N. A. A.; Sairi, I. H.; Zizi, N. A. M.; Khalid, F., „The Importance of Cybersecurity Education in School," *International Journal of Information and Education Technology, Vol. 10, No. 5.,* pp. 378-379, 2020.

[42] B. Bhatnagar, „One in six school-aged children experiences cyberbullying, finds new WHO/Europe study," World Health Organization, 27 03 2024. [Online]. Available: https://www.who.int/europe/news/item/27-03-2024-one-in-six-school-aged-children-experiences-cyberbullying--finds-new-who-europe-study. [Hozzáférés dátuma: 18 08 2025].

[43] S. Munk, „Információbiztonság vs. Informatikai biztonság," *Hadmérnök, Különszám Robothadviselés 7. Tudományos Szakmai Konferencia,* p. 1, 2007.

[44] Quayyum, Farzana; Cruzes, Daniela S. ; Jaccheri, Letizia, „Cybersecurity awareness for children: A systematic literature review," *International Journal of Child-Computer Interaction, Volume 30.,* 2021.

[45] Clemons, Eric k.; Wilson, Joshua S., „Family Preferences Concerning Online Privacy, Data Mining, and Targeted Ads: Regulatory Implications," *Journal of Management Information Systems, Volume 32, Issue 2,* 2015.

[46] Hofstra, Bas; Corten, Rense; Tubergen, Frank van, „Understanding the privacy behavior of adolescents on Facebook: The role of peers, popularity and trust," *Computers in Human Behavior, Volume 60,* pp. 611-621, 2016.

[47] Chang, Victor; Golightlyb, Lewis; Xua, Qianwen Ariel; Boonmeec, Thanaporn; Liu, Ben S., „Cybersecurity for children: an investigation into the application of social media," *Enterprise Information System, VOL. 17, NO. 11,* pp. 1503-1504, 2023.

[48] Albuquerque, Otávio de Paula; Fantinato, Marcelo; Kelner, Judith, „Privacy in smart toys: Risks and proposed solutions,” *Electronic Commerce Research and Applications, Volume 39,* 2020.

[49] Desimpelaere, Laurien; Hudders, Liselot; Sompel, Dieneke Van de, „Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior,” *Computers in Human Behavior, Volume 110,* 2020.

[50] J. L. Yen és C. Chamanadjian, „Cyberbullying and Online Aggression,” *Pediatric Clinics of North America,* pp. 333-349, 2025.

[51] Aponte, Diego Fernando Gutierrez; Richards, Deborah, „Managing cyber-bullying in online educational virtual worlds,” *IE '13: Proceedings of The 9th Australasian Conference on Interactive Entertainment: Matters of Life and Death, v.18,* pp. 1-9, 2013.

[52] Quayyum, Farzana, „Co-designing cybersecurity-related stories with children: Perceptions on cybersecurity risks and parental involvement,” *Entertainment Computing, Volume 52, January 2025,* 2024.

[53] Muir, Kate; Joinson, Adam, „An Exploratory Study Into the Negotiation of Cyber-Security Within the Family Home,” *Applied Digital Behaviour Lab, School of Management, University of Bath,* 2020.

[54] E. Lastdrager, I. C. Gallardo, P. Hartel és M. Junger, „How effective is anti-phishing training for children?,” *In Thirteenth symposium on usable privacy and security,* pp. 229-239, 2017.

[55] Von Solms, Rossouw; Von Solms, Suné, „Cyber Safety Education in Developing Countries,” 2015.

[56] Tsirtsis, Andreas; Tsapatsoulis, Nicolas; Stamatelatos, Makis; Papadamou, Kwstantinos; Sirivianos, Michael, „Cyber Security Risks for Minors: A Taxonomy and a Software Architecture,” 2016.

[57] M. Teimouri, S. R. Benrazavi, M. D. Griffiths és S. Hassan, „A Model of Online Protection to Reduce Children's Online Risk Exposure: Empirical Evidence From Asia," *Sexuality & Culture,* pp. 1205-1215, 2018.

[58] F. Giannakas, A. Papasalouros, G. Kambourakis és S. Gritzalis, „A comprehensive cybersecurity learning platform for elementary education," *Information Security Journal: A Global Perspective, volume 28,* pp. 82-85, 2019.

[59] „KiberPajzs Projekt," 2022. [Online]. Available: https://www.kiberpajzs.hu/a-kezdemenyezesrol. [Hozzáférés dátuma: 21 11 2023].

[60] S. Bannon, T. McGlynn, K. McKenzie és E. Quayle, „The internet and young people with Additional Support Needs (ASN): Risk and safety," *Computers in Human Behavior, volume 53,* pp. 495-503, 2015.

[61] Y.-Y. Choong, M. F. Theofanos, K. Renaud és S. Prior, „"Passwords protect my stuff" — a study of children's password practices," *Journal of Cybersecurity, volume 5, Issue 1,* pp. 1-19, 2019.

[62] Y. Tang és X. Ning, „Understanding user misrepresentation behavior on social apps: The perspective of privacy calculus theory," *Decision Support Systems, volume 165,* pp. 1-10, 2023.

[63] T. Fania és F. Ghaemib , „Implications of Vygotsky's Zone of Proximal Development (ZPD) in Teacher Education: ZPTD and Self-scaffolding," *Procedia - Social and Behavioral Sciences, volume 29,* pp. 1549-1554, 2011.

[64] A. Bourgeus, L. Vandercruysse és N. Verhulst, „Understanding contextual expectations for sharing wearables' data: Insights from a vignette study," *Computers in Human Behavior Reports, volume 15,* pp. 1-8, 2024.

[65] S. Carey, D. Zaitchik és I. Bascandziev, „Theories of development: In dialog with Jean Piaget," *Developmental Review, volume 38,* pp. 36-54, 2015.

[66] C.-Y. Tsai, W.-L. Shih, F.-P. Hsieh, Y.-A. Chen, C.-L. Lin és H.-J. Wu, „Using the ARCS model to improve undergraduates' perceived information security

protection motivation and behavior," *Computers & Education, volume 81,* pp. 1-11, 2022.

[67] K. Degirmenci, „Mobile users' information privacy concerns and the role of app permission requests," *International Journal of Information Management, volume 50,* pp. 261-271, 2020.

[68] F. Fatima, J. C. Hyatt, S. U. Rehman, E. De La Cruz, G. S. Nadella és K. Meduri, „Resilience and risk management in cybersecurity: A grounded theory study of emotional, psychological, and organizational dynamics," *Journal of Economy and Technology, volume 2,* p. 247–257, 2024.

[69] U. Kiran, N. F. Khan, H. Murtaza, A. Farooq és H. Pirkkalainen, „Explanatory and predictive modeling of cybersecurity behaviors using protection motivation theory," *Computers & Security, volume 149,* pp. 1-3, 2025.

[70] Hochbaum, Rosenstock and others, „The Rural Health Information Hub," [Online]. Available: https://www.ruralhealthinfo.org/toolkits/health-promotion/2/theories-and-models/health-belief. [Hozzáférés dátuma: 10 04 2025].

[71] M. Cummings, K. N. Bergman és K. A. Kuznicki, Emerging Methods in Family Research, National Symposium on Family, volume 4, 2024.

[72] Mesch, Gustavo S., Parental Mediation, Online Activities and Cyberbullying, Haifa: Department of Sociology and Anthropology, University of Haifa, 2009.

[73] L. Záhonyi és E. Szűcs, „Examining the relationship and legal regulation of information security and data protection, with particular regard to the communication habits of young people," *National Security Review, volume 1,* pp. 180-192, 2023.

[74] „Gyerek a neten Projekt," Nemzeti Média- és Hírközlési Hatóság (NMHH), [Online]. Available: https://gyerekaneten.hu/. [Hozzáférés dátuma: 13 11 2023].

[75] *Az állami és önkormányzati szervek elektronikus információbiztonságáról,* 2013. évi L. törvény.

[76] *A természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kív,* Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.).

[77] *A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet – GDPR),* Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.).

[78] *Az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv),* Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.).

[79] *Az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv – ePrivacy irányelv),* Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.).

[80] *Az informatikai rendszer védelméről,* MNB 1/2025. (I.13.) számú ajánlás.

[81] *Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe so,* 41/2015. (VII. 15.) BM rendelet.

[82] *Magyarország kiberbiztonságáról,* 2024. évi LXIX. törvény.

[83] *Magyarország kiberbiztonságáról szóló törvény végrehajtásáról,* 418/2024. (XII. 23.) Korm. rendelet.

[84] *Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer*

biztonságáért felelős személyek képzésének tartalmáról, 26/2013. (X. 21.) KIM rendelet.

[85] Baracsi Katalin LL.M., Interviewee, *Interjú.* [Interjú]. 22 05 2022.

[86] „WHO recommendations on child health: guidelines approved by the WHO Guidelines Review Committee," World Health Organization, 2017. [Online]. Available: https://www.who.int/publications/i/item/WHO-MCA-17.08. [Hozzáférés dátuma: 17 11 2024].

[87] „Child rights and human rights explained," UNICEF, [Online]. Available: https://www.unicef.org/child-rights-convention. [Hozzáférés dátuma: 17 11 2024].

[88] UNICEF, „Convention on the Rights of the Child," UNICEF, [Online]. Available: https://www.unicef.org/child-rights-convention. [Hozzáférés dátuma: 25 10 2024].

[89] Az információbiztonság lélektana, Budapest: Nemzeti Kibervédelmi Intézet, 2018, p. 10.

[90] „KSH," Központi Statisztikai Hivatal, [Online]. Available: https://www.ksh.hu/infografika/2023/becsongettek_2023.pdf. [Hozzáférés dátuma: 01 09 2023].

[91] „KSH," Központi Statisztikai Hivatal, [Online]. Available: https://statinfo.ksh.hu/Statinfo/index.jsp. [Hozzáférés dátuma: 01 09 2023].

[92] „Témák," Európai Parlament, 2021. [Online]. Available: https://www.europarl.europa.eu/topics/hu/article/20211008STO14521/miert-fontos-a-kiberbiztonsag-es-mibe-kerulhet-egy-kibertamadas-az-erintettnek. [Hozzáférés dátuma: 01 09 2023].

[93] „FBI," Federal Bureau of Investigation, 2024. [Online]. Available: https://www.ic3.gov/AnnualReport/Reports. [Hozzáférés dátuma: 02 05 2025].

[94] eSentire, „2023 Annual Cybercrime Report," 2023. [Online]. Available: https://www.esentire.com/web-native-pages/cybercrime-to-cost-the-world-9-5-

trillion-usd-annually-in-2024?utm_source=chatgpt.com. [Hozzáférés dátuma: 22 05 2024].

[95] Oktatási Hivatal, „oktatas.hu,” [Online]. Available: Digitális Kultúra. https://www.oktatas.hu/pub_bin/dload/kozoktatas/kerettanterv/Digitalis_kultura_K.docx. [Hozzáférés dátuma: 17 05 2023].

[96] L. Záhonyi és E. Szűcs, „Examining information security educational tool systems, in the light of juvenile cyber security risks,” *National Security Review,* pp. 134-144, 2023.

[97] A. Vitéz, Szerk., Digitális kultúra tankönyv 3., Budapest: Oktatási Hivatal, 2021.

[98] A. Vitéz, Szerk., Digitális kultúra tankönyv 4., Budapest: Oktatási Hivatal, 2022.

[99] G. Pintér, Szerk., Digitális kultúra tankönyv 5., Budapest: Oktatási Hivatal, 2020.

[100] G. Pintér, Szerk., Digitális kultúra tankönyv 6., Budapest: Oktatási Hivatal, 2020.

[101] S. Széll, Szerk., Digitális kultúra tankönyv 7., Budapest: Oktatási Hivatal, 2022.

[102] S. Széll, Szerk., Digitális kultúra tankönyv 8., Budapest: Oktatási Hivatal, 2023.

[103] B., Ságvári; B., Kollányi; Sz., Kovács;, „DIGIKID - Kérdőív- és applikáció-alapú adatgyűjtés a 8-15 éves korosztály digitális eszközhasználatáról,” Fabricula Bt., 2023.

[104] L, Székely; Z., Kántor; Domokos T.; Pillók P., „Magyar Fiatalok 2020 - Kérdések és válaszok - Fiatalokról, fiataloktól,” Társadalomkutató Kft., Budapest, 2020.

[105] B., Ságvári;, „Az EU Kids Online magyarországi kutatásáról,” Nemzeti Média- és Hírközlési Hatóság, Budapest, 2011.

[106] M., Bernschütz;, „Magyar Tinik a Neten 2021 online felmérés," Be Social, Budapest, 2021.

[107] „Magyar Tinik a Neten 2023," Be Social, Budapest, 2023.

[108] OFCOM, „Online Nation," https://www.ofcom.org.uk/, United Kingdom, 2023.

[109] K., Dr. Baracsi;, „Online Sangoval," *Nemzetközi Távközlési Egyesület (International Telecommunication Union, ITU),* %1. kötetHungarian Edition, 2020.

[110] „Child Online Safety Index Report," DQ Institute, Singapore, 2022.

[111] „Les enfants de moins de 6 ans et les écrans numériques…," L'Institut national de la statistique et des études économiques (Insee), Paris, 2022.

[112] „BornSocial #2023," @heavenagency, Paris, 2023.

[113] Vogels, Emily A., „Teens and Cyberbullying," PEW Research Center, Washington DC., 2022.

[114] „Kék Vonal," Kék Vonal Gyermekkrízis Alapítvány , [Online]. Available: https://kek-vonal.hu/projektek/beszelj-rola. [Hozzáférés dátuma: 05 09 2024].

[115] „Safer Internet," Magyarországi Safer Internet Center, [Online]. Available: https://saferinternet.hu/. [Hozzáférés dátuma: 05 09 2024].

[116] G., Fegyverneki; A., Horváth; Á., Horváth; Á., Lajtos; E., Ormai; E., Sipos; K., Temesi-Ferenczi; M., Tóth;, Iránytű az alsósokra hangolva - Médiatudatosságot fejlesztő óratervek és feladatok tanórai felhasználáshoz, Budapest: Bűvösvölgy Médiaértés-oktató Központ, 2021.

[117] Gy., Danó; É., Kósa; M., László;, „A digitális világ veszélyei," XII. kerületi Önkormányzat, Budapest, 2016.

[118] Internet Hotline, „Gyermekek a neten és digitális szülőség," Nemzeti Média- és Hírközlési Hatóság (NMHH), Budapest, 2020.

[119] P., Edvi;, „Beszámoló a Biztonsagosinternet.hu hotline 2023. évi tevékenységéről,” Nemzetközi Gyermekmentő Szolgálat Magyar Egyesület, Budapest, 2024.

[120] Foundation, Internet Watch, „www.biztonsagosinternet.hu,” [Online]. Available: https://www.biztonsagosinternet.hu/tippek/szexualis-behalozas-grooming. [Hozzáférés dátuma: 06 09 2024].

[121] „Cyber Safety for Vulnerable Populations,” Munster Technological University, [Online]. Available: https://cybersafety.ie/about-us/. [Hozzáférés dátuma: 12 09 2025].

[122] L. Záhonyi és E. Szűcs, „Examining the Information Security Attitudes among Primary School-Aged Children,” *Interdisciplinary Description of Complex Systems: INDECS, volume 23, issue 3,* pp. 309-315, 2025.

[123] KSH, „Az óvodai nevelésben, iskolai oktatásban részesülők a nappali és a nem nappali oktatásban, iskoláskorú népesség,” Központi Statisztikai Hivatal, Budapest, 2024.

[124] KSH, „Budapest 04. kerület,” [Online]. Available: https://www.ksh.hu/apps/hntr.telepules?p_lang=HU&p_id=05467. [Hozzáférés dátuma: 19 12 2024].

[125] A., Szabó;, „Újpest története: Egy folyamatosan változó kerület,” Újpesti Hírmondó, 21 10 2023. [Online]. Available: https://ujpestihirmondo.hu/ujpest/ujpest-tortenete-egy-folyamatosan-valtozo-kerulet/. [Hozzáférés dátuma: 19 12 2024].

[126] Újpestért, Egyesület;, „Újpest története,” [Online]. Available: https://ujpestertegyesulet.hu/ujpest-tortenete/. [Hozzáférés dátuma: 19 12 2024].

[127] J., Simon; Zs., Berezvai; I., Kemény; Zs., Kun; T., Pusztai;, Kvantitatív elemzési módszerek - SPSS használata a kutatási gyakorlatban, Budapest: Budapesti Corvinus Egyetem, 2024, pp. pp55-56..

[128] J., Simon; Zs., Berezvai; I., Kemény; Zs., Kun; T., Pusztai;, Kvantitatív elemzési módszerek - SPSS használata a kutatási gyakorlatban, Budapest: Budapesti Corvinus Egyetem, 2024, pp. 66-82.

[129] J., Simon; Zs., Berezvai; I., Kemény; Zs., Kun; T., Pusztai;, Kvantitatív elemzési módszerek - SPSS használata a kutatási gyakorlatban, Budapest: Budapesti Corvinus Egyetem, 2024, pp. 110-112..

[130] „SPSSABC.HU," Mayer Annamária, 2021. [Online]. Available: https://spssabc.hu/ketvaltozos-elemzes/spearman-korrelacio/. [Hozzáférés dátuma: 18 01 2025].

[131] „A Kruskal–Wallis-próba," Károli Gáspár Református Egyetem, 1952. [Online]. Available: http://www.kre.hu/ebook/dmdocuments/Jegyzet_a_Matematikai_Statisztika_margojara/chap_70.html. [Hozzáférés dátuma: 18 01 2025].

[132] L. Záhonyi és E. Szűcs, „Examining the Information Security Attitudes among Primary School-Aged Children," *Interdisciplinary Description of Complex Systems: INDECS 2025.06.30, volume 23, issue 3,* pp. 309-315.

TÁBLÁZATJEGYZÉK

ÁBRAJEGYZÉK

FÜGGELÉK

Kvalitatív kutatás szakmai interjú kérdései

1. Milyen digitális kockázatokkal találkozhatnak leggyakrabban az általános iskolás korú gyermekek az Ön megítélése szerint?
2. Mit gondol, mennyire vannak a szülők felkészülve erre a szerepre a mai digitális környezetben?
3. Milyen típusú támogatást tartana szükségesnek ahhoz, hogy a tanárok hatékonyabban tudják segíteni a gyerekeket az információbiztonsággal kapcsolatban?
4. Milyen szerepe van az államnak az információbiztonság oktatásában és a családok támogatásában?
5. Véleménye szerint mennyire tartja hatékonynak a jelenlegi jogi szabályozást és prevenciós törekvéseket?
6. Ön szerint hány éves korban lenne ideális, hogy a gyermekek első okostelefonjukat megkapják és milyen hatásai lehetnek annak, ha a gyermek túl korán vagy túl későn jut saját digitális eszközhöz?

Kérdések a kvantitatív kutatás eredményeinek szakértői értékeléséhez

1. A DigiÓ kutatás eredményei azt mutatták, hogy a gyermek érintettsége fokozza az igényt az állami szerepvállalás iránt az információbiztonsági védelemben és felkészítésben. Ön mennyire ért egyet ezzel a megállapítással?
2. Az eredmények alapján azok a gyerekek, akiknél a szülők rendszeresen beszélgetnek velük az online biztonságról, nagyobb arányban számolnak be incidensekről. Ugyanakkor a szülői közösségimédia-korlátozás csökkenti az online zaklatás esélyét és a tudatosság a kontrollal együtt bizonyult hatékony védelmi eszköznek. Ön szerint mennyire helytálló ez az összefüggés?
3. A kutatás kimutatta, hogy minél idősebbek a gyermekek, illetve minél magasabb évfolyamra járnak, annál nagyobb valószínűséggel találkoznak információbiztonsági kockázatokkal. Ön hogyan látja ezt a tendenciát?

4. A DigiÓ kutatás kimutatta, hogy az Y generáció szülői átlagosan korábban adnak okostelefont gyermekeiknek, mint az X generációs szülők, miközben az ideális életkor megítélésében nincs eltérés. Hogyan értékeli ezt a jelenséget?
5. Mit gondol arról a megállapításról, hogy a tanárok információbiztonsági felkészültségének önértékelése nem minden esetben esik egybe a valós szükségletekkel?

Kiberbiztonsági kockázatok csoportosítása (táblázat)

Kiberbiztonsági kockázatok csoportosítása			
Kiberbiztonsági kockázatok	Online adatvédelem Online Privacy)	Adatvédelem a közösségi hálózatokon	az információk megsértése és/vagy kitettség
			az információk túlzott mértékű megosztása
			földrajzi címkézés (megjelölés)
			közösségi média fiókok feltörése
		adatvédelem (magánvédelem) az intelligens játékokban	gyenge titkosítás
			audio injekciós támadás (audio sérüléses támadás)
			lehallgatás (eavesdropping)
			érzékeny információk kiszolgáltatása
			adatmegfigyelés, kémkedés
			gyermek reklám
			jogosulatlan távvezérlés
		Harmadik fél általi nyomonkövetés	
	online zaklatás (online harassement)	kiberbántalmazás (cyberbullying)	Lángolás (Flaming)
			hínévrontás (denigration)
			megszemélyesítés (impersonation)
			álcázás (masquerading)
			Outing
			csalás, tükkösködés (trickery)
			kiközösítés és kirekesztés
		cyberstalking	Lángolás (Flaming)
			személyazonosság-lopás (identity theft)
			e-mail hamisítás (email forgery)
			vírus
	idegen veszély (stranger danger)	cybergrooming	
		Catfishing	
		megszemélyesítés (impersonation)	
	social engeneering	Phising	
		személyazonosság-lopás (identity theft)	
	tartalommal kapcsolatos kockázatok (content related risks)	nem megfelelő tartalom	
		pornográfia	
		célzott reklám	
		erőszakos, káros, deviáns tartalom	

		illegális tartalmak	
		szerzői jog (copy right)	
		spamek	
	szexuális felbújtás (sexual solicitation) szexuális tartalmak megosztása?	sexting	
		kockázatos szexuális viselkedés / magatartás	
		kiberszex	
	technológiai alapú fenyegetések	rosszindulatú szoftver (malware)	
		vírus	
		hacking (hekkelés)	
		zsarolóvírus (ransomware)	
		örökölt genyegetések? (legacy threats)	
		hamisítás (spoofing)	
		kémszoftver (spyware)	
	gazdasági alapú kockázatok (economy risks)	online szerencsejáték	
		pénzügyi csalások(financial scams)	személyazonosság lopás (identity theft)
			csaló hívások (scam calls)
	internetfüggőség (internet addiction)		
	jelszókezelés gyakorlata (password practice and management)		

Óbudai Egyetem – DigiÓ Kutatást Támogató Levél

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Támogató levél - kutató részére

Kutató: Záhonyi Lajos hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola (1081 Budapest, Népszínház u. 8.) Neptun kód: GRCLXZ, Tel: +36 30 283 0098, E-mail: zahonyi.lajos@uni-obuda.hu

A kutatás keretei: hallgatói kutatói munka keretében zajlik, együttműködve több alapfokú intézménnyel és civil szervezettel.

A kutatás neve: "DigiÓ - kérdőív alapú adatgyűjtés az általános iskolás korú korosztály információbiztonságáról - kutatás".

A kutatás célja: Az általános iskolás korú fiatalok információbiztonsági és online biztonsági kihívásainak, valamint a kapcsolódó oktatási és jogi eszközök és eszközrendszerek vizsgálata az információbiztonság fejlődéstörténetének tükrében. A kutatásban arra szeretnék választ kapni, hogy az online térben mennyire tudatosan néz szembe ez a korosztály a veszélyekkel, illetve a szülők, pedagógusok mit tapasztalnak.

A kérdőíves vizsgálati kutatás időszaka: 2023.11.01. - 2024.01.31.

Kutatás eredményeinek megjelenése: doktori disszertáció keretében, publikusan.

Alulírott Prof. Dr. Goda Tibor János egyetemi tanár, az Óbudai Egyetem Biztonságtudományi Doktori Iskola vezetője, támogatom Záhonyi Lajos kutatói munkáját!

ÓBUDAI EGYETEM Biztonságtudományi Doktori Iskola I. Budapest

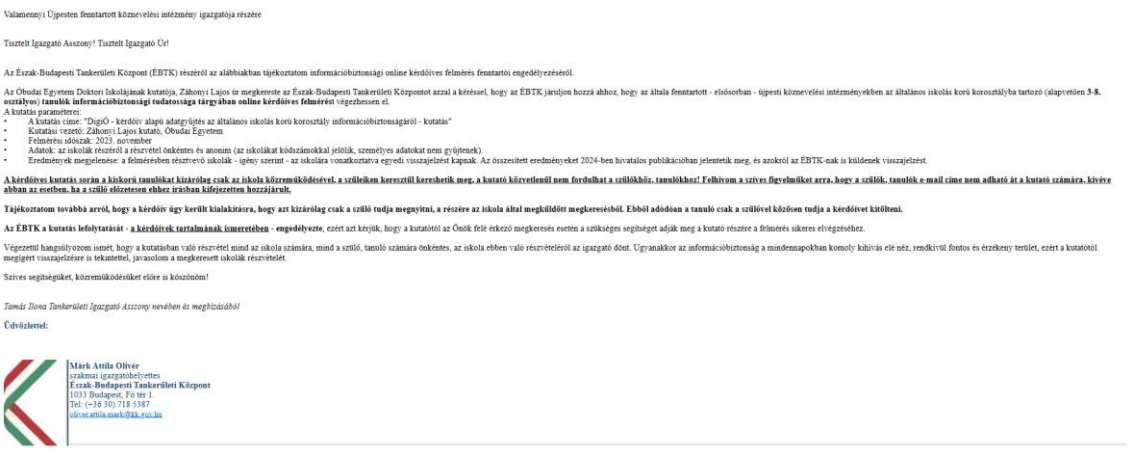
aláírás, Ph.

Kelt: Budapest, 2023. október 17.

DigiÓ kutatás - Észak-Budapesti Tankerületi Központ (EBTK) képviselőjének engedélyező levele

Feladó: Márk Attila Olivér <oliver.attila.mark@kk.gov.hu>

Elküldve: 2023. november 10., péntek 11:05



Valamennyi Újpesten fenntartott köznevelési intézmény igazgatója részére

Tisztelt Igazgató Asszony! Tisztelt Igazgató Úr!

Az Észak-Budapesti Tankerületi Központ (ÉBTK) részéről az alábbiakban tájékoztatom információbiztonsági online kérdőíves felmérés fenntartói engedélyezéséről.

Az Óbudai Egyetem Doktori Iskolájának kutatója, Záhonyi Lajos úr megkereste az Észak-Budapesti Tankerületi Központot azzal a kéréssel, hogy az ÉBTK járuljon hozzá ahhoz, hogy az általa fenntartott - elsősorban - újpesti köznevelési intézményekben az általános iskolás korú korosztályba tartozó (alapvetően **3-8. osztályos**) **tanulók információbiztonsági tudatossága tárgyában online kérdőíves felmérést** végezhessen el.
A kutatás paraméterei:

- A kutatás címe: "DigiÓ - kérdőív alapú adatgyűjtés az általános iskolás korú korosztály információbiztonságáról - kutatás"
- Kutatási vezető: Záhonyi Lajos kutató, Óbudai Egyetem
- Felmérési időszak: 2023. november
- Adatok: az iskolák részéről a részvétel önkéntes és anonim (az iskolákat kódszámokkal jelölik, személyes adatokat nem gyűjtenek).
- Eredmények megjelenése: a felmérésben résztvevő iskolák - igény szerint - az iskolára vonatkoztatva egyedi visszajelzést kapnak. Az összesített eredményeket 2024-ben hivatalos publikációban jelentetik meg, és azokról az ÉBTK-nak is küldenek visszajelzést.

A kérdőíves kutatás során a kiskorú tanulókat kizárólag csak az iskola közreműködésével, a szülőiken keresztül keresthetik meg, a kutató közvetlenül nem fordulhat a szülőkhöz, tanulókhoz! Felhívom a szíves figyelmüket arra, hogy a szülők, tanulók e-mail címe nem adható át a kutató számára, kivéve abban az esetben, ha a szülő előzetesen ehhez írásban kifejezetten hozzájárult.

Tájékoztatom továbbá arról, hogy a kérdőív úgy került kialakításra, hogy azt kizárólag csak a szülő tudja megnyitni, a részére az iskola által megküldött megkeresésből. Ebből adódóan a tanuló csak a szülővel közösen tudja a kérdőívet kitölteni.

Az ÉBTK a kutatás lefolytatását - a kérdőívek tartalmának ismeretében - engedélyezte, ezért azt kérjük, hogy a kutatótól az Önök felé érkező megkeresés esetén a szükséges segítséget adják meg a kutató részére a felmérés sikeres elvégzéséhez.

Végezetül hangsúlyozom ismét, hogy a kutatásban való részvétel mind az iskola számára, mind a szülő, tanuló számára önkéntes, az iskola ebben való részvételéről az igazgató dönt. Ügyeinkkor az információbiztonság a mindennapokban komoly kihívás elé néz, rendkívül fontos és érzékeny terület, ezért a kutatótól megígért visszajelzésre is tekintettel, javasolom a megkeresett iskolák részvételét.

Szíves segítségüket, közreműködésüket előre is köszönöm!

Tamás Ilona Tankerületi Igazgató Asszony nevében és megbízásából

Üdvözlettel:

Márk Attila Olivér
szakmai igazgatóhelyettes
Észak-Budapesti Tankerületi Központ
1033 Budapest, Fő tér 1.
Tel: (+36 30) 718 5387
oliver.attila.mark@kk.gov.hu

Az Észak-Budapesti Tankerületi Központ (EBTK) megkeresett intézményeknek szóló levél

Tárgy: Fw: tájékoztatás információbiztonsági online kérdőíves felmérés fenntartói engedélyezéséről_Szucs

Tisztelt Igazgató Úr!
Kedves András!

*Köszönöm a kezdeti nyitott hozzáállását és akkor el is indulnánk. Mostanra sikerült összeszedni minden olyan kiegészítő engedélyt ami a kutatáshoz kell.

Az Észak-Budapesti Tankerületi Központ (ÉBTK) 2023. november 10. megküldött tájékoztatása és jóváhagyása alapján, szeretném együttműködő segítségét kérni az Óbudai Egyetem által elindított "DigiÓ - kérdőív alapú adatgyűjtés az általános iskolás korú korosztály információbiztonságáról - kutatás" című kutatáshoz.
A kérdőíveknek két iránya van:

1. szülők és rajtuk keresztül a gyerekek;
2. pedagógusok, nevelők.

Több intézménnyel folytatott előzetes egyeztetés alapján, valamint figyelembe véve a tanári állomány leterheltségét szeretném segíteni a kutatás folyamatát azzal, hogy egy előre megírt szövegjavaslatot küldök illetve jelzem hogy a kérdőívek lényegretörőek, nem hosszúak.

Kérem, hogy ezt a levélszöveg javaslatot – mint intézményi vezető – saját szavakkal kiegészítve küldje ki az iskolai szülői közös listára vagy a Kréta programon keresztül vagy bármilyen egyéb - az iskolában szokásos – módon a szülők valamint a pedagóguskollégák részére.

Kutatással érintett javasolt gyerek évfolyamok: 3-8 (harmadikosoktól, nyolcadikig) minden évfolyam.
Szülők és pedagógusok esetében mindenkire számítunk.
Adatgyűjtésre javasolt határidő: kiküldéstől számított 2 hét. Példadátum: 2023. 11.30.
Az Ön iskolájának kódja:
ÚJPESTI SZÚCS SÁNDOR ÁLTALÁNOS ISKOLA EBTK114

Szülőknek szóló kérdőív:
https://docs.google.com/forms/d/e/1FAIpQLSf3AiwRaK2oKIEXqcbrG0_fGvN9Fm3l4nxcr-ypPq9pa8VrkQ/viewform?usp=sf_link
(A gyerekeknek szóló kérdőív a szülői kérdőívből indul!)

Tanárok, pedagógusok és nevelők kérdőíve:
https://docs.google.com/forms/d/e/1FAIpQLSfoehhMylHevR7SH4ody1qiSTYfg85wdRWsOwc743d6CSmGNw/viewform?usp=sf_link

Köszönöm szíves közreműködését, amennyiben kérdése van keressen bizalommal!
Levelemhez mellékelem a Tankerület és az Óbudai Egyetem támogató levelét.

Üdvözlettel:

Záhonyi Lajos
Óbudai Egyetem
Biztonságtudományi Doktori Iskola
1081 Budapest, Népszínház u. 8.
Tel: +36 30 283 0098
E-mail: zahonyi.lajos@uni-obuda.hu

levélszöveg javaslat
*****

Tisztelt Szülők!
Az Észak-Budapesti Tankerületi Központ (ÉBTK) támogatásával iskolánk részt vesz az Óbudai Egyetem Kutatásában, melyben a gyerekek információbiztonsági tudatosságát mérik fel. A kutatás anonim és nem gyűjt személyes adatokat.
A kutatás elvégzését iskolánk támogatja és az eredményéről visszajelzést kapunk.
Kérünk, minden kedves szülőt töltse ki a kérdőívet majd ezt követően a gyermekével a gyerekeknek szóló kérdőívet, amelyet a szülői kérdőívből tudnak majd megnyitni.

Szülőknek szóló kérdőív:
https://docs.google.com/forms/d/e/1FAIpQLSf3AiwRaK2oKIEXqcbrG0_fGvN9Fm3l4nxcr-ypPq9pa8VrkQ/viewform?usp=sf_link

Iskolánk kódja, amit a kérdőívben ki kell választani: EBTK114
A kérdőív kitöltésének határideje: 2023. 11.30.

***

Kedves Pedagógus Kollégák!
Az Észak-Budapesti Tankerületi Központ (ÉBTK) támogatásával iskolánk részt vesz az Óbudai Egyetem Kutatásában, melyben a gyerekek információbiztonsági tudatosságát mérik fel. A kutatás anonim és nem gyűjt személyes adatokat.
A kutatás elvégzését iskolánk támogatja és az eredményéről visszajelzést kapunk majd.
Kérünk, minden kedves kollégát hogy töltse ki ezt a rövid kérdőívet!

Tanárok, pedagógusok és nevelők kérdőíve:
https://docs.google.com/forms/d/e/1FAIpQLSfoehhMylHevR7SH4ody1qiSTYfg85wdRWsOwc743d6CSmGNw/viewform?usp=sf_link

Iskolánk kódja, amit a kérdőívben ki kell választani: EBTK114
A kérdőív kitöltésének határideje: 2023. 11.30.

Nemzetközi kutatási és projekt tapasztalatszerzés KREMS IMC Egyetem

FH KREMS
UNIVERSITY OF APPLIED SCIENCES

CONFIRMATION OF PARTICIPATION

TRANSCRIPT OF RECORDS

The IMC University of Applied Sciences Krems confirms the successful participation of

Lajos Zahonyi

in the

Blended Intensive Programme
VR/AR Innovative Applications for Example Companies

from April 24 - May 05, 2023

The student is awarded 4 ECTS for the participation in the physical and virtual component of the progamme.

IMC Fachhochschule Piaristengasse 1 A-3500 Krems Krems GmbH

Krems, May 05, 2023

Prof. (FH) Mag. Dr. Martin Waiguny
Academic Head

Részvétel nemzetközi kutatási projektben az írországi Munster Technological University - Chair of Cybersecurity tanszéken

MTU
Ollscoil Teicneolaíochta na Mumhan
Munster Technological University

Confirmation letter

To whom it may concern,

We are pleased to confirm that Mr. Lajos Záhonyi, a PhD researcher from the Doctoral School on Safety and Security Sciences at Óbuda University (Hungary), will undertake a short-term research placement with the Cyber Explore Research Group at Munster Technological University (MTU), Cork, Ireland.

During his stay, Mr. Záhonyi will engage in academic project work and collaborative research with both our Cyber Safety research team and our Cyber Resilience for SMEs research team. This placement will provide him with valuable insights into the ongoing research and innovation in Ireland on these topics, while also fostering international knowledge exchange and collaboration.

We look forward to welcoming Mr. Záhonyi to MTU and supporting his contribution to our research community.

Best regards,

Dr Hazel Murray
Chair of Cybersecurity
Munster Technological University

KÖSZÖNETNYILVÁNÍTÁS

Ezúton fejezem ki hálámat és köszönetemet mindazoknak, akik szakmailag és emberileg is támogattak a disszertáció elkészítése során. Mindenekelőtt hálás vagyok Dr. Szűcs Endre témavezetőmnek, aki szakmai iránymutatásával, türelmével és építő kritikáival végig kísérte munkámat és hozzájárult ahhoz, hogy kutatásom tudományos keretek között teljesedhessen ki. Kiemelt hálával gondolok családomra, különösen feleségemre, aki türelemmel és megértéssel segített átlendülni a legnehezebb időszakokon és támogató jelenlétével biztos hátteret nyújtott e hosszú folyamatban. Köszönöm az újpesti 1918. sz. Xántus János Cserkészcsapat tagjainak, akik közösségi értékeikkel példát mutattak és gondolataikkal hozzájárultak a gyermekek világának mélyebb megértéséhez. Köszönettel tartozom Márk Attila Olivér szakmai igazgatóhelyettes úrnak, az Észak-Budapesti Tankerületi Központból, aki intézményi oldalról támogatást és együttműködést biztosított számomra a kutatás előkészítése és lebonyolítása során. Hálás vagyok valamennyi interjúalanyomnak, akik időt és bizalmat szántak arra, hogy megosszák tapasztalataikat és ezzel értékes empirikus alapot szolgáltattak kutatásomhoz. Köszönöm az Óbudai Egyetem könyvtárosainak segítségét, akik tanulmányaim során készséggel biztosították számomra a könyvtári és online forrásokhoz való hozzáférést. Külön köszönettel tartozom Széll Gábor könyvtáros kollégának, aki időt és energiát szakított arra, hogy támogassa a disszertáció stilisztikai átnézését és formálását. Köszönöm az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Biztonságtudományi Doktori Iskola titkárságán dolgozó Lévay Katalin és Hronyecz Erika segítségét, akik minden adminisztratív kérdésben készséggel és szakértelemmel támogatták tanulmányaim előrehaladását. Külön köszönettel tartozom Dr. Hazel Murraynek, az írországi Munster Műszaki Egyetem (MTU – Munster Technological University, Cork, Ireland) tanszékvezetőjének, valamint a „Cyber Safety for Vulnerable Populations” projekt munkatársainak, akik lehetővé tették számomra, hogy kutatómunkám utolsó szakaszában értékes nemzetközi kutatási tapasztalatokat szerezzek.

Mindannyiuk hozzájárulása pótolhatatlan és e munka nem jöhetett volna létre nélkülük.