ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉSTERVEZET

CSERCSA KLAUDIA,

Alfa és Z generáció kiberbiztonsági-tudatosítási oktatásának vizsgálata

Témavezető: Prof. Dr. Rajnai Zoltán

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2025.12.03.

TARTALOMJEGYZÉK

BEVEZETÉS

A HOLNAP SZAKEMBEREIT A MA OKTATÁSA BIZTOSÍTJA

A szélessávú, gyors internetszolgáltatások, az okoseszközök könnyedén elérhetővé tétele, illetve a világon szinte mindenhol elérhető lakossági internet használat következtében újabb és újabb veszélyforrások jelennek meg az adathalászat területén. Az Alfa és Z generáció tagjai kiemelten hajlamosak az azonnali reagálás irányába mozdulni és ennek következtében nagy kockázatnak vannak kitéve kiberbiztonsági szempontból. A személyes adatok védelme érdekében egyre több biztonságot fokozó lépés történt az Európai Unióban, [1] erre vonatkozóan az ENISA (European Union Agency For Cybersecurity, Európai Uniós Kiberbiztonsági Ügynökség) egy tanulmányt is megjelentetett, amelyben értékeli az egyes tagállamok kiberbiztonsági oktatási szintjét és átfogó képet ad az EU-ról. [2] Továbbá ajánlásokat és bevált gyakorlatokat is gyűjt és megoszt egyes országok között az EU tagállamok között. [3] Bevezetésre került a kétfaktoros azonosítás, illetve a GDPR alkalmazása melyek megjelenésével jelentősen megnőtt a kiberbiztonsági szint. Azonban ezek ellenére is nő a bűnelkövetések száma. Ennek kiemelkedően magas része az alacsony biztonságtudatossági szintből ered. Adatainkhoz különféle módszerekkel jutnak hozzá a bűnelkövetők. A kiberbiztonsági rendszerek legkritikusabb láncszeme az emberi tényező. [4] Éppen ezért a megfelelő edukálás már kisgyermekkortól kezdődően elengedhetetlenül fontos. [5]

Magam is több éves oktatói múlttal rendelkezem. Egyetemi és gimnáziumi Z generációs fiatalokkal dolgozom már több éve. Digitális alkalmazások tárgyat is oktattam több éven át. Ennek köszönhetően személyes tapasztalatra tettem szert a kiberbiztonság oktatásának hiányosságaival kapcsolatban. További személyes tapasztalatomhoz járult hozzá, hogy Z generációba tartozó kamasz gyermek édesanyja vagyok. Ezeknek a tapasztalatoknak köszönhetően fedeztem fel azt az űrt, amely a közoktatásban tátong a kiberbiztonság oktatásában. Az életünket egyre inkább az online világ határozza meg. Az életünk jelentős szegmensében jelen van az internet, a digitális eszközök használata és ezzel párhuzamosan a kiberbiztonság kérdése.

A generációk közötti különbségeket és hasonlóságokat évek óta teszem különböző kutatásaim tárgyává. A Z generáció nemzedéke — a mai fiatal felnőttek és kései tinédzserek — az első olyan társadalmi csoport, akik már a digitális világ jólétébe születtek bele. A Z és az utána érkező Alfa generáció nemzedéke elképzelni is csak nehezen tudja, hogy milyen az, amikor nem volt távirányító a televíziókészülékekhez, nem volt telefon minden háztartásban és nem voltak személyi számítógépek az otthonokban. Értelmükkel felfogják, de számukra ez egy ugyanolyan történelmi frázis, mint az, hogy egykor királyok uralkodtak. Nem tapasztalták meg annak az életformának a nehézségeit.

Én az Y generáció eleje X generáció vége felé születtem, kutatásoktól függően tartozom egyik vagy másik generációba. Amikor én születtem még nem volt távirányító, mobiltelefon, mosogatógép, automata mosógép a háztartásokban, a személyi számítógépek használatáról pedig még elképzelése sem volt az akkori korszakban élő hétköznapi embereknek. Amikor 8-9 éves voltam, akkor vettünk egy Commodore 64-et, ami igencsak ritkaság volt akkoriban és az egész iskolában rajtunk kívül egyetlen családnak volt számítógépe az otthonában.

1. ábra Commodore 64 személyi számítógép [Digitalhungary.hu]

A telefonfülkéhez le kellett sétálni, ha telefonálni akart valaki, és nem tudtuk felhívni a távoli rokonokat az otthonukban. A velem egykorúak még egy ilyen korba születtek bele.

A szüleim fiatalkorában pedig még számomra is elképzelhetetlen életforma volt az általánosan elterjedt, pl. nem minden háztartásban volt meleg víz bevezetve vagy angol vécé. Miért fontos ez a kutatásom szempontjából és miért ezzel kezdem? Mert egy olyan turbulens technikai ugrás történt az elmúlt 50-70 évben, amilyenre a történelem során eddig még sosem volt példa. Ezen okokra vezethető vissza az a szakadék, amely a tapasztalat hiányából ered az Alfa és Z, illetve az őket megelőző generációk szülöttei között.

A személyi számítógépek először csak a háztartásokban tűntek fel, majd az egyre kisebb és gyorsabb okoseszközök elterjedésének köszönhetően már minden egyes személynek ott lapul a zsebében egy szuper intelligens miniszámítógép, aminek segítségével megszűntek az országhatárokon belüli ismerkedések, a lokalizációt szinte teljes mértékben felváltotta a globalizáció minden előnyével és hátrányával együtt. Már ugyanazok a franchise cégek árulják termékeiket Magyarországon, mint a világ másik pontján. Ez nagy hatással bír a divatra, a trendekre, a nyelvezetre és az elvárásokra.

A fiatalabb nemzedék tagjainak számára egy teljesen új digitális eszköz alkalmazása, egy addig számukra teljesen ismeretlen platform gond nélküli, rutinszerű használata nem okoz nehézséget, mivel egy olyan korban születtek, amikor már baba koruktól kezdve volt lehetőségük arra, hogy okoseszközökkel a kezükben nőjenek fel. Számukra a különböző okoseszközök használata már magától értetődő és autodidakta módon valósult meg, ellentétben a korábban született nemzedékek tagjaival, akik még keményen megdolgoztak ezért a tudásért.

A Z generáció az online világ nyújtotta előnyöket leginkább szórakozásra, valamint egymás közötti kommunikálásra használja. A jelszavak megfelelő alkalmazásáról, a nyílt hálózatok veszélyeiről, az adataik nagyfokú védelméről nem kapnak releváns és egzakt tájékoztatást megfelelő intézményi keretek között. A kibertámadási incidensek döntő többsége emberi tényezők miatt következik be. Ezért is annyira fontos a megfelelő edukáció intézményesített keretek között már óvodáskortól kezdődően.

A most a felnőttkor küszöbén álló fiatalok potenciális veszélynek vannak kitéve kiberbiztonsági szempontból. Ők azok, akik most kezdenek el napi szinten önálló vásárlásokat, banki tevékenységeket folytatni. A központi kérdés, hogy mennyire sikerült felvértezni ezeket a gyermekből felnőtté érő fiatalokat a csalások és megtévesztések fondorlatos közegével szemben.

A tudományos probléma megfogalmazása

A Z generációtól kezdődően (körülbelül 1995 után született fiatalok) szinte minden kisgyermeknek lehetősége van valamilyen okoseszköz használatára. Gyakori, hogy már az egy éves kor alatti gyermekek is naponta több órán keresztül vannak jelen az online térben. A túlterhelt szülők digitális dadaként alkalmazzák ezeket a termékeket. A kisgyerekek éveken át használják a digitális világ nyújtotta élvezeteket. Naponta több órán át az online térben játszanak, de nincs semmilyen kontroll vagy iránymutatás intézményesített szinten. Kizárólag a gyermeket körülvevő felnőtteken múlik, hogy a gyermek találkozik-e bármilyen formában a kiberbiztonság fontosságával, alapvető óvintézkedések ismertetésével, minimális szabályok bevezetésével. A szülőknek sok esetben sejtelmük sincs arról, hogy milyen weboldalakat látogatnak a gyerekeik.

A problémát tovább fokozza, hogy sok esetben maguk a felnőttek sem rendelkeznek megfelelő vagy elégséges információval az online térben fellelhető veszélyforrásokkal, illetve egy nem kívánatos incidens vagy kibertámadás utáni teendőkkel kapcsolatban. A gyerekek 3 éves koruktól kezdődően kötelező az óvodába járás Magyarországon.

A Nemzeti Alaptanterv nem követi a turbulens infokommunikációs fejlődést, nincs elég szó a vírusokról az app letöltésekről, a biztonságos online jelenlétről, a fake oldalakról, a csaló eladókról, a megtévesztésekről, az internetes zaklatókról, a biztonságos online vásárlásról, banki tevékenységről. Óvodáskorban és alsó tagozatban nincs intézményesített keretek között digitális eszközhasználattal kapcsolatosan bármilyen nemű oktatás. Ez azt jelenti, hogy (jobb esetben „csak") 3 éves korától körülbelül 12 éves koráig használja a gyermek a digitális eszközt mindenféle hivatalos oktatás vagy felvilágosítás nélkül. Ezen idő alatt több tízezer órát tölt el az online világban. Éppen ez a korosztály van a legnagyobb veszélynek kitéve. Az ilyen kicsi korosztályba tartozó gyerekek még könnyen becsaphatóak, kihasználhatóak. Az ingyenes játékok letöltése közben hatványozottan vannak kitéve a különféle veszélyeknek.

Az ötödikes tananyagban sem kap a kiberbiztonság oktatása külön szerepet, ez már a szakos tanár kompetenciájára van bízva, hogy a Nemzeti Alaptantervben megadott nagyobb témakörökön belül hajlandó-e és ha igen, milyen mélységben oktatni a kibertérben fennálló potenciális veszélyekről.

Az is egy létező jelenség, hogy gyakran a gyerekek jobban eligazodnak a digitális életben, mint a náluk jóval idősebb tanáraik. A kibertámadások olyan turbulensen változnak, olyan sokfélék lehetnek, hogy egy informatika tanárnak nagy kihívást jelenthet naprakésznek maradni az adott témában és erre gyakran nincs elég erőforrása és/vagy lehetősége az amúgy is túlterhelt tanároknak, oktatóknak. Az ehhez szorosan kapcsolódó nehézség, hogy az informatika tanár egy hiányszakma. Aki ennek a pozíciónak a betöltéséhez megfelelő képesítést szerez, az sokkal kecsegtetőbb feltételekkel bíró állásajánlatot kap, mint egy pedagógus általában. További nehézség, hogy a dinamikus technikai fejlődésnek köszönhetően nincsen naprakész tananyag, amit a diákok használni tudnának és ez a tanárok munkáját is nehezíti. A tanároknak kell az újabb digitális trendekkel és platformokkal kapcsolatban tájékozódniuk, központi iránymutatás és tanítási segédletek nélkül. Ez nagyon sok plusz munkaórát jelent egy közismereti tárgyat oktató kollégájához képest.

Azok a szerencsés fiatalok, akiknek a szüleik, illetve az őket körülvevő felnőttek tudnak és hajlandóak is beszélgetni a gyerekeikkel a kiberbiztonság témájáról nagy előnyre tesznek szert a nem megfelelően (vagy egyáltalán nem) informált társaikhoz képest. Ez nagy szakadékot képez az Alfa és Z generáción belül a digitális tudatosság és műveltség tekintetében.

A mostani fiatalok azonnal reagálnak és kellő óvatosság nélkül kattintanak rá linkekre és töltenek le felelőtlenül tartalmakat. A közoktatásnak nagy szerepe van (lenne) abban, hogy a gyors és meggondolatlan kattintás helyett legyenek kellően körültekintőek és elővigyázatosak az online térben. Amíg nincs a tanmenetbe integráltan szó arról, hogy mire kell figyelniük, mik az óvva intő jelek, addig nem is várhatjuk el, hogy ezzel a fajta tudással rendelkezzenek. Honnan is kellene tudniuk, ha nincs egy, a kiberbiztonság témájában kompetens felnőtt, akihez fordulhatnának.

A naprakész és bármikor elérhető tananyag éppolyan fontos lenne, mint az intézményesített oktatás bevezetése. A tananyag lehetne digitális (elearning) vagy nyomtatott tankönyvi verzió is, a lényeg, hogy jól strukturált legyen, tartalmazzon minden fontos és releváns információt a kiberbiztonság témájában, amire egy hétköznapi felhasználónak szüksége lehet és tartalmazzon egy külön fejezetet, amiben egy esetleges kibertámadás során felmerülő komplex probléma kapcsán megoldási lehetőségeket vázol

fel, illetve elérhetőségeket, mikor kihez lehet és kihez kell kötelezően fordulni egy kibertámadás során, például a bankot, a hatóságot értesíteni satöbbi.

A mai gyerekek és fiatalok azok, akiknek a kezében van a jövőnk. A rájuk fordított idő, energia fogja meghatározni azt, hogy milyen lesz az országunk, nemzetünk és jövőnk. Ha nem fordítunk kellő figyelmet a gyermekek kiberbiztonsági szempontból történő edukálására, akkor szenzitív adataink könnyen kerülhetnek rossz kezekbe és akár az egész országunk kritikus infrastruktúrája (így az energiaellátásunk, ivóvíz készletünk, légi és szárazföldi közlekedésünk, közbiztonságunk, energiaellátásunk, egészségügyi szektorunk, élelmiszer ellátásunk) és így az életünk is közvetlen veszélybe kerülhet. A holnap szakembereit a ma oktatása biztosítja.

A kiberbiztonság digitális korszakunk egyik legkiemelkedőbb területe és ennek ellenére a közoktatásban szinte semmilyen teret nem kap. A cél az lenne, hogy a gimnazista korosztály már önállóan tudja képezni magát, ismerje a fontos weboldalakat, elérhetőségeket az adott témában és önállóan is tudja naprakészen tartani a tudását a biztonságos digitális jelenlét során, illetve legyen információja arról, hogy hová, kihez fordulhat egy esetleges kibertámadást követően.

A gimnazista évek közepe, legkésőbb vége felé már majdnem minden fiatalkorú önálló gazdasági tevékenységet folytat napi, heti vagy havi rendszerességgel. Ennyi idős korra ideális esetben már rendelkezniük kellene azzal a tudással, ami a biztonságos online vásárláshoz, hétköznapi banki műveletek végrehajtásához szükséges. Ha csak ennyi idősen kezdenek el a témával érdemben foglalkozni, már nagy a valószínűsége annak, hogy kibertámadás vagy csalás áldozatává válnak.

Célkitűzés(ek)

Kutatásomban szeretném megvizsgálni a korábbi fejezetben felvázolt problémafelvetés kapcsán, hogy az Alfa és Z generáció, vagyis a mostani 30 éves és tőlük fiatalabb korosztályba tartozó fiatalok részesültek-e érdemben bármilyen kiberbiztonsággal kapcsolatos oktatásban az iskolában, tanórai keretek között, akár tanmenetbe integráltan, akár csak pár szó erejéig. Volt-e szó a kiberbiztonság fontosságáról, a megfelelően körültekintő digitális eszközhasználatról, megfelelő erősségű jelszavak alkalmazásáról, a megfelelő gyakorisággal történő jelszó cseréről, a kétlépcsős azonosításról, a jelszavak biztonságos tárolásáról és kiadásáról, a felelősségteljes eszközhasználatról, a körültekintő netbanki alkalmazások használatáról vagy a biztonságos online vásárlásról az eddigi oktatásuk során. A kvantitatív kutatásban a vizsgált időintervallumot leszűkítettem az utolsó 5 évre figyelembe véve a turbulens változásokat.

Az előző kérdéshez szorosan kapcsolódva, arra is választ kerestem, hogy kaptak-e bármilyen tananyagot a kiberbiztonsággal kapcsolatosan az elmúlt tanéveik során. Akár online, akár tankönyv formájában. A tananyag biztosítása hangsúlyt fektet egy tantárgy vagy témakör fontosságára, továbbá az a tananyag, amit leírva is látunk, mélyebben bevéső dik a hosszútávú memóriánkba. Továbbá bármikor újra fellapozhatunk egy írott tananyagot, ha kezünk ügyébe kerül, vagy ha kiberbiztonsági incidens ér, hasznos lehet egy jól felépített tananyag, külön fejezetbe foglalva egy esetleges kibertámadás utáni teendőkkel kapcsolatban.

Szeretném továbbá megvizsgálni azt is, hogy az Alfa és Z generáció mennyire tudatos az online vásárlásaik során. Tudják-e és alkalmazzák-e a megfelelő vagy legalább minimális biztonsági óvintézkedéseket? Tudják-e mire figyeljenek a biztonságos online vásárlásaik során? (Biztonságos fizetés, kétlépcsős azonosítás, fake oldalak felismerése, kamu eladók valószínűsíthetősége, az eladás során feltűntetett képeknek nem megfelelő minőségű termékek vásárlásának esélyének kiszűrése, illetve a lehetséges probléma megoldásokkal tisztában vannak-e. Ezeknek a kérdéseknek a megválaszolására kerestem a választ kutatásom során.

Hipotézisek

A kutatási célokhoz kapcsolódóan a következő 2 hipotézist fogalmaztam meg:

H1: Feltételezem, hogy a magyar közoktatás nem fordít elegendő figyelmet a kiberbiztonság témájára

H2: Feltételezem, hogy a magyar közoktatásban nincs megfelelően felépített, naprakész tananyag kiberbiztonság témájában

Kutatási módszerek

A kutatási kérdések megválaszolásához, a teljesség igényére törekedve kvalitatív és kvantitatív vizsgálatot is folytattam. Oktatói és tanulói (hallgatói) aspektusból is megközelítettem a kiberbiztonság oktatását és az ahhoz kapcsolatosan elérhető tananyagok vizsgálatát.

- Kvalitatív kutatás: Több éves (esetlegesen több évtizedes) tapasztalattal rendelkező digitális oktatást tanító szakoktatókkal készítettem mélyinterjút, melynek során tölcsér módszert alkalmaztam, ahol a kezdeti általánosabb kérdéseket követően, kifejezetten csak a kiberbiztonság oktatásával kapcsolatosan kérdeztem interjúalanyaimat.

Másrészt tanulókkal készítettem fókuszcsoportos vizsgálatot, melynek keretén belül „kötetlenebb" beszélgetés során kérdezgettem egyszerre több tanulót (általában 8-10 tanulót egyszerre) a kiberbiztonság oktatásával és az ezzel kapcsolatban elérhető tananyaggal kapcsolatos tapasztalataikról. 3 alkalommal készítettem fókuszcsoportos gondolatébresztő interjút, ahol körvonalazódott bennem a témával kapcsolatosan egy általánosabb összkép, amire alapoztam a sztrenderdizált kérdőív konkrét kérdéseit.

- Kvantitatív kutatás: Kérdőíves felmérést készítettem, hólabda mintavételi eljárással. A kérdőívet az interneten osztottam meg több alkalommal, különböző platformokon, az utolsó kiküldés időpontja 2025. augusztus. A kitöltés teljesen anonim módon, önkitöltéssel történt. A kérdőívet 6 szakaszra osztottam és szűrőkérdésekkel irányítottam a válaszadási lehetőségeket. A kiberbiztonság oktatására vonatkozó kérdéseket csak az Alfa és Z generációba tartozók tudták megválaszolni.

A minta nem reprezentatív.

1 A DIGITÁLIS JELENLÉT JELLEMZŐI A KÜLÖNBÖZŐ GENERÁCIÓKBAN, ONLINE VESZÉLYFORRÁSOK ÉS ADATHALÁSZAT

1.1 Generációk definiálása

Nem tudunk meghúzni egy éles határvonalat az időben, amely egzakt módon elválasztaná egymástól a különböző generációk tagjait. A főbb jellemző tulajdonságok finoman árnyalódnak az idő múlásával. Többféle évszámot is alkalmaznak a kutatók az egyes generációk kezdetének és végének meghatározására. Bakewell, & Mitchell, 2003-ban megjelent kutatásában [6] az Y generációba tartozókat 1977-től kezdődően értelmezték. Howe, & Strauss, 2000-ben megjelent publikációjában [7] Millenium generációnak nevezik az Y generációt és 1982-től született személyeket számítják bele.

Kutatásaimban én az alábbi évszámokat tekintem mérvadónak az öt különböző generáció meghatározására:

- Baby Boomer 1946-1964

- X generáció 1966-1979

- Y generáció 1980-1994

- Z generáció 1990-2010

- Alfa generáció 2011-

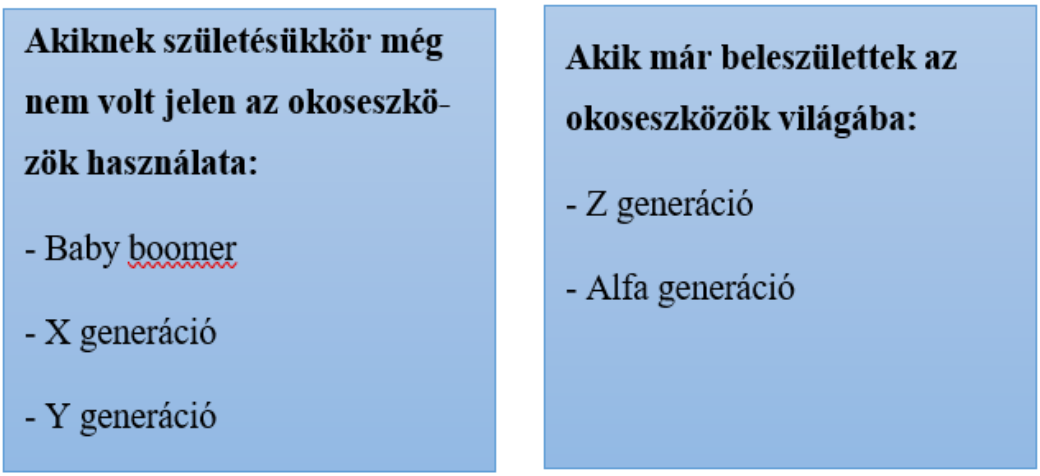
A különböző generációknál a születési évet tartjuk kiindulópontnak, vagyis egy adott kohorszhoz való tartozást. [8] A nevelés és környezet nagyon fontos meghatározó tényező a növekedés és fejlődés során. [9] Erre több kutató is felhívja a figyelmet, többek között Steigervald, akinek legfőbb kutatási területe a generáció kutatás, illetve Vekerdy, akinek számos publikációja jelent meg a gyermeknevelésről. [10] [11] Az életkor és a generáció között jelentős különbség van, erre hívja fel a figyelmet Steigervald a Mindent a generációkról című podcast-ben. Egy újszülöttnek az a normális, amibe beleszületik. A nevelés arról szól, hogy mit tanulunk a környezetünkről, hogy földi életünk első 1000 napjában mi volt a normális. Hogy milyen kiindulópontunk van, ezt hívjuk generációs origónak, ezek a születéskori élménytartományaink, és ez a generációs origó a jövőben hogyan fogja majd meghatározni a működésünket, az életünket. Ez különbözteti meg a gondolkodási sémáinkat. Erről szól a generációelmélet alapja. Egy generációba tartozók

életkora egészen nagy különbségeket mutat, 10-12 év korkülönbség is előfordul egy generáción belül. [12]

A generációs kohorszok elmélete szerint az egy generációba tartozó egyének politikai, gazdasági és történelmi, szempontból azonos eseményeket élnek át. [13] Ezektől a közösen átélt eseményektől alakulnak ki a kollektív élmények az adott generációkon belül és ezek alakítják ki az egymáshoz nagyon hasonló értékeket és életstílust, [14] illetve magatartási mintákat. [15]

Több szakirodalmi kutatás is foglalkozott már a különböző generációkkal, [16] amelyekben megállapításra kerültek a generációk attitűdjében lévő különbségek [17], különös tekintettel többek között a motivációjukra, [18] a munkavégzésükre és a konfliktuskezelésükre is. [19] [20]

A teljesség igényére törekedve röviden bemutatom az öt generáció szülötteinek főbb jellemzőit. A bemutatás során 2 csoportra bontottam a generációkat az alapján, hogy kik azok, akik már a digitális korba születtek bele (Alfa és Z generáció), illetve az őket megelőző, idősebb korosztályt tekintettem egy másik csoportnak, akiknek még nem voltak jelen az okoseszközök használata a mindennapokban születésük időpontjában. Kutatásomnak fontos aspektusa ez a különbség az általam alkotott két csoport között. A továbbiakban ezt a két csoportot külön alfejezetben tárgyalom.



2. ábra Generációk csoportosítása [Saját szerkesztés]

Baby boomer, X generáció, Y generáció jellemzőinek bemutatása

- A Baby Boom generáció tagjai 1946 és 1964 között születtek. [21] Lojális munkavállalók és kifejezetten csapat orientáltak. Nevük onnan ered, hogy ebben az időszakban (a második világháború befejezése után), jelentősen megnőtt a születések száma az Egyesült Államokban és Európában és erre utal a baba-robban kifejezés. Optimista attitűd és szorgalom jellemzi őket. [22] E generáció megtapasztalta az előnyeit és hátrányait is a háborúnak és a civil jogi mozgalmaknak. [18] Az Amerikai Egyesült Államokban nagy hatást gyakorolt rájuk a vietnámi háború, a szexuális forradalom és a Kennedy gyilkosság. [23] Fő jellemzőik közé tartozik, hogy erősen van jelen náluk a stabilitásra és a biztonságra való törekvés, hiszen a szüleik átélték a második világháború borzalmait. Fontos számukra a stabil munkahely és a kiszámítható, rendszeres jövedelem. Ennek érdekében keményen dolgoznak, hitvallásuk, hogy a siker szorgalommal és munkával érhető el. Kifejezetten lojálisak, gyakran hosszú évtizedeken át dolgoznak egy vállalatnál. Előnyben részesítik a személyes kontaktuson alapuló kapcsolatokat, kevésbé a digitális világ fogjai, ugyanakkor sikeresen adaptálták a technológiai innovációkat. Hosszú időn át ők alkották a vezetői réteget, ma már azonban többségük nyugdíjban van, vagy nyugdíj mellett dolgoznak.

- Az X generáció tagjai 1966-1979 között születtek. Ebben az időszakban terjedt el a nők munkavállalása és emiatt a nők otthoni szerepe jelentősen csökkent, emiatt a gyerekek gyakran voltak szüleik nélkül és gondoskodniuk kellett magukról, így alakult ki az önálló és alkalmazkodóképes jelleg, mely erősen jellemzi ezt a generációt és „kulcsos gyerekek” generációjaként is szokták emlegetni őket utalva arra, hogy amikor hazaértek az iskolából, nem várták őket otthon a szüleik, mert dolgoztak. Emlegetik őket digitális bevándorlóként is. [24] Még analóg világban nőttek fel, de felnőttként már a mindennapjaik része lett a számítógép, mobiltelefon, internet használata. A korábbi generációkhoz képest nagyobb valószínűséggel hagyják el a munkaadót magasabb fizetés vagy kedvezőbb feltételek reményében. [25] Már kevésbé munka orientáltak, mint elődeik, számukra fontos a szabadidő és a család. Munkavégzésüket az eredményközpontúság és a szkepticizmus jellemzi. Átéltek forradalmakat és hidegháborúkat, gazdasági válságokat, rendszerváltásokat, ezért jellemzőbb rájuk a bizalmatlanság az intézményekkel szemben. Fontos ennek a generációnak a visszacsatolás iránti vágy. [26] Ők a híd a hagyományos ipari korszak és a digitális korszak között.

- Az Y generáció tagjai 1980-1994 között születtek. Sok féle elnevezéssel találkozhatunk: ezredfordulós, bumeráng generáció (újra hazatérnek az iskolák elvégzése után), „kulcsos gyerekek" (utalva arra, hogy iskola után ők érnek haza először és náluk van a lakás kulcsa, amit gyakran a nyakukba akasztva hordtak), Peter Pan generáció (hosszabb idő alatt nőnek fel), millennium generáció, digitális bevándorlók. [27] Ez a nemzedék az, amelyik együtt nőtt fel a digitális technológiával. [28] A rendkívül gyors technológiai fejlődés az Y generáció születését követően indult útnak. Ők azok, akiknek az internet és a számítástechnika életük természetes velejárója. [29]

Tari Annamária [28] az Y generációról megállapítja, hogy számukra a technikai eszközökön keresztül való érintkezés az emberi kommunikáció természetes formája. Az Y-generáció tagjai egyszerre élnek a virtuális és a valós létben. A számítástechnika világának megfelelő ritmusban up to date jelleggel a munkájukban is azonnali visszajelzést követelnek. Tudásuk a digitális világról nagyobb, mint a szüleiké, a tanáraiké. Ez a generáció az első fordított szocializációs generáció. Tudásuk egy részét természetesen elődeiktől szerzik, de – ellentétben az előző generációkkal – igen nagy szerepet kap az egymástól, kortársaiktól, sőt gyermekeiktől szerzett tudás is. Életük nagy részét a világháló segítségével élik és tudásszerzésük, szabad idő eltöltésük, kapcsolatépítésük elsődlegesen az online térben valósul meg. A társadalom és a piac globalizációja óriási hatással volt az értékrendjükre. [7]

A generációval kapcsolatos általános sztereotípiák közé tartozik, hogy bizalmatlanok a szervezetekkel szemben, erős a munka iránti vágyuk, az egész életen át tartó tanulást kiemelt prioritásként kezelik és a családot a boldogulás kulcsaként fogják fel. Fontos számukra a siker, amit a munka jelentőségével mérnek. [29] Alapvető fontosságú számukra a karrier, a siker és a pénz. Nem jellemző rájuk a munka világában az előző generációkról elmondható engedelmesség, alázat; inkább az öntörvényűség, a lojalitás csökkenése figyelhető meg a korosztály tagjainál. Ha nem felel meg számukra egy munkahely, gond és habozás nélkül újat keresnek, tovább állnak. Ez a nemzedék abban a korban nőtt fel, amikor megjelent a terrorizmus, újabb válságok ütötték fel fejüket és a szegénységről és a hajléktalanná válásról (ami korábban nem ismert fogalom volt) szóltak a napi híradások. Látták a szüleik hétköznapi küzdelmeit, a taposómalmot és nem szeretnének ilyen életet élni. Ugyanakkor vágynak a biztonságra, amelynek eléréséhez azonban keménynek és határozottnak kell lenni. Keresik a csoporthoz való tartozás élményét, mert ez adja számukra a biztonság érzését. [24]

Alfa és Z generáció jellemzőinek bemutatása

A Z generáció tagjai 1995-2010 között születtek. A Z generáció a világ első globális nemzedéke. A születésük idején a digitalizáció már olyan mértékben elterjedt, hogy minden családban általánosan elterjedt volt az okoseszközök használata. Számukra már teljesen hétköznapi volt a folyamatosan elérhető online jelenlét. Úgy is jellemezi őket a szakirodalom, mint Facebook-generáció, digitális generáció, digitális bennszülöttek vagy iGeneráció. [30] Ők már a technológia világába születtek és számukra fontos, hogy ez a környezet vegye körül őket. Mindig online vannak bármilyen technikai eszközön virtuálisan, megállás nélkül. [31] Kutatások kimutatták, hogy a folyamatos online jelenlét hatással van a fiatalok önértékelésére, későbbi sikereikre, boldogságukra. [32]

Egyszerre több dolgot csinálnak és figyelmüket eszkalálják, így gyakori a figyelem-fókusz probléma, a szövegértési nehézség és a kitartó figyelemre való képesség. [33] Ők a digitális forradalom, a globális 2008-as világválság, a covid járvány és a klímaválság idejében nőttek fel. Kiemelendő a multitasking képességük. Egyszerre több információforrást kezelnek, tanulás közben csetelnek, videót néznek stb. Erős a vizuális kultúrájuk. A rajzolás a különböző digitális eszközökön nagyon elterjedt ebben a generációban, A képek, videók, mémek és rövid videós tartalmak fontosabbak és informatívabbak számukra, mint a hosszú szövegek olvasása és jellemző rájuk a szövegértési nehézség az írott szövegek olvasása során.

Gondolkodású értékalapú, fontos számukra a környezetvédelem, a sokszínűség, a társadalmi felelősségvállalás, az állatvédelem. Nem szeretik a merev hierarchikus rendszereket, inkább projekt alapú szemléletmód jellemzi őket. Fontos számukra az azonnali elismerés vagy reakció, amit a közösségi média használata során megszoktak a like-ok és kommentek formájában. A világ számukra már határokon átívelő, mondhatni határok nélküli, hiszen a nemzetközi trendek és kultúrák, az online játékoknak is köszönhető más nemzetekkel történő közösség alkotás (még ha csak egy online meccs vagy verseny erejéig is) a mindennapjaik része. Ennek köszönhetően az angol nyelv használata számukra már nem jelent akkora kihívást, mint szüleiknek.

Most lépnek be a munka világába. Fontos számukra a rugalmasság, a távoli munkavégzés lehetősége és a mentális egészség fenntartása. Jobban értékelik azokat a munkahelyeket, ahol a munkájukban értelmet is látnak, illetve értéket teremthetnek a munkájuk által. Fontos számukra, hogy legyen fejlődési és előrelépési lehetőség.

Kevésbé jellemző rájuk a lojalitás, mint a korábbi generációk szülötteire, inkább a fejlődés lehetőségét és az élményt keresik. Munka iránti attitűdük főbb jellemzői: gyakorlatiasak, gyorsan reagálnak, korukból is fakadóan nem elég bölcsek ugyanakkor szeretnek ők irányítani. Türelmetlenek, szükségük van új kihívásokra és impulzusokra. [34] Nem félnek az örökös változásoktól és az okoseszközeiknek köszönhetően rengeteg információval rendelkeznek. A problémák megoldására az internet segítségével találnak megoldásokat. [30] A karrier fontos számukra, technikai- és nyelvtudásuk magas szintű. Ezért kiváló munkaerőnek számítanak. Minden tényező közül számukra a legfontosabb a munka-magánélet egyensúly megteremtésének lehetősége. [35]

- Alfa generáció (2011 -) A ma született és születendő gyermekek, a XXI. század társadalmának és gazdaságának meghatározó szereplői, az informatikai forradalom teljes kibontakozásának időszakában élnek. Még nincsenek aktív, cselekvőképes társadalmi státuszban. Az ő életüket már nem csak az okoseszközök, de a mesterséges intelligencia társadalmi szintű, napi használata is jellemzi. Sokkal előbb tanulnak meg okoseszközöket kezelni, mint írni-olvasni. Születésük idején már társadalmilag elterjedtek az okosotthonok, a mesterséges intelligencia napi használata, a robotika, az 5G és a digitális oktatás. Az ő oktatásukban egyre nagyobb szerepet kap a gemifikáció a játékos digitális tartalmaknak köszönhetően. Már egészen baba koruktól az életük hétköznapi részévé vált a fenntartahatóság, a klímavédelem, a környezetvédelem és az egyenlőség kérdése. Számukra az önkifejezés része a különböző márkák használata és az online életük az identitásuk részévé vált. A legtöbb rájuk jellemző tulajdonságban megegyeznek a Z generáció tagjaival. [36] A Covid járvány hatására sokan online tanulással kezdték meg az iskolás éveiket. Ők lesznek az első teljesen AI-generáció a munka világában. Rugalmasságot, technológiai integrációt és folyamatos tanulás lehetőséget várnak el és ez feltehetően erősen jellemző lesz rájuk munkavállalóként is. Feltehetően életpályájuk során a lojalitás és a nem megfelelő körülmények tolerálása náluk tovább fog csökkeni a korábbi generációkhoz képest. Valószínűleg több rövidebb karriert és karrierváltást fognak megélni életük során és nem lesz jellemző rájuk az egyetlen vállalat irránti több évtizedes elköteleződöttség.

1.2 Az online térben fellelhető veszélyforrások, adathalászati módszerek

A fogalom bemutatását Kevin Mitnick szavaival szeretném kezdeni, aki napjaink egyik legendájának számít a kiberbiztonság történetében.

„A social engineer ugyanazokat a meggyőző technikákat alkalmazza, amiket mindannyian használunk a mindennapok során. Szerepeket veszünk fel. Hitelességet próbálunk megteremteni. Viszonzandó szívességeket teszünk. A social engineer azonban manipuláló és megtévesztő, nagyon etikátlan módon alkalmazza e technikákat – és gyakran elsöprő sikereket ér el velük.” [37, p. 267]

„Bár magától értetődőnek tűnik, hogy a pénzügyi bűncselekmények indítéka az anyagi haszonszerzés, ez mégsem tekinthető kizárólagos motivációnak. Számos esetben derült ki ugyanis, hogy az elkövetők egy részét nem a haszonszerzés, hanem a szakmai kíváncsiság és kalandvágy, vagy valamilyen sérelem megtorlására, illetőleg személyes bosszúra irányuló vágy hajtotta tetteiknek az elkövetésében. Emellett egyes államok államérdekből, terrorista szervezetek és bűnszervezetek pedig politikai célok érdekében indítanak kibertámadást a védett infrastruktúrák – közük a pénzügyi szektor – ellen.” [38, p. 19]

Kevin Mitnick [39] az egyik legjobb példa erre, aki az amerikai FBI egyik legkeresettebb ifjú bűnelkövetője volt az 1980-as években. [40] Több nagyvállalat informatikai rendszerébe hatolt be illetéktelenül, anyagi, illetve bármilyen egyéb haszonszerzési cél nélkül. Kizárólag az izgalom, a hecc kedvéért. [41] Az ifjú kiberbűnöző, büntetőjogi felelősségre vonása után, 2023. júliusban bekövetkezett haláláig harcolt a kiberbiztonság megerősítése érdekében. [42]

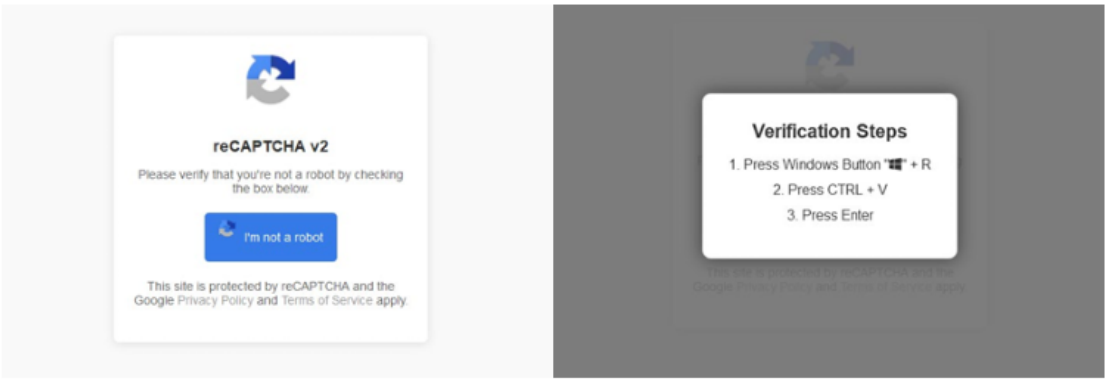
Munkássága sokat hozzátett az online tér biztonságosabbá tételéhez. Sok hiányosságra és veszélyre hívta fel a közvélemény figyelmét a rablóból lett pandúr. Könyvében így határozza meg a social engineering fogalmát: „A social engineering a befolyásolás és a rábeszélés eszközével megtéveszti az embereket, manipulálja, vagy meggyőzi őket, hogy a social engineer (adathalász) tényleg az, akinek mondja magát. Ennek eredményeként a social engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni.” [37, p. 59]

A social engineering magyar megfelelője pszichológiai manipuláció vagy pszichológiai befolyásolás. Ezen támadások ellen elsősorban nem technikai eszközök alkalmazásával kell védekezni, hanem a felhasználói ismeretek széles körben kiterjesztett oktatása és ismeretnövelése által. Ezekben az incidensekben nagy hangsúly van az emberi természet megismerésén, az emberek megtévesztésén és nem a technológiai eszközök sebezhetőségét használja ki a támadó. A módszer lényege, hogy több esetben egy bizalmi viszony alakul ki az elkövető és az áldozat között, mely során értékes információkat nyer meg a támadó és ezt saját érdekére fordítja és kihasználja az áldozat óvatlanságát, jóhiszeműségét. Más helyzetben pedig a célszemély vagy inkább kiszemelt áldozat figyelmetlenségéből fakadhat a károkozás.

2025. júliusában Richard Bilton tudósított a BBC hírcsatorna közreműködésével egy hírt, miszerint hacker támadás következtében ment csődbe Northamptonshire-ben egy 158 éves múltra visszatekintő cég, aminek következtében 700 ember vált munkanélkülivé. Feltételezhetően egy céges alkalmazottnak törték fel a nem megfelelő erősségű jelszavát és fértek hozzá a cég adataihoz, majd ezeket titkosították, zárolták és olyan magas összegű váltságdíjat követeltek, melyet a cég nem tudott megfizetni, így végül csődöt mondott. [43] Az esetről Magyarországon a HVG.HU is beszámolt. [44] Bilton további példával is szolgál, ami tavalyelőtt 2023-ban történt és 500 teherautót üzemeltető céggel. Ez a cég is elvesztette a hackerek által zárolt adatokat és csődbe ment. Iparági kutatások szerint az Egyesült Királyságban a váltságdíj átlagosan 4 millió font körüli összeg (középárfolyamon számítva ez hozzávetőlegesen 1.852.000.000 forint), amelyet a vállalatok nagyjából egyharmada képes kifizetni.

Béres Péter egy magyarországi cég IT-vezetője egy új típusú social engineering technikáról számol be az Economx.hu-n. [45] A technika lényege, hogy a weboldal küld egy üzenetet, amelyikben arra kéri a felhasználót, hogy bizonyítsa be, hogy nem robot. Ilyennel gyakran lehet találkozni, amikor meg kell jelölni a motort vagy lámpát tartalmazó képkockákat. Ehhez már hozzászokott a legtöbb felhasználó. Ezzel kapcsolatban az új feladat, amit nem kérdőjeleznek meg a gyanútlan felhasználók, hogy valamilyen tartalmat másoljanak ki és illesszenek be az eszközükön. És már le is töltötték a zsarolóvírust vagy egyéb kártevőt az általuk használt eszközre. Béres ugyanebben a cikkben kifejti, hogy az adatlopó kártevők terén is lényeges változásokat figyelhetünk meg. Van olyan adathalász program (SnakeStealer), amely a billentyűleütéseket naplózza, elmenti a hitelesítéssel kapcsolatos adatainkat, továbbá alkalmas a vágólap

tartalmának a mentésére is, ezáltal a képernyőképek és egyéb ctrl+c művelettel végzett tartalmaink hozzáférésére. Ez a vírus ClickFix néven is elterjedt a köztudatban [46] [47] [48] [49]



Hamis reCAPTCHA üzenet, amely arra utasítja az áldozatot, hogy illesszen be és hajtson végre egy rosszindulatú parancsot az eszközén.

3. ábra Hamis reCAPTCHA üzenet [Kurt.hu]

Több kiemelkedő színvonalú hazai kutatási eredmény is bizonyította információbiztonsági kockázatként az emberi tényezőt és a tudatos felhasználás alacsony szintjét. [50] [51]

Beke kutatásában az Oktatás 4.0 főbb pontjai között az élethosszig tartó tanulást és a digitális eszközök oktatásban történő megjelentetésére helyezi a hangsúlyt (egyebek mellett). [52] Ehhez elengedhetetlen feltétel a kiberbiztonságra vonatkozó oktatás és tananyagok megléte, digitális adataink védelme érdekében. [53]

A teljesség igényére és a könnyebb áttekinthetőségre törekedve, a továbbiakban 2 csoportra bontom az esetleges kibertámadások lehetséges elkövetésének módját és ezt a csoportot a következő 2 alfejezetben külön tárgyalom. Az egyik csoportba azok az adathalász technikák tartoznak, amelyekhez nem szükséges IT alapú tudás. Az adatok eltulajdonítása nem az online térben történik, mégis veszélyeztetik digitális adataink védelmét, segítségükkel betörnek személyes platformjainkra. A másik csoportban azokat az adathalászati technikákat mutatom be, amelyek kizárólag az online térben történnek és az elkövető rendelkezik mélyebb tudással a digitalizáció terén.

IT alapú tudást nem igénylő adathalász technikák

Ezek az adathalászati módszerek igen hétköznapiak és ezek a legveszélyesebbek az elkövetők szempontjából, hiszen ezekkel a módszerekkel a legnagyobb a lebukás veszélye. Jellegükből fakadóan többnyire fizikai jelenlétet is igénylő információ szerzésre irányuló technikák, de némelyik adathalász módszer elkövetése során csak a hangját használja a támadó. De ez is egy közvetlen kapcsolatot alakít ki a támadó és az áldozat között. Ezek a módszerek komoly felkészülést és lélekjelenlétet követelnek az alkalmazásuk során.

„Az alaptaktika egyszerű. Mielőtt egy adott cél érdekében a social engineeringhez folyamodnánk, fel kell deríteni a terepet. Össze kell szedni az információmorzsákat: miként működik egy osztály vagy szervezeti egység, mi a feladata, milyen infomációkhoz férnek hozzá az alkalmazottak, mi a kérelmek szokásos menete, …, milyen sajátos szakszavakat és nyelvezetet használ a cég.” [37, p. 27]

- Vishing (adathalászat telefonon keresztül): A csaló általában úgy tesz, mintha egy törvényes üzletkötő lenne, például nyereséges üzletet kínál és általában hitelkártya információt, esetleg más személyiség lopásra alkalmas információt igyekszik ezzel a módszerrel megszerezni.

„Saját trükk, és nagyon gyakran bejön. Ha bizalmas információkra kérdezünk rá, az emberek azonnal gyanakodni kezdenek. De ha úgy teszünk, mintha már a birtokában lennénk ennek az információnak és helytelenül adjuk meg nekik, akkor gyakran kijavítanak. Ezzel pedig megtudjuk, amire kíváncsiak voltunk.” [37, p. 39]

- Dumpster diving (Kuka búvárkodás): Az emberek gyakran értékes információt dobnak ki felelőtlenül a szemétbe. A támadó kereskedelmi vagy lakossági szemét tárolókban keresgél. Először információt gyűjt a kukák tárolásáról, elszállításáról majd a kuka tartalmát átvizsgálva kerül értékes információk birtokába, amelyek alapján a későbbiekben csalást vagy lopást tud elkövetni. A támadónak nincs más dolga, csak a megfelelő szemetesben keresgélni. Érdemes minden dokumentumot megfelelő körültekintéssel megsemmisíteni.

- Pretexting: Olyan támadásforma, amellyel a támadók nyílt forrásból vagy adathalászattal előzetesen felkészülnek az áldozatokkal kapcsolatos információkból és így próbálnak meg általában telefonon még több információhoz jutni.

- Eavesdropping (hallgatózás, a beszélgetések jogosulatlan lehallgatása): Ha két fél beszélgetését akár négyszemközt, akár telefonon illetéktelen harmadik személy lehallgatja, sokszor fontos adatokat gyűjthet. Ha számítógéppel történik a lehallgatás, akkor a támadó kihasználja a nem biztonságos hálózati kommunikáció hátrányait a küldött és fogadott adatok eléréséhez. Az ilyen támadásokat nehéz felismerni, mert a hálózati átvitelben nem okoznak rendellenes működést. Ha személy hallgatózik, akkor megpróbál elrejtőzni is. Bizalmas információk közlésénél fontos, hogy megfelelő környezetben, odafigyelve tegyünk.

- A shoulder surfing (váll feletti leskelődés): Kedvelt technikája a PIN-kód vagy jelszó megszerzésének. A támadó nem kerül közvetlen kapcsolatba az áldozattal, hanem a támadó közel kerül hozzá, elhelyezkedik mögötte, és az áldozat válla felett közvetlenül megfigyeli, amikor az a karaktereket leüti a billentyűzeten. Közben úgy tesz, mintha nem is nézne oda. A leggyakoribb esetek a PIN kódok, beléptető rendszerek, kaputelefonok kódjai, hívókártyák, hitelkártyaszámok stb. Gyakori a pénzkiadó automatáknál, hogy valamilyen szerkezet, távcső vagy kamera felhasználásával igyekeznek megszerezni a PIN kódot. A legegyszerűbb védekezés a leselkedők ellen, ha vigyázunk arra ki áll mögöttünk és a kódok bevitelekor eltakarjuk a konzolt. [54]

- Segítségkérés-segítségnyújtás: A támadó az emberek segítőkészségére támaszkodva csal ki információkat. A hibát maga a támadó is okozhatja, így ő teremti meg a helyzetet, ahol segítségét felajánlva szerez meg bizalmas információkat.

- Tailgating (besurranási módszer): Ezen technika alkalmazása során a támadó besurran egy épületbe. Ehhez használhat hamis beléptetőkártyát, megtéveszthetti a beléptetésért felelős személyeket vagy besurranhat egy belépésre jogosult személy mögött az automata ajtózáródásig. Értékes információkhoz juthat az irodákba való bejutás során, ahol számítógépekhez és nyomtatott dokumentumokhoz is hozzáférhet. [55]

- Jelszavak kitalálása: Itt kifejezetten a nem megfelelő erősségű jelszavak kitalálásáról van szó, ahol a támadó egyszerűen próbálkozik különböző jelszavak használatával. Gyakran a felhasználók megadják egymásnak a jelszavaikat, illetve mások által hozzáférhető helyen tárolják.

Ezeknek az adathalászati technikáknak az eredménye általában olyan információ, melyet a későbbiekben fel lehet használni más jellegű, technikai támadások kivitelezéséhez. Ezek az egyszerűnek tűnő technikák nem kívánnak IT alapú tudást, csupán rátermettséget

és bátorságot. A későbbiek folyamán azonban az ilyen jellegű támadások már jelentős kárt okozhatnak a felhasználóknak és a szervezetnek is. Ezért nagyon fontos a tudatos felhasználás és az odafigyelés a leghétköznapibbnak tűnő szituációkban is.

Az összes említett adathalász fajta, emberi manipulációt alkalmaz, ezért technikai intézkedésekkel nehéz ellenük védekezni. A leghatékonyabb védelem a tudatosság növelése és a hatékony adatvédelmi viselkedés kialakítása lehet.

IT alapú tudást igénylő adathalász technikák

Ezek közé tartoznak a valamilyen IT eszköz segítségével végrehajtott támadások, ahol rendszerint az elkövető nem is lép közvetlenül kapcsolatba az áldozatával és ebből fakadóan kisebb a lebukás veszélye. A támadók felkészültek és járatosak a szoftverek és IT eszközök használatában. Ezeknek a támadásoknak a kivédése már bizonyos fokú felhasználói tudást igényel, hiszen itt már az online lét világában történnek a különböző incidensek. [56]

- Phishing (adathalászat): Gyűjtőfogalom. A személyes adatokat azért gyűjtik, hogy visszaélést kövessenek el. Az egyik leggyakoribb elkövetési mód. Egyesek azt feltételezik, hogy a phishing szó a password harvesting fishing angol szavak összevonásából alakult ki, de sokan ezt megkérdőjelezik. Az ilyen fajta támadásokat tapasztalt bűnözők vezetik, gyakran egész bűnözői csoportok rejlenek mögöttük, vagy: akár egész államok is. A támadások legegyszerűbb módja az e-mail, amelyben a támadó különféle ürügyeket használ. Például: banki értesítésben tájékoztatják az ügyfelet, hogy valamely esemény kapcsán azonnali beavatkozásra van szükség, amelynek során szenzitív adatokat, személyazonosító információkat (hitelkártya számot vagy internetes banki hozzáférési kódokat) kérnek el. Az adathalász e-mailek gyakran olyan személyek e-mail címeiről érkeznek, akiket a felhasználó ismer, megbízik bennük és/vagy esetleg a munkahelyi felettese. Az ilyen fajta adathalász jellegű leveleket elküldik egyszerre több címzettnek, azzal az elvárással, hogy lesz valaki, aki azonnal reagál az üzenetre és megadja a személyes adatait. Az adathalászat célja érzékeny személyes (cím, születési idő, társadalombiztosítási szám, hitelkártya-adatok), vagy bejelentkezési adatok megszerzése az áldozat információs rendszereihez, rosszindulatú alkalmazások telepítése a számítógépre vagy mobiltelefonra.

Sikeres támadás után a támadó szinte bármilyen tevékenységet elvégezhet a számítógépen a felhasználó tudta nélkül. Például: a felhasználó fájljainak megsemmisítése vagy titkosítása, fizetés a felhasználó bankszámlájáról, rosszindulatú tevékenységek végrehajtása az áldozat IP-címéről (SPAM, behatolási kísérletek), vírusok terjesztése (az interneten és a helyi hálózaton keresztül). Jellemzői közé tartozik az általános megszólítás, a gyakori és/vagy súlyos helyesírási hibák előfordulása, tartozásra való felhívás, sürgetés, személyes adatok kiadására irányuló kérés.

- Whaling (bálnavadászat): Célzottan, cégvezetőkre („bálnákra") irányul. „A célzott támadás az internetről érkező fenyegetések körébe tartozik, amely során a támadó az elektronikus információs rendszer infrastrukturális szegmensét célozza annak érdekében, hogy e szegmensben felügyelet nélkül „tevékenykedjen". Ezen magatartás arra irányul, hogy a támadó az adott célpont eszköze feletti rendelkezési jogosultság gyakorlását megszerezze. Rendkívül összetett módszereket és magas szakértelmet igénylő támadási forma, amely ellen nehéz védekezni és így gyakran jár „eredménnyel". [37, p. 25]

A bálnavadászat során az adathalászok megtalálják a társaság legfontosabb ügyvezetőjének vagy vezetőjének nevét és e-mail címét, melyek legtöbb esetben szabadon hozzáférhetőek a cég weboldalán, és személyre szabottan e-mailt készítenek a társaságban betöltött szerepükre vonatkozóan. Az elefántok vérnyomása magas. Az email tartalma megpróbálja rávenni a vezetőket, hogy kattintsanak egy linkre, amely azután egy olyan webhelyre irányít, amelyről rosszindulatú szoftverek töltődnek le a gépükre, vagy vállalati titkokat is közzé tehetnek a hiszékeny vezetők.

- Spear phishing (szigonyozás vagy lándzsás adathalászat): Míg az „adathalász" tömeges e-mailt használ, a „szigonyos" célokat és nagyon kevés címzettet használ. Az email első ránézésre úgy tűnik, hogy megbízható forrásból, például banktól, a vállalat belső informatikai részlegétől, belső alkalmazottól vagy üzleti partnerétől származik. Az üzenet általában felhasználónevet és jelszót igényel, esetleg hivatkozást tartalmaz egy webhelyre, de egyéb kártékony mellékleteket is tartalmazhat.

- Baiting (elhagyott adathordozó): Az emberek kíváncsiságán alapszik. A támadó valamilyen hordozható adathordozót (CD, DVD, pendrive, memóriakártya) hagy egy jól látható helyen (célszerűen egy számítógép közelében). A hatékonyabb csalogatás érdekében gyakran egy figyelemfelkeltő felirattal is ellátják a csaliként bevetett eszközt pl.: „szexi képek", „bizalmas" stb. Az arra elhaladó személy azt gondolja, hogy találta.

A talált tárgyon azonban kártékony programok rejlenek, és amikor a gyanútlan áldozat az eszközt csatlakoztatja a számítógéphez, akkor bekövetkezik a fertőzés. De megtörténhet ez az online világban is. Az ingyen letölthető szoftverek esetében is előfordulhat, hogy letöltés után megfertőzik a számítógépet. Ezután a kártékony szoftverek információkat küldenek a felhasználók tevékenységeiről a támadóknak.

- Typosquatting (URL-eltérítés): Az eredeti weblappal első ránézésre teljesen megegyező, alternatív weboldalra irányítja a felhasználót. Az alternatív oldal grafikai dizájnja, első pillantásra nehezen különböztethető meg az érintett intézmények által használt eredetiktől. Az álweboldal webcíme többnyire egyetlen karakterrel különbözik az eredetileg felkeresni kívánt weboldal címétől és a legtöbb esetben a felhasználó észre sem veszi, hogy nem megfelelő helyen jár. Gyanútlanul megadja a hitelesítő adatait, amit a támadó ezután könnyedén felhasználhat. Kiváló magyar példa erre: legjobbank.hu vagy Iegjobbank.hu A különbség nehezen észrevehető. Az első karakter az egyiknél a kis „L” betű a másiknál a nagy „i”.

- Pharming (Farmolás, átirányítás hamisított weblapra): A támadó a felhasználót egy hamis, de a megbízhatóhoz nagyon hasonlító weboldalra irányítja. Az átirányítás általában valamilyen szoftver segítségével történik, többnyire nem is látszik különbség az eredeti és az álweboldal URL címében. A hacker az általa létrehozott hamis weboldal segítségével szerzi meg a felhasználótól a bizalmas információkat.

- SMiShing (SMS-alapú adathalászat): A támadó a mobiltelefonokon lévő szöveges üzeneteket (SMS: Short Message Service) használ arra, hogy megpróbálja rávenni az áldozatát, hogy elárulja személyes adatait vagy egy linket tartalmaz, amire, ha rákattint a felhasználó egy ártalmas weboldalra lesz irányítva. Ennek folyományaként kártékony program kerülhet telepítésre, vagy a támadó megszerezheti a felhasználó személyes akár banki adatait is. [57]

További social engineering adathalász formák és elnevezésük

- Search engine phishing: Egy rendkívül nagy kedvezményt nyújtó vásárlási lehetőséget kínáló weboldal, mely azonnali vásárlásra buzdít és azonnali klikkelésre szólítja fel a gyanútlan felhasználót. Ezek között szerepelhet egy szerencsekerék megforgatása klikkeléssel, melynek segítségével 90%-os vásárlás kedvezményt nyer az illető, ha néhány percen belül felhasználja a nyeremény kupont. És amint klikkel a felhasználó, máris a támadó által létrehozott weboldalon landol.

- Social data mining: A különböző social media felületeken, mint például a Facebook, Twitter, TikTok, Instagram, YouTube sok felhasználó posztol magáról és magával kapcsolatosan mindenféle privát információt, amit egy későbbi támadás során fel tud használni egy támadó. Gyakran a pontos helymeghatározást is nyilvános adattá teszik magukról és ezáltal könnyedén nyomon követhető válik, hogy mely helyeken fordul meg gyakrabban, mikor merre járt külföldön, vagy milyen ételeket, italokat fogyaszt szívesen az illető. Ezek az adatok nyilvánosan elérhetők és ez a tevékenység önmagában nem illegális, hiszen a felhasználók saját akaratuk szerint osztanak meg magukról információkat, viszont nagyon hasznos információkkal szolgálhat egy későbbi kibertámadáshoz.

- Böngésző előzményeken alapuló adatgyűjtés és automatikus kitöltés funkció kihasználása: Ha az eszközünkhöz, melyet napi tevékenységeink során használunk, hozzáférhet más személy, akkor könnyedén rá tud keresni, mely oldalakon jártunk korábban, mennyi ideig tarózkodtunk az adott oldalon, melyik oldalról érkezett a felhasználó. Mindezt akár hónapokra visszamenően is. Ezekből az előzményekből szintén megismerhetőek vagyunk, szokásaink, ízlésünk, gyakran látogatott weboldalaink alapján feltérképezhetővé válik, milyen módon lehet a legkönnyebb módon a közelünkbe férkőzni. Könnyedén tudnak a támadók egy általános profilt alkotni a böngészési előzmények alapján, illetve érzékeny adatokra lelhetnek. A böngészési előzményeken alapuló adatokkal történő visszaélés megelőzés érdekében érdemes néhány gyakorlatot bevezetnünk, különösen akkor, ha más is hozzáférhet az eszközünkhöz. Az inkognitó mód használatával el tudjuk kerülni, hogy az általunk látogatott oldalak megjelenjenek a böngészési előzményekben, vagy az automatikus kitöltési funkció használatának elkerülése, a beleegyezés-kezelés vagy anonimizálás előnyben részesítése, korábbi előzmények rendszeres törlése mind hasznosak lehetnek. [58]

1.3 Az online tér biztonságos alkalmazására bevezetett jogszabályok

GDPR

2018. május 24-től bevezetésre került az Európai Unió Általános Adatvédelmi Rendelete (General Data Protection Regulation). Ez a rendelet közvetlenül alkalmazandó minden személyes adat kezelési tevékenységére, amely az Európai Unió területéhez vagy piacához kapcsolódik. A rendelkezés megsértése akár 100 millió euróig terjedő szankcióval is büntethető. Ez az Európai Unióban egységes és közvetlenül alkalmazandó adatvédelmi jog szinte az összes meglévő tagállami rendelkezést felváltja és vállalkozásoknak, magánszemélyeknek, bíróságoknak és a hatóságoknak a nemzeti jogba való átültetés nélkül kell alkalmazniuk. A GDPR szinte az összes adatvédelemmel kapcsolatos kérdést közvetlenül szabályoz. [59] A GDPR egy rendelet, nem pedig egy irányelv, a megfelelés kötelező, anélkül, hogy minden tagállamnak ratifikálnia kellene a saját jogszabályában. A GDPR kiterjesztette az adatvédelem hatályát, így az mindenkire és minden szervezetre vonatkozik, amely uniós polgárokkal kapcsolatos információkat gyűjt és dolgoz fel, függetlenül attól, hogy hol tartózkodnak, vagy hogy hol tárolják az adatokat. [60] Egyes kutatások szerint a GDPR káros hatással van a piaci versenyre és innovációra, miszerint korlátozza a versenyt az adatpiacokon, koncentráltabb piaci struktúrákat hoz létre és megerősíti a már meglévők piaci erejét. Korlátozza az adatmegosztást a különböző adatgyűjtők között, ezáltal megakadályozza a kisebb cégek adatalapú ismereteit és a cégóriások további erősödését segíti elő. [61]

Hatalmas mennyiségű adatot generálunk és anélkül osztjuk meg őket, hogy törődnénk magánéletünk biztonságával. Mielőtt megszólalt volna az ébresztő az okostelefonunkon, alvási szokásainkat, szívdobbanásainkat egész éjjel rögzítette a karunkon viselt okosóra. Van személyre szabott lejátszási listánk a különböző zenehallgató appokon, lájkolunk, posztolunk, hozzászólásokat írunk, vásárlás után online értékelést írunk az eladóról vagy termékéről. Gyakori, hogy önkéntesen adunk meg magunkról szenzitív adatokat életkorunk, tartózkodási helyünk, vallási meggyőződésünk, szexuális irányultságunkkal kapcsolatban is. Hitelkártyánkkal fizetett tranzakcióink évekre visszamenőleg ellenőrizhetők. Minden tevékenységünk rögzítésre kerül. Akár tudatában vagyunk ennek, akár nem. Az Alfa és Z generációra hatványozottan igaz, hogy gyorsan reagálnak és elfogadják a felhasználási feltételeket anélkül, hogy végig olvasnák azt. Gyorsan kattintanak és tovább lépnek az általuk keresett weboldalra. Egy ilyen incidens kapcsán

2016 májusában 70.000 felhasználó adatait tette közzé az OK Cupid társkereső oldal. Az adatok anonim módon történő kezelésének az elmaradását azzal indokolták, hogy a felhasználók önkéntesen hozzájárultak a személyes adataik felhasználásához. [62]

Akár tudunk róla, akár nem, digitális lábnyomot hagyunk magunk mögött. Ezzel kapcsolatosan számos kérdés felvetül. Kié az adat? kinek van joga eladni azt? mennyit érnek ezek az adatok? megoszthatják-e az adatgyűjtők az adatainkat?

A fiatalokban természetes vágy él önmagukkal kapcsolatos információk megosztása iránt. Ehhez remek lehetőséget nyújt az internet. Bizalommal kitesznek magukról és életük nagyon sok aspektusáról képeket, amiket akár évekkel később is vissza tudnak keresni róluk. A cég óriások pedig a rólunk megszerzett adatok alapján személyre szabott hirdetéseket küld nekünk célzottan.

A kereskedelmi érdek, a figyelmük irányítása az adott termékekre, gondolataink befolyásolása egyre aggasztóbb méretek ölt. Az adataink védelmével kapcsolatban felmerülő aggályok egyre inkább nőnek a technológia, a közösségi hálózatok és egyéb társadalmi normák turbulens fejlődésével. A személyes adatokkal történő visszaélés megelőzésére és az esetleges visszaélések szankcionálására fókuszál a GDPR.

Nemzetközi kiberbiztonsági védelem

A kiberbiztonság egy kiemelt figyelmet igénylő aspektusa, a határokon átívelő jelleg. E-tekintetben különleges megoldási metódust igényel és kiemelt jelentőséggel bír, méltán, bárminemű incidens, illetve támadás jelenléte globális fenyegetettséget is jelenthet.

A korábbiakban tárgyalt és többször hangsúlyozott különlegessége a Z és az őket követő generációknak a globális jelenlét a világháló segítsége által. Az internet összeköti az embereket a világ bármely két különböző pontján helyezkedjenek is el. Ebből a tényből következik, hogy nem lehet kizárólag országhatáron belül intézkedéseket hozni digitális adataink védelme érdekében. Hiszen amit az egyik országban evidens és magától értetődő, azt nem ismerik vagy nem értik a világ más pontján élő lakosok. Ez a helyzet könnyen kihasználhatóvá és védtelenné teheti a felhasználókat, akik természetesen nem csak magánszemélyeket, hanem cégeket és államokat is érint.

Többek között ezért is volt szükség egy nemzetközileg elfogadott és alkalmazandó kiberbiztonsági stratégiára. A nemzetközi védelem kialakítása érdekében támogatja az

ENISA több, mint egy évtizede az EU-tagállamokat nemzeti kiberbiztonsági stratégiáik kialakításában. 2017 óta minden uniós tagállamnak konkrét nemzeti kiberbiztonsági stratégiája van. Az ENISA (European Union Agency For Cybersecurity) (Európai Uniós Kiberbiztonsági Ügynökség) erőfeszítéseinek köszönhetően a tagállamok felismerték, hogy a kiberbiztonságban az innovációnak feltétlenül prioritást kell élveznie, hogy a polgárok és az EU tagállamai határokon átnyúló együttműködéssel a kiberbiztonság magas szintjét tudják biztosítani. Ehhez elengedhetetlen a köz és magánszféra szoros partneri viszonya (PPP) Public Private Partnership), a nemzeti kiberbiztonsági stratégiák (NCSS) (NKBS Nemzeti Kiberbiztonsági Stratégiák) kialakítása, alkalmazása és naprakészen tartása, az információmegőrző és elemző központok (ISAC Information Sharing and Analysis Center) mindenkor aktuális felügyelete és támogatása. Az információmegőrző és elemző központok (ISAC) nonprofit szervezetek, melyek központi forrást biztosítanak a kiberfenyegetésekkel kapcsolatos információk szerzéséhez, illetve a magán és közszféra közötti kétirányú információ megosztást tesz lehetővé. [63]

Az országhatárokon átívelő érintettség, illetve a PPP (köz és magánszféra partneri viszonya) egy említésre méltó rizikófaktora, hogy az incidensekre vagy fenyegetésekre való reagálás, illetve ezeknek a mérséklésére történő intézkedés, megoszthatja az érintett feleket több aspektusból is, különös tekintettel a hírnévkockázatra vagy a gazdasági érdekre. Az ENISA modelljének fő kérdései arra vonatkozóan, hogy mi kell a sikeres PPP-hez a következők:

1: Why? – Miért? Az együttműködés célja. Mi a konkrét fenyegetés vagy kockázat.

2: Who? – Kik? Mely szereplők vegyenek részt (állami, magán, civil)

3: How? – Hogyan? A működési keretek, szabályok, jogi alapok, döntéshozatal

4: What? – Mit? Milyen közös gyakorlatok, védelmi intézkedések, együttműködés

További főbb kihívások és sikertényezők:

- Bizalom: Az egyik legfontosabb tényező a magánszféra és az állami szereplők között

- Jogi keretek és szabályozás hiánya: Gyakran nincs egyértelmű jogalap vagy szabályzat

- Motiváció és részvétel: Különös tekintettel a kis- és középvállalkozói szektorra

- Fenntarthatóság, adaptivitás: A PPP-knek képesnek kell lenniük alkalmazkodni a változó fenyegetésekhez és technológiákhoz.

A köz és magánszféra partnerségéről az ENISA tanulmányt is készített, [64] amelyben információkat gyűjtött a legjobb gyakorlatok lehetőségeiről és a közös megközelítésről. [65] A kutatás elemzi a PPP-k jelenlegi helyzetét az EU-ban, valamint azonosítja az együttműködés főbb modelljeit, a magán- és a közszféra jelenlegi kihívásait a PPP-k létrehozása és fejlesztése során és ajánlásokat fogalmaz meg a PPP európai fejlesztésére. [66]

Az ENISA hangsúlyozza, hogy nem az információátadás jelentősége a döntő, hanem az információcsere a különböző érdekelt felek között. A téma fontosságát és egzakt meghatározását erősítendően 2009-ben az ENISA kiadta a GPG-t (Good Practice Guide on Information Sharing), vagyis az információmegosztásról szóló helyes gyakorlati útmutatóját. [67]

2018-ban megjelent az ISAC (Information Sharing and Analysis Center) az információmegosztó és elemző központok együttműködési modelljéről. Ebben a kutatásban az ENISA összegyűjti a bevált gyakorlatokról szóló információkat és három különböző modellbe sorolja a megközelítéseket: országközpontú, ágazatspecifikus és nemzetközi struktúrák. Az ISAC-k olyan megbízható entitások, melyek elősegítik az információmegosztást a kiberfenyegetésekkel, illetve azoknak a mérséklésével szemben. [68]

2020-ban az ENISA kidolgozott egy keretrendszert, [69] amely segíti a különböző tagállamokat az NCSS (National Cybersecurity Strategies) (Nemzeti Kiberbiztonsági Stratégiák) céljaik elérének érdekében stratégiai és operatív szinten egyaránt. [70] Minden tagállam kifejlesztette a saját NCSS-jét. [71]

2022-ben napvilágot látott egy újabb kutatás az ISAC-k tevékenységéhez kapcsolódóan (Cross Sector Exercise Requirements). Ennek a tanulmánynak az elsődleges célja, hogy az európai információmegosztó és elemzőközpontok között a kommunikáció eredményes és sikeres legyen. [72]

NIS és NIS-2 irányelvek

A NIS 1 (2016/1148 irányelv) volt az első olyan átfogó uniós jogszabály, amely a kiberbiztonsági irányelveknek megfelelő, az uniós társadalmi és gazdasági infokommunikációs és hálózati rendszerek kiberbiztonsági szempontból történő fokozására irányultak. [73] A NIS (hálózat és információbiztonság) jövője a köz és magánszféra együttműködésével kapcsolatban egy tanulmány is megjelent az ENISA közreműködésével. [74]

Az Európai Köz-Magán Partnerség a Rugalmasságért az EP3R-t 2009-ben hozták létre, azzal a céllal, hogy köz és magán partnerséget (PPP) alkalmazzanak a telekommunikációs szektor határokon átnyúló biztonsági és ellenálló képességi aggályainak a kezelésére. [75] 2020 decemberben javasolta az Európai Bizottság a NIS 1 felülvizsgálását, amelynek eredményeként lépett hatályba a NIS 2 2023. januárban. 2024. október 17-ig a tagállamoknak át kellett ültetniük a nemzeti jogukba a NIS 2 irányelvet. 2024. október 18-tól hatályon kívül helyezték a NIS 1-et. A NIS 1 által lefedett hálózatok: energia, közlekedés, egészségügy, pénzügy, vízgazdálkodás, digitális infrastruktúra.

A NiS 2 (2022/2555) irányelv egységes jogi keretet hoz létre annak érdekében, hogy az Európai Unióban 18 kritikus ágazatban fenntartsa a kiberbiztonságot. A NIS 2 szélesebb körben és magasabb szigorral terjeszti ki az EU-s kiberkövetelményeket. Nagyobb felelősséget jelent és hangsúlyosabb vállalati felelősségre vonhatóságot eredményez. Ez nagy hatást gyakorol mind az állami stragtégiára mind a vállalatok működésére Magyarországon. Kiterjeszti az irányelv hatályát több (18+) szektorra és sokkal több vállalatra. Szigorúbb kockázatkezelési, beszállítói, audit és jelentési kötelezettséget jelent. Egységesebb uniós megközelítést követel meg, de a végrehajtás (transzpozíció) tagállami szinten történik, ezért fontos, hogy a magyar jogrend pontosan hogyan ülteti át az irányelvet. [76] A tagállamoknak ki kell dolgoznia nemzeti kiberbiztonsági stratégiákat, az Európai Unióval közös együttműködésben a határokon átívelő mihamarabbi reagálás és végrehajtás érdekében. Előírja a tagállamok számára, hogy javítsák kiberbiztonsági képességeiket, továbbá kockázatkezelési intézkedéseket és jelentéstételi követelményeket vezessenek be. Ezentúl szabályok felállítását is kötelez az együttműködés, információmegosztás, felügyelet és kiberbiztonsági intézkedések végrehajtására vonatkozóan. Az irányelv előírja, hogy minden tagállamnak nemzeti

kiberbiztonsági stratégiát kell elfogadnia, amely magában foglalja a kiberbiztonság oktatására és tudatosságára vonatkozó szakpolitikát is.

A NIS 1 által már lefedett ágazatok mellett a nyilvános elektronikus hírközlési szolgáltatókra, több digitális szolgáltatásra (pl. közösségi platformok használata), hulladék és szennyvízgazdálkodásra, kritikus termékek gyártására, futárpostai szolgáltatásra, központi és regionális szintű közigazgatásra, valamint az űrágazatra is vonatkoznak.

E kritikus ágazatokban a közepes és nagy méretű szervezeteknek megfelelő kiberbiztonsági kockázatkezelési intézkedéseket kell hozniuk és értesítési kötelezettségük van a nemzeti hatóságok felé. [77] Bevezeti továbbá a felső vezetés elszámoltathatóságát a kiberbiztonsági kockázatkezelési intézkedéseknek való meg nem felelés esetén. [78]

Hazánkban is fel kell készülni a 21. század szinte legnagyobb fenyegetésének a legküzdésére, amely a kibertér. Az új Európai Uniós irányelv ebben segítséget mutat hazánk számára is, viszont a NIS2 irányelv megfelelő implementálása rendkívül fontos, mert ez fogja a jövőben meghatározni Magyarország kibervédelmi alapjait. [79]

Az irányelv létrehozza a számítógép-biztonsági eseményekre reagáló csoportok hálózatát (CSIRT). Ezek a csoportok elengedhetetlenek a kiberfenyegetésekre vonatkozó információk gyors cseréje és az eseményekre való reagálás tekintetében.

Az irányelv továbbá létrehozza az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatás (EU-CyCLONe). Az a hálózat támogatja az összehangolt irányítást és biztosítja a tagállamok és az uniós intézmények közötti rendszeres információcserét nagyszabású események és válságok esetén.

A Kiberbiztonsági Együttműködési Csoport a kiberbiztonsági irányelv által létrehozott platform, amelynek célja az uniós tagállamok, az Európai Bizottság és az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) közötti stratégiai együttműködés információcsere megkönnyítése. [80]

Fejezet végi összefoglalás

A bevezetésben megfogalmaztam a tudományos problémát és ehhez kapcsolódóan definiáltam kutatásom két hipotézisét, melyek a következők voltak:

H1: Feltételezem, hogy a magyar közoktatás nem fordít elegendő figyelmet a kiberbiztonság témájára

H2: Feltételezem, hogy a magyar közoktatásban nincs megfelelően felépített, naprakész tananyag kiberbiztonság témájában

Részletesen ismertettem a témához kapcsolódó kutatási tevékenységemet, mely kvalitatív kutatást követően kvantitatív módszereket is tartalmazott. A **kvalitatív kutatás** keretében fókuszcsoportos megkérdezést és szakértői mélyinterjúkat készítettem. Az oktatásban résztvevő mindkét fél véleményét felmértem: hallgatókat és oktatókat egyaránt. Ezekre a felmérésekre alapozottan készítettem el **kvantitatív kutatás** keretein belül a kérdőívet, melyet többször is megosztottam különböző social media felületeken. Az utolsó kiküldés időpontja 2025. augusztus. A kitöltés teljesen anonim módon, önkitöltéssel történt. A kérdőívet 6 szakaszra osztottam és szűrőkérdések segítségével irányítottam a kitöltési lehetőségeket. A kiberbiztonság oktatására vonatkozó kérdéseket csak az Alfa és a Z generáció tagjai tudták kitölteni. A kérdőív hólabda mintavételi eljárással készült.

Ezt követően az első fejezetben a digitális jelenlét jellemzőit mutattam be a különböző generációk eltérő szokásainak figyelembevételével. Magyarázattal szolgáltam arra vonatkozólag, hogy miért éppen az Alfa és a Z generáció áll kutatásom fókuszában, ezt saját készítésű ábrával is szemléltettem. Ők az első olyan nemzedék, akik már digitális korba születtek bele és ennek megfelelően eltérő a szocializációjuk és gondolkodásmódjuk.

Ezt követően az online térben fellelhető veszélyforrásokat és adathalászati módszereket mutattam be. Két csoportra bontva mutattam be ezeket a technikákat, mely szerint IP tudást nem igénylő, illetve kifejezetten IP alapú, mélyebb szakmai ismereteket kívánó támadások. Ismertettem a különböző social engineering adathalászati technikákat és szakmai berkeken belül történő elnevezésüket. Ezekután bemutattam az online tér biztonságos alkalmazására bevezetett jogszabályokat, külön részletesen bemutattam a GDPR, a NIS és a NIS 2 irányelvek bevezetését az Európai Unióban, kiemelten bemutatva a köz és magánszféra partnerség fontosságát e-tekintetben (Public Private Partnerships).

2 PRIMER KUTATÁS EREDMÉNYEI

2.1 A kutatás átfogó bemutatása

A kutatás előzményei

Több éve oktatom a Z generációba tartozó fiatalokat egyetemi és szakgimnáziumi közegben egyaránt. Gyermekem Z generációba tartozik és születése óta célom volt, hogy nagyon tudatos szülő legyek, így élete minden aspektusában igyekeztem jelen lenni, természetesen megfelelő távolságot tartva, hogy tudjon kibontakozni is. Ezen történések okán tanúja voltam, hogy már a 8-10 éves gyermekek is jelentős mértékű privát tartalmat kezelnek az online térben, például különböző online játékok vagy közösségi platformok használata által. Azt is megfigyeltem, hogy a gyerekekkel legtöbb esetben nem beszélgetett el senki a tudatos és biztonságos internethasználatról. Magam több esetben is tanúja voltam annak, hogy milyen traumákat éltek meg ezek a fiatalok, amikor több hónapnyi játszás (és pénz ráfordítás) után, elvesztették a hozzáférésüket a kedvenc platformjukhoz, mert valamilyen kecsegtető ajánlat miatt kiadták a jelszavukat egy idegennek. És gyakran sajnos a gyerekek ezt el sem mondták a szülőknek vagy más felnőtteknek. Rosszabb esetben a közösségi térben éltek vissza a gyerekek óvatlanságával. A primer kutatás eredményeiben több esetet is bemutatok, ahol egészen fiatal 8-10 éves gyermekek szenvedtek el kibertámadás okozta traumát. És ezzel szoros összefüggésben kezdtem el kutatni, hogy intézményesített keretek között kaptak-e bármilyen iránymutatást, oktatást vagy bármilyen módon segítségnyújtást az iskolák kapuin belül a gyerekek és fiatalok, vagy e-tekintetben teljesen magukra és szüleikre vannak hagyva.

A kutatási célok

Kutatási célom az volt, hogy megvizsgáljam az Alfa és Z generáció körébe tartozó fiatalok kiberbiztonsággal kapcsolatos tapasztalatait a magyar közoktatásban. Szerettem volna megtudni, hogy az eddigi tanulmányi éveik alatt volt-e oktatásba integráltan szó a biztonságos jelszóhasználatról, online jelenlétről, a jelszavak tárolásáról és másoknak történő kiadásáról, továbbá kaptak-e bármilyen módon elérhető tananyagot a kiberbiztonsággal kapcsolatosan, úgymint: tankönyvet, jegyzetet vagy e-learning tananyagot. További kutatási célom, mely szorosan kapcsolódik az előzőekhez, hogy kaptak-e bármilyen iránymutatást intézményesített kereteken belül az online vásárlással kapcsolatos biztonsági óvintézkedésekkel kapcsolatosan.

A kutatási módszerek

Munkám során törekedtem arra, hogy az Alfa és a Z generáció kiberbiztonsági oktatását a lehető legteljesebb módon, több aspektusból is megvizsgáljam. Ennek érdekében több kutatási módszert is alkalmaztam, melyek a következők:

- Szekunder kutatás keretein belül a legújabb kutatási eredményekre fókuszáltam és több – a témában kiváló – kutató munkáját ismertem meg. Szekunder adatgyűjtésem során definiáltam a különböző generációkat, bemutattam jellemzőiket és kitértem az Alfa és a Z generáció különleges jellemvonásaira. Ismertettem az online térben fellelhető veszélyforrásokat, adathalászati módszereket, a social engineering fogalmát. Elkülönítettem az IT alapú tudást igénylő és IT alapú tudást nem igénylő adathalászati technikákat. Bemutattam az online tér biztonságos alkalmazására bevezetett jogszabályokat hazai és nemzetközi kitekintésben is.

- Kvalitatív kutatás keretein belül kétféle vizsgálatot folytattam:

- Mélyinterjút készítettem oktatókkal, akik több éve valamilyen digitális jellegű órát tartanak, illetve

- Fókuszcsoportos megkérdezés keretein belül készítettem egy átfogó jellegű kutatást az Alfa és a Z generációba tartozó fiatalokkal. Ennek során a kiberbiztonság oktatásával kapcsolatban szerzett tapasztalataikról kérdeztem őket.

A kvalitatív kutatás eredményeire alapozottan folytattam le a későbbiekben a kvantitatív kutatást.

- Kvantitatív kutatáshoz sztenderdizált kérdőívet készítettem. Hólabda mintavételi eljárást alkalmaztam és különböző közösségi oldalak igénybevétele által többször is közzé tettem. Az utolsó kiküldés időpontja 2025. augusztus. A kitöltés teljesen anonim módon, önkitöltéssel történt. A kérdőívet 6 szakaszra osztottam és szűrőkérdések segítségével irányítottam a kitöltési lehetőségeket. A kiberbiztonság oktatására vonatkozó kérdéseket csak az Alfa és a Z generáció tagjai tudták kitölteni.

A következő fejezetben a könnyebb áttekinthetőség érdekében külön alfejezetekre tagoltan fogom bemutatni a kvalitatív és a kvantitatív kutatási eredményeket.

2.2 Kvalitatív kutatás

Mélyinterjúk

Az alanyok kiválasztása önkényes mintavétel keretében valósult meg. A kvalitatív fázisban félig-strukturált vezérfonalat (guide) alkalmaztam, melynek főbb témakörei:

- Általános, bevezető kérdések

- A témához köthető személyes érintettség

- A témához köthető személyes tapasztalatok általánosságban

- A témához köthető személyes történetek, emlékek

- Azon konkrét kérdések feltevése, amelyek nyitva maradtak a személyes tapasztalatok megosztása közben, vagy teljes egészében kimaradtak és a témához kapcsolódnak.

- Befejezés

Szakmai mélyinterjúk készítése során összesen 5 olyan pedagógussal, illetve oktatóval beszélgettem, akik több éves oktatói tapasztalattal rendelkeznek valamilyen digitális jellegű tantárgyban. Az interjúkat személyes jelenléttel készítettem el, kivéve egy alkalmat, melyet Messenger videóhívás segítségével online módon valósítottunk meg.

Az interjúkat összegezve értékelem.

Kezdetben általánosabb kérdéseket tettem fel, hány éve tanít, milyen tantárgyakat oktatott, melyik intézményekben dolgozott ezelőtt satöbbi. Az idő haladtával a kezdeti zavart fázist követően megnyíltak az interjúalanyok és több személyes tapasztalatot is megosztottak velem.

- Amiben minden interjúalanynak egyezett a véleménye, hogy a mostani fiataloknak szövegértési nehézségeik vannak, nehezebb a figyelmüket fenntartani, mint a korábbi generációba tartozó fiatalokét, nem szeretnek írni és jegyzetelni, a telefonjukat és az ehhez köthető alkalmazásokat rutinszerűen tudják használni elsősorban csevegésre, vagy valamilyen közösségi média felületen, de a valódi tudást igénylő programok használatával kapcsolatban, mint például a Word vagy Excel, esetleg Power Point, gyakran nehézségekbe ütköznek és nem ritka, hogy egészen alapvető készségekre sem

tettek még szert ezeknek a programoknak a használatával kapcsolatban. Az sem ritka jelenség, hogy 9. osztályban van olyan fiatal, aki nem tud az asztalon létrehozni egy mappát és átnevezni. Nem tudják mi a különbség a mentés és a mentés másként funkció között, illetve mit jelent az asztal, tálca, fájl hierarchia fogalma a számítógép használat során. Az a központi intézkedés, melynek keretén belül az iskolában elzárásra került a fiatalok telefonja a tanítás idejére, egyöntetű tetszést keltett az interjúalanyokban a kezdeti nehézségek, illetve ellenállás legyőzését követően. Ennek az intézkedésnek a bevezetésével csökkent a gyakorisága a kijelzőre való rápillantásnak, ami korábban nagymértékű problémaként volt jelen a tanórák során. Kiberbiztonság oktatásával kapcsolatban nincs egy rendszeresen alkalmazott tananyag, többször szóba kerül tanórákon, de nincsen strukturáltan körbejárva a téma. Ennyi idős korban már rendelkezni kell(ene) az ilyen irányú alapvető tudással. A tanóráknak meg van a szigorú tervezete egy tanévre előre, amelyben nem kap külön figyelmet a digitális adatvédelem, netbank használat. Tudatosan kell tanítani a vizsgakövetelményeknek megfelelően, melynek keretein belül az Office alkalmazások készségszintű használata van inkább fókuszban.

- Az interjúalanyok egyedi, a többiektől eltérő véleményei, személyes történetei: A kiberbiztonság oktatásával kapcsolatban eltérő vélemények is megfogalmazódtak az interjúalanyokban. A több, mint 20 éve oktatók körében (3 interjúalany) az a vélemény állta meg a helyét, hogy nincs szükség egy kiberbiztonsági oktatóanyag központi bevezetésére. Ennek magyarázata, hogy a középszintű oktatásban már különböző szakoknak megfelelő célzott oktatás történik. A kiberbiztonság témáját ennyi idősen már tudniuk kell. A tanórák száma úgy van meghatározva, hogy nagyon feszített tempóban lehet a kötelezően előírt tananyag végére érni, melyek a vizsgák teljesítéséhez elengedhetetlenül szükségesek. Ebből az óraszámból elvenni már nem tudnának a kiberbiztonság oktatására. A másik két interjúalany, aki több, mint 10 éve és több, mint 5 éve tanító pedagógusok, már nyitottabbnak bizonyultak a kiberbiztonság oktatásának bevezetésével kapcsolatban. Szerintük is nagyon fontos lenne erre időt szánni és hasznosnak tartanának egy jól felépített szakmai anyagot, amire támaszkodhatnának a tanév és a tanmenet kialakítása során a kibervédelemmel kapcsolatosan. Véleményük szerint a tudást ismételni kell azoknál a témáknál is, ahol a tanulnivaló permanens, de a kiberbiztonság témaköre turbulensen változik és akár 1-2 év elteltével is elavulttá válhat a tudás nagy része.

Fókuszcsoport

Az alanyok kiválasztása önkényes mintavétel keretében valósult meg. A kvalitatív fázisban félig-strukturált vezérfonalat (guide) alkalmaztam, melynek főbb témakörei:

- Általános gondolatébresztő kérdések a témában

- A témával kapcsolatos vélemények, tapasztalatok általánosan

- A témával kapcsolatban érzett hiányokra való rákérdezés

- Személyes emlékek, tapasztalatok

- Befejezés

A fókuszcsoportos interjúk felvételére 3 alkalommal került sor és egyszerre 8-10 fiatal részvételével történt, akik 16-19 év közöttiek. A fókuszcsoportos megkérdezés során törekedtem arra, hogy az interjúalanyok a saját gondolatmenetüket tudják követni és hagytam a fiatalokat, hogy brainstorming jelleggel egymást ösztönözzék a kiberbiztonság témájával kapcsolatos tapasztalataik megosztása során. Egy rávezető kérdéssel elindítottam a beszélgetés fonalát és hosszú perceken keresztül csak figyeltem és jegyzeteltem a 16-19 év közötti fiatalok észrevételeit, emlékeit, tapasztalatait. Gyakran egymást is kérdezték, ha egy felvetés nem volt egyértelmű, vagy nyitott maradt egy kérdés vagy esetleg megválaszolatlan. Ennek a módszernek híve vagyok, mert az igazán értékes gondolatok és tartalmak így könnyebben áradnak ki a fejekből, mint amikor irányítottan kell egy kérdést megválaszolni. Nagyszerű csoportokat sikerült kialakítanom, ahol a résztvevők kifejezetten proaktívak és lelkesek voltak. A fókuszcsoportos interjúk során sikerült összeállítanom a kérdőívem fontos, sarkalatos kérdéseit. Sokat segített, hogy hogyan, milyen módokon tegyek fel majd kérdéseket a kérdőívben, hogy minél kevesebb legyen benne a nem egyértelmű vagy többesélyes kérdés-válasz lehetőség. A fókuszcsoportok alkalmával sok tapasztalatot nyertem. Sok ötletet merítettem a kérdésekre vonatkozóan és hihetetlen személyes történeteknek lehettem a tanúja. Volt olyan fiatal, akinek mentálisan komoly nehézséget okozott az, amikor 10 éves korában kizárták őt egy online játékból, amit évek óta játszott és ahol már komoly sikereket ért el. A trükk egyszerű social engineer technika volt, meg kellett adnia a felhasználó név és jelszó párost, amelyek a belépéshez szükségesek és ennek fejében egy, a játékban nehezen megszerezhető jutalomban részesült volna. Miután megadta a szükséges adatokat, kizárták őt. Elveszett több év munkája. A szüleivel és más felnőttekkel nem beszélte meg,

mert „úgysem értették volna meg” és nem szerette volna hallgatni még a „leszidásokat” is. Viszont ebből az esetből tanulva, a fókuszcsoportos beszélgetés során kiderült, hogy ennek a fiatalnak az egyik legkiemelkedőbb a tudása a kibervédelemmel kapcsolatban. Sajnos olyan történet is elhangzott, hogy egy fiatal lánynak a személyes fotóival a saját legjobb barátnője élt vissza, amikor összevesztek. Ebből egyébként iskolai szintű botrány lett a szülők bevonásával, mert aktképekről volt szó és igencsak fiatal volt még akkor a hölgy. Ezek olyan történetek, amelyeket nem írna meg senki egy kérdőív kitöltése során, mégis nagyon hasznos információkkal szolgáltak. Ezért is tartottam nagyon lényegesnek a kutatásom szempontjából a fókuszcsoportos megkérdezést.

Személyes esettanulmányok

Kutatásom során az elmúlt 4 évben számos személyes tapasztalatra is szert tettem, amelyekből szeretnék néhány konkrét példát kiemelni, mert szorosan kapcsolódnak a kutatási témámhoz és a személyes érintettség miatt személyközelibbé válik a kutatás. Véleményem szerint a személyes tapasztalatok patinássá teszik és tovább emelik a tudományos munka színvonalát.

Egy általam nagyon kedvelt kolléganőmmel történt meg az eset, hogy egy széleskörű kibertámadás áldozata lett. Amikor engem felkeresett már sajnos több hete sikertelenül próbálták megoldani a helyzetet, amibe belekerült. Minden személyes jellegű platformjába behatoltak illetéktelen személyek, a nevében vírussal (vagy egyéb kártevővel) fertőzött linket tartalmazó üzeneteket küldtek Messenger és Gmail alkalmazásokon keresztül. Én is kaptam tőle ilyen jellegű üzenetet, de nem nyitottam meg, mert gyanús volt, ezért rákérdeztem és így derült fény az esetre. Minden személyes platformjából kizárták őt, pedig neki a munkájához kapcsolatosan elengedhetetlen ezeknek a szoftvereknek a napi szintű használata. Amikor összeültünk, hogy átbeszéljük mi történt, olyan súlyú felhasználói gondatlanságról számolt be, amit elképzelni sem tudtam volna. A hölgy elmúlt 60 éves és diplomás, intelligens és értelmes asszony. A szakmájában kiemelkedő eredményeket ért el. Ezt szeretném hangsúlyozni, mielőtt leírom a tapasztalataimat az esettel kapcsolatban: Vannak közös és saját használatra szánt gépek is a munkahelyén. Gyakran használta a közösségi gépeket, ahonnan nem lépett ki használat után. A közös használatú gépeken nyitotta meg a közösségi médiás felületeket is (ezek a munkájához elengedhetetlen fontosságúak). Online banki tevékenységet csak a

telefonján végzett, de ott sem lépett ki a banki applikációból használat után. Nem volt kétlépcsős azonosítása, sem biometrikus azonosításra alkalmas védelem a telefonján. Csupán 4 számjegyből álló pin kóddal használta a banki applikációt. Sajnos annyira megfosztották minden személyes elérhetőségétől, hogy teljesen újra kellett minden felületre regisztrálnia. Majd az új regisztrációit követően is kizárták őt az új felületekről. Az esettel kapcsolatban sok kérdés és érzelem felmerül az emberben, de a kutatásom témájához szorosan köthetően az a tanulság, amelyet többször is hangsúlyozok a disszertációmban, hogy edukálni kell a lakosságot. Strukturáltan, releváns, naprakész információval, szakemberek által előállított tananyaggal. Az ilyen tananyag hasznos lenne az idősebb korosztálynak is, akik így szégyenérzet nélkül tudnának tájékozódni a kiberbiztonsággal kapcsolatban.

Egy kicsit könnyedebb hangvételű tapasztalatom volt a következő eset: Megosztottam a social media felületemen a kérdőívem linkjét és néhány percre rá egy szintén kiberbiztonsággal foglalkozó, doktori végzettséget már megszerzett kutatótársam küldött egy like jelet reakcióként a posztom alá. Privát üzenetben megköszöntem neki. Erre visszaválaszolt, hogy honnan tudom, hogy kitöltötte a kérdőívet, ha egyszer anonim módon történik a kitöltés. Visszaírtam, hogy a reakciójelet köszöntem meg (ezzel is növeli a link népszerűségét), de akkor a kitöltést is köszönöm. Erre csak annyit írt, hogy „a jó social engineer”. Így viszont az időbélyeg alapján bármikor vissza tudnám követni, hogy nagy valószínűség szerint melyik kitöltött kérdőív lehetett az övé. Természetesen ezt nem tettem meg.

A személyes esettanulmányok tanulsága, hogy a kiberbiztonság és a tudatos felhasználás nagyon gyerekcipőben jár napjainkban. Miközben rengeteg adatot osztunk meg magunkról és az életünkről, a véleményünkről vagy a gondolatainkról ezeket az adatokat nem védjük megfelelően, láthatóvá tesszük teljesen idegen emberek számára, nyilvános internetes keresőmotorok találati listáján megjelenik és nagyon sok az olyan felhasználó, akiknek sejtésük sincs arról, mennyire könnyen követhetők és áldozattá tehetők a nem megfelelően kialakított tudatos felhasználásuk hiányában. Sajnos ez rendszerszinten és gyakran iskolázottságtól függetlenül jelenik meg. Ha nem tudunk egy probléma meglétéről, akkor nem is tudunk tenni a védelem érdekében. Az edukálásra figyelmet kellene fordítani a közoktatás területén kívül minden vállalat minden dolgozó tekintetében, illetve nagyobb figyelmet kellene fordítani rá tévéreklámok és más marketing eszközök segítsége által is.

2.3 Kvantitatív kutatás

Kérdőíves kutatás az Alfa és Z generáció tagjaival

A kérdőíves kutatást a fókuszcsoportos megkérdezés előzte meg, melyet az Alfa és a Z generáció tagjaival készítettem. A sztenderdizált kérdőívet Google Forms platformon szerkesztettem meg és tettem közzé. Kiküldésére többször sor került, az utolsó kiküldés időpontja 2025. augusztus.

A kitöltés teljesen anonim módon, önkitöltéssel történt. Napjainkban az Alfa és a Z generáció tagjai számára az 1-5-ig tartó skálán csillagokkal történő értékelés már teljesen rutinszerű, napi tevékenység. Ezt a tulajdonságukat a kérdőív program szerkesztői is figyelembe vették és egy újítás keretén belül bevezettek egy új kérdéstípust is a minősítést. Mivel egy ilyen értékelés könnyen kezelhető, és magától értetődő a kitöltők számára, több ilyen típusú kérdést is alkalmaztam. Ezenkívül a kérdőív tartalmazott rövid szöveges válasz, hosszú szöveges válasz és feleletválasztós kérdéseket is. Hólabda mintavételi eljárást alkalmaztam, több platformon is elérhetővé tettem a kérdőívet.

A minta nem reprezentatív.

A kutatási eredményeket némiképpen torzítja, hogy az interneten elsősorban, de nem kizárólagosan az én ismerőseim között osztottam meg a kérdőívet. Én jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskola hallgatója vagyok. Ezenkívül egy közgazdasági szakiskolában vagyok pedagógus. Ebből fakad, hogy a kérdőívet kiberbiztonság témájában kifejezetten magasan képzett Z generációs fiatalok is kitöltötték. Az Ő oktatásukat is az elmúlt 5 év tapasztalataira alapozva vizsgáltam. Viszont ez a doktori végzettséggel már rendelkező, illetve a jelenleg még doktorandusz hallgatók körében teljesen más eredményeket hozott, mint a közoktatásban résztvevőknél.

Természetesen felmerült annak a lehetősége, hogy szűrjem ezeket a válaszokat, de az Alfa és a Z generációba ők is beletartoznak. Amennyire lehetett a kérdéseket a közoktatásra irányítottam, de érthető okokból a magasan kvalifikált személyek esetében a tapasztalataik merőben eltérnek az elmúlt 5 év tekintetében, mint a gimnazista korosztálynak. Továbbá, ha szűrtem volna a magasan képzett doktoranduszok és már végzett doktorok válaszait, akkor felmerül a kérdés, hogy aki jelenleg nem tanul és nem vesz részt semmilyen képzésben, azoknak a személyeknek a válaszaik relevánsnak tekinthetőek-e a kutatásom szempontjából.

Amennyiben szűröm, hogy csak a jelenleg a közoktatásban tanuló fiatalok tudjanak válaszolni, akik még nem egyetemisták, akkor nagyon sok értékes választ veszíthettem volna el. Hiszen, aki most főiskolára jár és még az alapszintű képzésen vesz részt, az illető 5 évvel ezelőtt még középszintű oktatásban vett részt, tehát a válaszai relevánsnak számítanak a kutatásom tekintetében. Ezért úgy döntöttem, hogy vállalom azt a kockázatot, hogy a kutatásom eredményei némileg torzulnak a doktori végzettséggel (illetve a jelenleg még doktorandusz hallgatók) rendelkező kitöltők válaszai következtében.

Az első kérdés egy szűrő kérdés volt. Feleletválasztás keretében kellett kiválasztania a kitöltőnek, hogy mikor született. A következő 5 opció közül lehetett választani:

- 1965-1979 (X generáció)

- 1980-1994 (Y generáció)

- 1995-2009 (Z generáció)

- 2010 után (Alfa generáció)

- 1965 előtt

Azoknak a kitöltőknek, akik 1965 előtt születtek, illetve az X vagy az Y generációba tartoznak szakaszugrás történt és a továbbiakban már csak a demográfiai adatokat, illetve az utolsó hosszú választ tudták kitölteni, (ahol személyes tapasztalataikat, véleményüket és a témával kapcsolatban felmerült gondolataikat tudták leírni). Az Alfa és a Z generációt megjelelő kitöltők a következő szakaszba léptek és a továbbiakban csak ők tudták a kérdőív oktatással kapcsolatos kérdéseit megválaszolni.

A kérdőívet 6 fő témakörre tagoltam az alábbiak szerint:

1. szakasz: A kérdőív rövid bemutatása, Szűrő kérdés (a születési dátum kiválasztásának lehetősége)

2. szakasz: Bevezető, általános jellegű kérdések

3. szakasz: Netbank használatára vonatkozó kérdések

4. szakasz: Kiberbiztonság az oktatásban

5. szakasz: Kibertámadás, személyes történetek (ez opcionális szakasz volt. Korábbi szűrőkérdés alapján lehetett ezt a szakaszt kitölteni. A szűrőkérdés az előző, vagyis a 4. szakasz utolsó kérdése volt, amely így hangzott: Előfordult-e már Veled, hogy feltörték valamelyik online platformodat és visszaélés áldozata lettél? És, aki itt az igen opciót választotta, az tudott a 4. szakaszban írni a saját történetéről. Egyéb esetben ez a szakasz átugrásra került).

6. szakasz: Demográfiai adatok. A kérdőívet egy hosszú szöveges válasz opcióval zártam le, ahol a kitöltő megoszthatott bármilyen észrevételt a témával vagy a kérdőívvel kapcsolatban. Ez nagyon hasznosnak bizonyult az eredmények vizsgálatakor.

A kérdőív beküldése után, rövid üzenetben megköszöntem a kutatásban való részvételt.

A könnyebb áttekinthetőség érdekében a kérdőív válaszait hipotézisenként, a különböző hipotézisekhez kapcsolódóan fogom elemezni.

A kutatáshoz általam készített kérdőív konkrét bemutatása:

Kiberbiztonság, netbank használat

Kedves Kitöltő!

Doktori disszertációmhoz gyűjtök adatokat arra vonatkozóan, hogy mennyire vagy tájékozott az online térben gyakran előforduló kibertámadásokkal kapcsolatban.
Kérdéseim arra irányulnak, hogy mennyire figyelsz oda arra, hogy adataidat biztonságban tudd és mennyire vagy tudatos az adatvédelemmel kapcsolatban.

Arra is kíváncsi vagyok, hogy tanórákon, iskolai tanítás keretén belül mennyire kaptál megfelelő minőségű tanítást a kiberbiztonságról, az adatvédelemről, és támadás esetén tudod-e hogy hová fordulj segítségért.

A válaszaid teljesen anonim módon történnek. Nem lehet beazonosítani a válaszadókat.

Harmadik félnek nem adom ki sem az adatokat, sem a kutatásban résztvevők nevét.

Kérlek, hogy gondoldd át a válaszokat, mert fontos minden válaszod!

Nem lesz hosszú a kérdőív
Kitöltése kb. 3 perc

Köszönöm a segítséged!

* Kötelező kérdés

1. Mikor születtél? *

Soronként csak egy oválist jelöljön be.

- ◯ 1965-1979 (X generáció) *Ugrás a(z) 22. kérdésre*
- ◯ 1980-1994 (Y generáció) *Ugrás a(z) 22. kérdésre*
- ◯ 1995-2009 (Z generáció)
- ◯ 2010 után (Alfa generáció)
- ◯ 1965 előtt *Ugrás a(z) 22. kérdésre*
- ◯ Egyéb: _____

Bevezető, általános jellegű kérdések

2. Most gondolj a **számodra legfontosabb** online platformokra, amiket gyakran használsz. Ezeknek a védelmével kapcsolatban melyik a leginkább igaz rád? *

Soronként csak egy oválist jelöljön be.

- ◯ Jelszavaim legalább 12 karakter hosszúak. Tartalmaz kis és nagybetűt, különös karakteret. (Különös karakterek pl: ? ! %)
- ◯ Jelszavaim legalább 12 karakter hosszúak, különös karakter nélkül
- ◯ Jelszavaim nem érik el a 12 karakter hosszúságot
- ◯ Fogalmam sincs róla
- ◯ Nem akarok válaszolni

3. Ha kibertámadás érne és feltörnék valamelyik online fiókod, van-e olyan **felnőtt** személy, akihez fordulhatnál? *

Soronként csak egy oválist jelöljön be.

- ◯ Igen
- ◯ Nem *Ugrás a(z) 5. kérdésre*
- ◯ Nem tudom, nem akarok válaszolni *Ugrás a(z) 5. kérdésre*

4. Kihez fordulnál?

Netbank használata

A következő néhány kérdés arra vonatkozik, hogy netbanki applikáció használata során mennyire óvod magad egy esetleges kibertámadástól

5. Nyílt vagy ingyenes wifi kapcsolat használatával milyen gyakran lépsz be banki applikációba? *

Soronként csak egy oválist jelöljön be.

- Soha, erre nagyon odafigyelek
- Előfordult már, hogy kénytelen voltam, de igyekszem elkerülni
- Gyakran előfordul
- Nem használok banki applikációt
- Nem tudom
- Nem akarok válaszolni

6. Online bankolás során mindig használok kétlépcsős azonosítást. *

Soronként csak egy oválist jelöljön be.

- Igen
- Nem
- Nem használok banki applikációt és nem netbankolok
- Nem akarok válaszolni

7. A banki adataidat elmented-e, hogy egy későbbi vásárlás során könnyebben tudj fizetni? *

Soronként csak egy oválist jelöljön be.

- Minden általam gyakran használt eszközön elmentettem
- Több eszközön is elmentettem
- Egyetlen eszközön van elmentve
- Egyetlen eszközön sem mentettem el, inkább beírom kézzel amikor fizetek
- Nem fizetek online soha, így rám nem vonatkozik ez a kérdés

8. Azokon az eszközökön, amiken elmentetted a banki fizetéshez szükséges adataidat, hozzáférhet-e más? *

Soronként csak egy oválist jelöljön be.

- Igen, másokkal közösen használjuk (pl. család, barát) egymástól függetlenül
- Igen, de csak a felügyeletem mellett
- Nem férhet hozzá más rajtam kívül
- Nem mentettem el egyetlen eszközre sem fizetéshez szükséges adatot

Kiberbiztonság az oktatásban

Ebben a szakaszban azt vizsgálom, hogy részesültél-e megfelelő oktatásban a kiberbiztonsággal, adatvédelemmel, kibertámadással kapcsolatban iskolai keretek között

9. Volt-e olyan tanórád az elmúlt 5 év során, ahol a **tananyag részeként** tanultál a kiberbiztonságról? *

Soronként csak egy oválist jelöljön be.

- Igen
- Nem
- Talán

10. Volt-e **tankönyv** vagy jegyzet amit kaptál az elmúlt 5 év során a kiberbiztonsággal, az online adatvédelemmel kapcsolatban? *

Soronként csak egy oválist jelöljön be.

- Igen
- Nem
- Talán

11. Volt-e olyan **tanórád** az elmúlt 5 év során ahol hallottál a kiberbiztonságról, a digitális adataid védelméről? *

Soronként csak egy oválist jelöljön be.

- ◯ Igen, többször is
- ◯ Igen 1x vagy 2x szóba jött
- ◯ Nem volt

12. Szeretnéd-e, hogy **tananyagban** szerepeljen a kiberbiztonság, a digitális adatok védelme és tanórán legyen erre idő? *

Soronként csak egy oválist jelöljön be.

- ◯ Igen, nagyon fontosnak tartom
- ◯ Nem, szerintem fölösleges lenne
- ◯ Nem tudom, nem akarok válaszolni

13. Volt olyan **tanóra** az elmúlt 5 évben, ahol elhangzott, hogy milyen a **megfelelő erősségű** jelszó? *

Soronként csak egy oválist jelöljön be.

- ◯ Igen
- ◯ Nem
- ◯ Nem tudom, nem akarok válaszolni

14. Volt olyan **tanóra** az elmúlt 5 évben, ahol hallottál a tudatos és felelős online életről és eszközhasználatról? *

Soronként csak egy oválist jelöljön be.

- ◯ Igen
- ◯ Nem
- ◯ Nem tudom

15. Szerinted mennyire volt megfelelő az **iskolai oktatás** a biztonságos **online vásárlással** kapcsolatban? *
(1: Egyáltalán nem 5: Teljesen elégedett vagyok)

1 2 3 4 5

☆ ☆ ☆ ☆ ☆

16. Szerinted mennyire volt megfelelő az iskolai oktatás a **megfelelő jelszavak** használatával kapcsolatban? *
(1: Egyáltalán nem 5: Teljesen elégedett vagyok)

1 2 3 4 5

☆ ☆ ☆ ☆ ☆

17. Szerinted mennyire volt megfelelő az iskolai tanítás **általában véve** a kiberbiztonsággal kapcsolatban? *
(1: Egyáltalán nem 5: Teljesen elégedett vagyok)

1 2 3 4 5

☆ ☆ ☆ ☆ ☆

18. Mennyire vagy elégedett a **tankönyvekkel** és oktató anyagokkal, amiket kaptál az iskolában kiberbiztonsággal kapcsolatban? *
(1: Egyáltalán nem 5: Teljesen elégedett vagyok)

1 2 3 4 5

☆ ☆ ☆ ☆ ☆

19. Szerinted mennyire volt megfelelő az iskolai oktatás a **digitális adataid védelmével** kapcsolatban? *
(1: Egyáltalán nem 5: Teljesen elégedett vagyok)

1 2 3 4 5

☆ ☆ ☆ ☆ ☆

20. Előfordult már Veled, hogy feltörték valamelyik online platformodat és visszaélés áldozata lettél? *

Soronként csak egy oválist jelöljön be.

- Igen
- Nem *Ugrás a(z) 22. kérdésre*

Kibertámadás személyes történetek

21. Kérlek írd le, hogy mi történt amikor feltörték valamelyik platformon a profilodat! Azt írj le, amit fontosnak érzel, amit szívesen megosztanál másokkal, vagy ami nagyon emlékezetes számodra.

Néhány segítő kérdés:
Hogyan érezted magad?
Volt-e valamilyen maradandó károd?
Mennyire viselt meg?
Volt-e, hogy elvesztettél emiatt barátságot?
Volt-e anyagi veszteséged?
Volt-e szégyenérzeted?
Volt-e kellemetlenséged?
Tudtál-e fordulni valakihez?

Demográfiai adatok

A válaszok összehasonlítása miatt kellenek. Hogy meg lehessen állapítani, hogyan viselkednek a férfiak vagy nők, a gimnazisták vagy az egyetemisták

22. Nemed *

Soronként csak egy oválist jelöljön be.

- Férfi
- Nő

23. Jelenleg milyen képzésre jársz? *

Soronként csak egy oválist jelöljön be.

- Egyetem, főiskola
- Gimnázium, technikum, szakképzés
- FOSZK
- Nem járok képzésre

24. Ha van kedved írj néhány érzést vagy gondolatot a kiberbiztonságról, a kibertámadásról, a netbank használatáról, az oktatásról vagy a témával kapcsolatban bármiről.

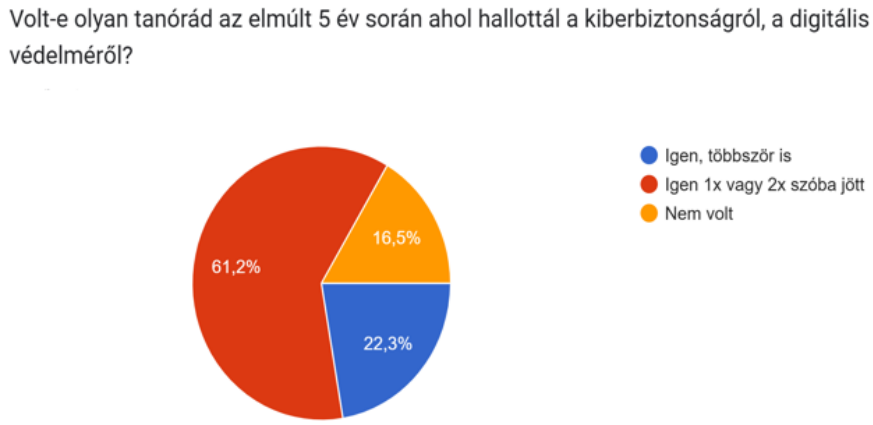
Ha nem szeretnél írni, nyugodtan hagyd üresen ezt a mezőt.

- Az 1. Hipotézisem vizsgálatához kapcsolódó kérdések és válaszainak elemzése:

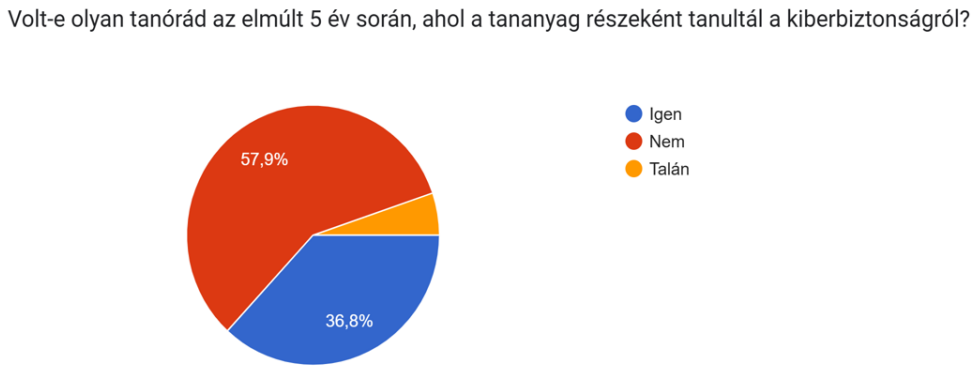
H1: Feltételezem, hogy a magyar közoktatás nem fordít elegendő figyelmet a kiberbiztonság témájára

A kérdőívben az 5/4. szakasz (Kiberbiztonság az oktatásban) kérdései vonatkoztak erre a vizsgálatra.

A következő két ábrán (4. és 5. ábra) egymással szorosan összefüggő kérdéseket vizsgálok. A különbség a két kérdés között annyiban tért el, hogy a kiberbiztonság oktatása az elmúlt 5 év során a tananyag részeként volt-e jelen a tanórán, vagy csak említés szintjén került szóba. A válaszokat a következő 2 diagram ábrázolja:



4. ábra Tanóra alatt a digitális adatok védelméről hallott az elmúlt 5 év során

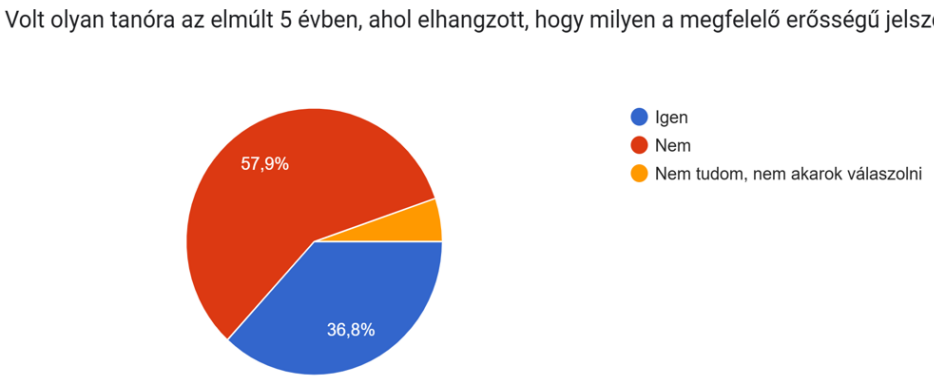


5. ábra Tanóra alatt tananyag részeként hallott a kiberbiztonságról az elmúlt 5 év során

A kitöltők válaszait elemezve megállapítom, hogy említés szintjén a diákok 85%-a hallott a kiberbiztonság fontosságáról, azonban tananyagba integráltan a kitöltők 37%-a tanulta. Ebből a jelentős különbségből arra lehet következtetni, hogy a Nemzeti Alaptantervben nincs integráltan, megfelelő súlyozással benne a kiberbiztonság témaköre. Ennek a

kijelentésnek a részletes bemutatásával a 3. fejezetben foglalkozom mélyebben. A kitöltők válaszai alátámasztják ezt a kijelentést.

A 6. ábra azt szemlélteti, hogy tanóra keretén belül elhangzott-e, hogy mik a megfelelő erősségű jelszó kritériumai. A piros szín illusztrálja a nem választ adók arányát.



6. ábra Tanóra alatt elhangzott mik a megfelelő erősségű jelszó kritériumai az elmúlt 5 év során

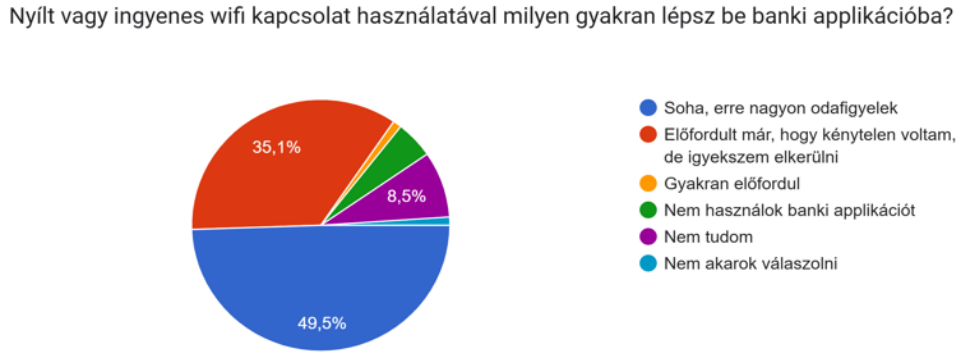
A kitöltők 58%-a szerint nem hangzott el tanórai keretek között, hogy milyen a megfelelő erősségű jelszó az elmúlt 5 év során. A Nemzeti Alaptantervben nem szerepel strukturáltan és konzekvensen a digitális adatok védelmének egyik legfontosabb alapköve, amely a jelszavak erősségére, tárolására, cseréjére és kiadására vonatkozik. A 3. fejezetben részletesen kitérek a Nemzeti Alaptanterv bemutatására.

A 7. ábra Azt mutatja be, hogy a kitöltő a tudatos online életről hallott-e tanóra keretein belül. A kék szín az igen, a piros szín a nem választ jelölil.

7. ábra Tanórán hallott a tudatos és online jelenlét feltételeiről az elmúlt 5 évben

A kitöltők közel 53%-a hallott tanórai keretek között a tudatos és felelős online jelenlétről és eszközhasználatról, azonban 42% nem hallott erről a fontos témáról. A kitöltők saját érzései és bevallása alapján a Nemzeti Alaptantervben kisebb hiányosságokat lehet megállapítani a felelősségteljes online eszközhasználat és digitális jelenléttel kapcsolatban, mint általában a kiberbiztonság oktatásának más területein.

A 8. ábra azt szemlélteti, hogy milyen gyakran használ nyílt vagy ingyenes wifi kapcsolatot banki tevékenység során. A kék szín a soha választ ábrázolja, a piros pedig, hogy igyekszik elkerülni, de már előfordult.



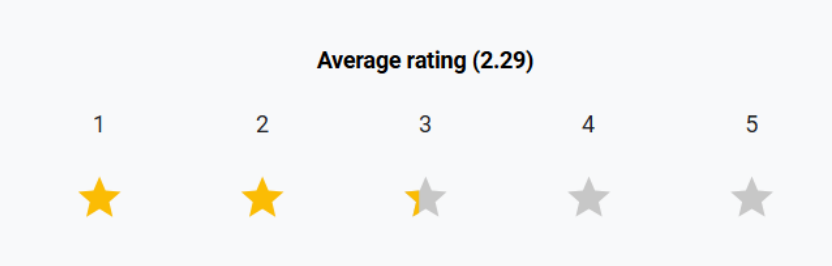
8. ábra Ingyenes Wifi és banki applikáció használata

Az ingyenesen elérhető Wifi hálózatok használatai minden esetben kiemelt kockázatot jelentenek a kibertérben. Használatuk során szenzitív adataink könnyebben hozzáférhetővé válnak. Ezért is ajánlatos nem csatlakozni ezekre a hálózatokra. Ennek a kérdésnek a válaszait megfigyelve megállapíthatjuk, hogy a kérdőívet kitöltő Alfa és Z generációba tartozó fiatalok 49,5%-a odafigyel arra, hogy ne használjon ingyenes wifi hálózatot netbanki tevékenysége során. Ez a kitöltőknek picivel kevesebb, mint a fele.

Az első hipotézisem vizsgálatához kapcsolódóan minősítés típusú kérdéseket is alkalmaztam, ahol 1-5-ig kellett értékelni saját tapasztalatok alapján a kiberbiztonság oktatásával kapcsolatosan felmerülő egyes állításokat. Az eddigi válaszokra adott értékekkel egybehangzó eredmények születtek.

A következő ábra az oktatás minősítését ábrázolja a kitöltők véleménye alapján egy 1-től 5-ig terjedő skálán. Az értékelés a megfelelő jelszóhasználat oktatására vonatkozik.

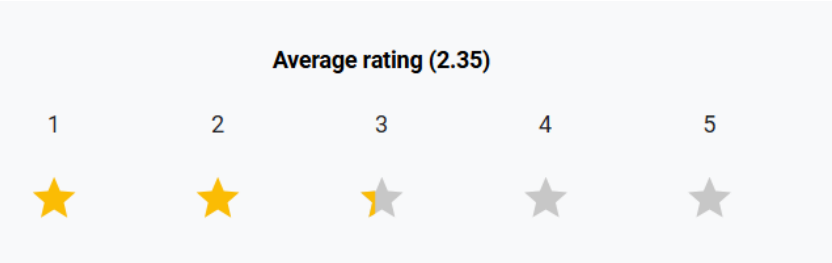
Mennyire volt megfelelő az iskolai oktatás a megfelelő jelszavak használatával kapcsolatban:



9. ábra Az oktatás minősítése a megfelelő jelszavak használatával kapcsolatban

Az Alfa és a Z generáció tagjai 2,3 csillagra értékelték az intézményesített kereteken belül megvalósuló kiberbiztonsággal kapcsolatos közoktatást. Az 5 csillag volt a maximum érték és ennek még a felét sem érte el az oktatás minősítése a válaszok alapján. A tanulók elégedetlenek a tanórai keretek között kapott oktatás minőségével a jelszóhasználat kérdésében.

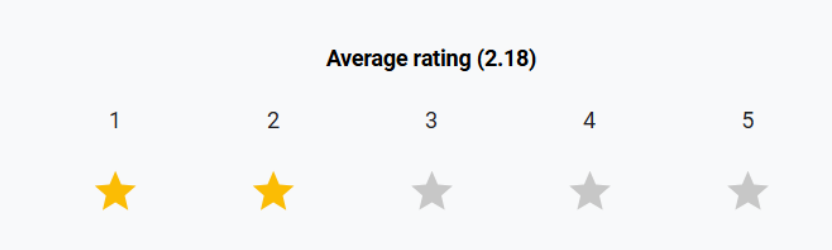
A következő, 9. ábra szemlélteti, hogy a kitöltők szerint mennyire volt megfelelő az iskolai tanítás a kiberbiztonsággal kapcsolatban.



10. ábra A kiberbiztonság oktatása az iskolán belül

A lehetséges 5 csillag közül 2,35 csillagra értékelték a kiberbiztonság oktatását intézményi keretek között a kitöltők. Ebből a válaszból is kitűnik az elégedetlen attitűd a kiberbiztonság oktatásával kapcsolatban. Ez az értékelés tükrözi a Nemezti Alaptanterv hiányosságait a kiberbiztonság témakörében. A kitöltők alapvetően elégedetlenek a kibervédelem oktatásával kapcsolatban, magasabb szintű képzésben szeretnének részesülni.

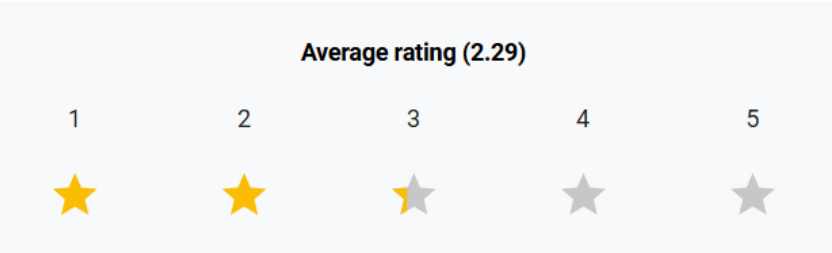
A következő, 10. ábra azt szemlélteti, hogy mennyire volt megfelelő az iskolai oktatás a digitális adatvédelmével kapcsolatban.



11. ábra Digitális adatvédelem a tanítása az iskolában

A kitöltők 2,2 csillagra értékelték az oktatás minőségét a digitális adatvédelem tanításával kapcsolatban. Ez a válasz is összhangban van a korábbi eredményekkel és azt tükrözi, hogy a kitöltők alapvetően elégedetlenek a digitális adatvédelem oktatásával kapcsolatban és magasabb szintű képzés részesei szeretnének lenni a kiberbiztonság ezen témakörében is.

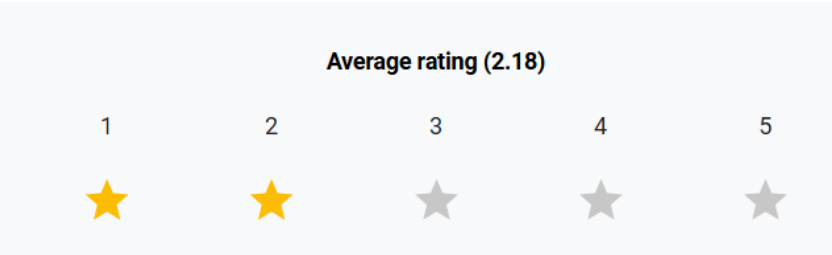
A következő, 11. ábra azt szemlélteti, hogy mennyire volt megfelelő az iskolai oktatás a jelszavak cseréjével, tárolásával kapcsolatban.



12. ábra Megfelelő oktatás a jelszavakkal cseréjével, tárolásával kapcsolatban

A kitöltők a lehetséges 5 csillagból 2,3 csillagra értékelték a jelszavak cseréjével, tárolásával kapcsolatos oktatást. Ez is tükrözi azt, hogy a NAT módosításra szorul a kiberbiztonság oktatásának témakörében. A kitöltők ezt értékelték a legmagasabb pontszámmal a minősítés típusú kérdések közül, de még ez az érték sem éri el a lehetséges 5 csillag felét sem.

A következő, 12. ábra azt szemlélteti, hogy mennyire volt megfelelő az iskolai oktatás a biztonságos online vásárlással kapcsolatban.



13. ábra Biztonságos online vásárlás feltételeiről való tanítás az iskolában

A biztonságos online vásárlással kapcsolatban kutattam, hogy tanórai kereteken belül volt-e szó a biztonságos online vásárlásról vagy az ehhez köthető biztonságos online banki tevékenységről. Ez az érték is csak épphogy eléri a 2-es szintet az 5-ből. Ez arra enged következtetni, hogy habár a legtöbb ember rendszeres, napi tevékenységei közé tartozik az online tranzakciók bonyolítása, mégsem oktatják ennek megfelelő módját tanórai keretek között. Az Alfa és a Z generáció válaszai alapján nincsenek eléggé felkészítve a biztonságos online vásárlásra intézményesített keretek között, hiányérzetük van és magasabb szintű oktatást szeretnének e tekintetben (is).

A válaszok összegzése és értelmezése során megállapítom, hogy az Alfa és a Z generáció nem kapott megfelelő oktatást intézményesített kereteken belül a kiberbiztonság témakörével kapcsolatosan. Nem került strukturált, több tanórán át tartó, egymásra épülő jelleggel oktatás az iskolában az elmúlt 5 évben a felelősségteljes, biztonságos felhasználással, adat kezeléssel és jelszóvédelemmel kapcsolatosan. A kitöltők válaszai alapján hiányérzet van bennük a kiberbiztonság oktatásával kapcsolatban, ami már legalább az elmúlt 5 évre visszanyúló jelenség.

Ezen vizsgálatok eredményeire alapozva, kutatásom 1. hipotézisét, mely szerint:

H1: Feltételezem, hogy a magyar közoktatás nem fordít elegendő figyelmet a kiberbiztonság témájára

elfogadottnak, beigazoltnak tekintem.

- A 2. hipotézisem vizsgálatához kapcsolódó kérdések és válaszainak elemzése:

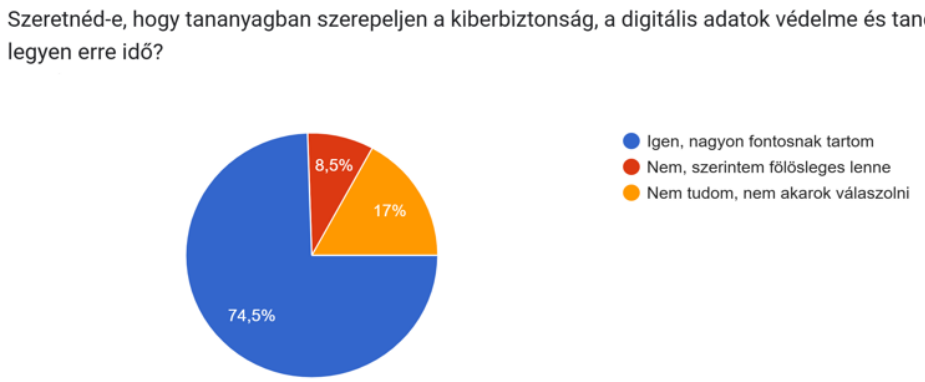
H2: Feltételezem, hogy a magyar közoktatásban nincs megfelelően felépített, naprakész tananyag kiberbiztonság témájában

A következő, 13. ábra azt szemlélteti, hogy a kitöltők hány százaléka kapott tankönyvet a kiberbiztonság témájával kapcsolatban az elmúlt 5 év során. A piros szín a „nem" választ jelöli az ábrán.

14. ábra Kapott tankönyvet az iskolában a kiberbiztonsággal kapcsolatban az elmúlt 5 évben

A kitöltők 77%-a azt választotta, hogy egyértelműen nem kapott semmilyen tananyagot a kiberbiztonság és a kibervédelem témakörével kapcsolatban. A kitöltők további 14%-a nem biztos benne, hogy kapott-e bármilyen tananyagot és összesen 9%, aki határozottan biztos abban, hogy kapott akár nyomtatott akár e-learning jellegű tananyagot az elmúlt 5 során. Ez egy óriási hiányosság és rendszerszintű probléma. Az Alfa és a Z generáció tagjai nem tudnak megfelelő, releváns és naprakész információt szerezni és azt kellő szinten elsajátítani, ha nincs ehhez biztosítva megfelelő tananyag. Az, hogy elhangzik egy órán, nem ad biztos alapokat a kiberbiztonság témájában. Egy esetleges kibertámadás során nehezebben tudnak releváns, szakmailag is megfelelő iránymutatás alapján cselekedni. Kénytelenek ebben az esetben a Google és a társak tanácsaira hagyatkozni, melyek relevanciája megkérdőjelezhető.

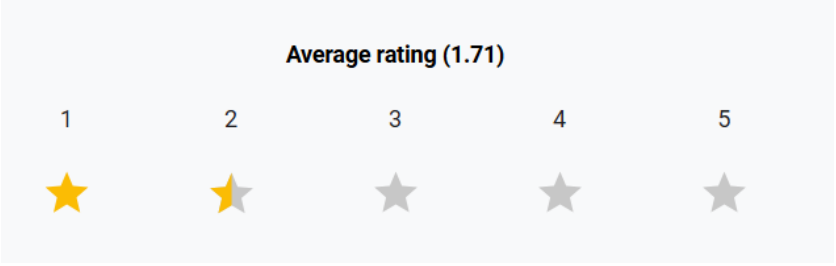
A következő, 14. ábra azt szemlélteti, hogy a kitöltők hány százaléka szeretné, hogy a tananyagban és a tanítási órán szerepeljen a kiberbiztonság témaköre. A kék szín az „igen, fontosnak tartom” választ illusztrálja.



15. ábra Szeretné, hogy szerepeljen a kiberbiztonság oktatása a tanórákon

A kitöltők közel 75%-a nagyon fontosnak tartja, hogy kellő hangsúlyt kapjon a kiberbiztonság oktatása a Nemzeti Alaptantervbe integráltan. Ez is azt mutatja, hogy az Alfa és a Z generáció tagjainak nagy igénye lenne a megfelelő oktatásra kiberbiztonság témakörében. A probléma jelentős része abból adódik, hogy a Nemzeti Alaptanterv elavult, nem veszi figyelembe a fiatalok igényeit az oktatás terén. Sok olyan témakört tartalmaz meglehetősen magas óraszámban a NAT, amire az életük során nagy valószínűség szerint sosem lesz szükségük, ugyanakkor a napi tevékenységükhöz elengedhetetlenül fontos kiberbiztonság megalapozására és készségszintű elsajátítására egyáltalán nem helyez figyelmet. Ezt részletesen a 3. fejezetben mutatom be.

A következő, 15. ábra egy minősítés típusú kérdést szemléltet, hogy mennyire volt elégedett a tankönyvekkel és oktató anyagokkal kapcsolatban, amiket az iskolában kapott.



16. ábra Elégedettség a tankönyvekkel kapcsolatban a kiberbiztonságról

Ennél a kérdésnél a korábbinál is lesújtóbb eredmények születtek. A magyar közoktatás a kiberbiztonsággal kapcsolatos tananyagok tekintetében megbukott az Alfa és a Z generáció körében.

A legtöbben nem kaptak semmilyen tananyagot, ami azért is jelent kiemelt kockázatot, mert sehol nem látják leírva, a legalapvetőbb biztonsági előírásokat, illetve nem tudnak elővenni egy tananyagot szükség szerint, ha problémájuk adódna a kibertérben. Elfogadom, hogy naprakész tananyagot készíteni a kibervédelemmel kapcsolatban, ahol turbulens változások történnek egyik napról a másikra nagy kihívást jelent. De az írott szónak bizonyítottan nagyobb hatása van az elménkre, mint ha csak egyszer meghallgatunk valamit pár percben. Még, ha bizonyos részek elévülnek is akár 1-2 év alatt, az alapvető és kiemelkedően fontos információk megmaradnak és tud hová lapozni a fiatal, ha valamilyen kérdés vagy probléma felmerül. Nem a neten kell kétes értékű információk között keresgélni, amivel esetlegesen csak még nagyobb bajt okoznak.

A kiberbiztonság oktatását nem lehet kizárólag főiskolai, illetve egyetemi szintre szorítani. Kifejezetten a fiatalabb korosztálynak van égetően szüksége a tudásra, hogy megóvják mentális jóllétüket. Ehhez szükség van egy strukturált, szakmailag jól felépített és ellenőrzött tananyagra, akár nyomtatott, akár elektronikus formában. Amiből tanulhat a gyerek és (jobb esetben) nem csak az órán hangzik el pár mondatban egy egészen apró része a kibervédelem átfogó témakörének.

Ezen vizsgálatok eredményeire alapozva, kutatásom 2. hipotézisét, mely szerint:

H2: Feltételezem, hogy a magyar közoktatásban nincs megfelelően felépített, naprakész tananyag kiberbiztonság témájában

elfogadottnak, beigazoltnak tekintem.

Fejezet végi összefoglalás

A kvalitatív kutatásban bemutattam a fókuszcsoportos interjúk eredményeit, illetve a digitális tantárgyat oktató pedagógusokkal készített mélyinterjúk összegzését. A kvalitatív kutatásra alapozottan építettem fel a kvantitatív kutatásomat, melyet kérdőíves megkérdezéssel készítettem hólabda mintavételi eljárással. Röviden összegezve az eredményeket elmondható, hogy az Alfa és a Z generáció tagjainak hiányérzetük van, a kiberbiztonság témakörének oktatásával kapcsolatban. Szeretnének többet tanulni az iskolában a tanórákon a biztonságtudatos digitális jelenléttel, a megfelelő jelszó kezeléssel és használattal, a biztonságos online vásárlással, biztonságos banki tevékenységekkel, kibertámadásokkal, vírusokkal és a kiber teret érintő minden fontos jelenséggel kapcsolatban. Nincsenek megelégedve az elérhető és számukra biztosított tananyaggal sem. Szükség lenne egy strukturált, szakmailag jól felépített és ellenőrzött tananyagra, amely lépésről felépítve végig kalauzolja a fiatalokat a fontosabb definíciókon, jelenségeken a kibervédelemmel kapcsolatban.

A szakmai mélyinterjúk készítése során, az általam megkérdezett oktatók közel felének a véleménye megegyezik az Alfa és a Z generáció véleményével és örömmel fogadnának egy ilyen jellegű kezdeményezést. Ezzel ellentétes vélemények is születtek a mélyinterjúk készítése során és a több, mint 20 év oktatási tapasztalattal rendelkező interjúalanyok szerint a 9. évfolyamtól kezdődően már szakirányú képzés történik és már célzottan a vizsgákra való felkészítés zajlik, feszített tempóban, amibe már nem férne bele külön több órás foglalkozás keretén belül a kibervédelem oktatása.

A kutatás eredményeinek függvényében mind a két hipotézisemet elfogadottnak tekintem.

✓ **H1:** Feltételezem, hogy a magyar közoktatás nem fordít elegendő figyelmet a kiberbiztonság témájára

✓ **H2:** Feltételezem, hogy a magyar közoktatásban nincs megfelelően felépített, naprakész tananyag kiberbiztonság témájában

3 BIZTONSÁGTUDATOSÍTÓ TANANYAGOK A KÖZNEVELÉSBEN

A kiberbiztonság és a tudatos online adatvédelem kialakítása és annak folyamatos naprakészen tartása nem egy adott szervezeten belüli feladat, hanem egy társadalmi ügy. Ehhez szükség van a családok és az oktatási intézmények közreműködésére is, hogy a gyermekkor mielőbbi szakaszában már biztonságtudatosságra szocializálják a gyermekeket. [81] Ennek fontos módja lenne, hogy a Nemzeti Alaptantervben megfelelő módon történjen meg a kiberbiztonság strukturált, gyakorlati tudást fókuszba helyező oktatása. A következőkben részletesen bemutatom, hogy hányadik évfolyamon milyen fő témakörök oktatása történik a NAT alapján és mely fontos készségek és definíciók tudására tesznek szert a különböző korosztályok tagjai.

A megfelelően felépített tantervnek kiemelkedő szerepe van. Egy jól átgondolt és megfelelően felépített tanmenet felkészíti a diákokat az adott tantárgy legfontosabb és legalapvetőbb tudnivalóira. A kiberbiztonság egy olyan téma, amelyre nem elég pár mondat erejéig kitérni a közoktatás során eltöltött 12 év alatt. A kibertámadások sokszínűek és turbulensen változnak. A kiberbűnözők kreativitása végtelen. A mai tudás 1 év múlva már elavult lesz. Ez a dinamikus változás már önmagában elég indok lenne arra, hogy minden tanévben több órán át tartó figyelmet szenteljünk a kiberbiztonság oktatására. Ezzel szemben a valóság az, hogy egyetlen évfolyamban sem kap a kiberbiztonság oktatása megfelelő figyelmet. Ahogy ebben a fejezetben részletesen bemutatom majd, nincs egyetlen olyan tanév sem, ahol a kiberbiztonság témaköre több órán keresztül strukturált tanmenetet követve oktatás tárgya lenne. Sőt, egyetlen tanóra sincs biztosítva konkrétan a kiberbiztonság témájában a Nemzeti Alaptantervben.

A problémát tovább nehezíti, hogy a fiatalokat oktató felnőttek jelentős hányada nem kapott semmilyen képzést kibervédelemmel kapcsolatban és nem ritka, hogy a tanárok gyakran maguk sincsenek tisztában nagyon fontos kiberbiztonsági óvintézkedésekkel. Így nehéz arról tanítani a fiatalokat, hogy mire figyeljenek oda digitális adataik védelme során.

A legalapvetőbb biztonsági óvintézkedések szabályai sincsenek tananyagban rögzítve, ezek az alapvetések pedig nem változnak az évek múlásával, például, hogy a jelszó ne az 1234 legyen, vagy hogy ne add ki a jelszavadat a barátaidnak. Ezek olyan alapvető biztonsági szabályok, amik nem évülnek el, mégis gyakori, hogy ez a problémák gyökere. Ezeket le lehetne írni tananyagban még akkor is, ha a kibervédelem számos más aspektusa turbulensen változik. A Nemzeti Alaptanterv tanulmányozása alapján ezek az egyszerű és örökérvényű szabályok el sem hangoznak egyetlen tanóra keretén belül sem. Vagy ha igen, az nagyban függ az oktató személyes preferenciájától.

A megfelelően felépített tanterv mellett az emberi attitűdnek is kiemelkedő szerepe van. A közoktatásban dolgozó pedagógusok hozzáállása nagy mértékben befolyásolja a fiatalok tantárgyhoz, sőt élethez való hozzáállását is. A gyarkolati tapasztalatom alapján a 9. évfolyamot kezdő fiatalok nincsenek nagyobb tudás birtokában programozás, programnyelvek és egyéb témákkal kapcsolatban sem, amiket viszont tartalmaz a NAT. Felmerül a kérdés, hogy akkor valójában miről tanulhatnak általában a 9. osztály előtt a gyerekek Digitális kultúra című tantárgy keretein belül. Feltételezem, ez nagyban függ a tárgyat oktató személytől. Van olyan fiatal, aki tanulta az Excel program használatát, sőt még egyszerűbb függvényeket is tud használni, de olyan tanuló is akad, aki megnyitáson kívül nem igazán tudja kezelni az Excel programot.

A tapasztalatok függvényében a tanárok többsége nem tartja be szigorúan a NAT-ban évi 16 órában meghatározott „robotika és kódolás alapjait” vagy az „algoritmizálás és blokkprogramozást” évi 11 tanórában. Ezek a témakörök a Nemzeti Alaptanterv magvas részét képezik. Ezt részletesen bemutatom a fejezet további részében. Míg ezek a témakörök igen jelentős óraszámmal szerepelnek a NAT-ban évfolyamról évfolyamra, a kibervédelem, kiberbiztonság témaköre egyetlen hivatalos órát sem kap. Egy külön kutatás témájául szolgálhatna, hogy a Nemzeti Alaptantervben szereplő témaköröket mennyire oktatják és mennyire tanulják meg a fiatalok a 8. évfolyam befejezését követően.

Az Alfa és a Z generációnál a legmegfelelőbb tanulási és tanítási forgatókönyv már nem tanár központú, hanem az aktív hallgatói tevékenységre és interakcióra helyezi a hangsúlyt. [82] Ez a korosztály már szeret tevékenyen részt venni a tanulásuk folyamatában, náluk már kevéssé opció az, hogy leülnek az asztalhoz és bemagolják a tanulnivalót. Ők szeretik a gyakorlati hasznát látni a tananyagnak és ennek megfelelően sajátítják is el a tudást.

A pedagógusoknak és a szülőknek kiemelkedő szerepe van a tudásalapú fejlődésben. Ehhez szükség van a pedagógusok tudományelméleti, kutatásmódszertani felkészültségére, illetve a folyamatos szakmai megújulásra. [83] A felnőttek nem tudnak segíteni a fiatal generáció tagjainak, ha ők maguk nem rendelkeznek megfelelő ismeretekkel a kiberbiztonsággal kapcsolatban. A jelenleg oktatói / pedagógusi státuszt betöltő emberek sem részesültek megfelelő oktatásban a kiberbiztonság alapjairól. Ez a mai napig nem változott. A megfelelő edukáció fontosságára már számos kutató felhívta a figyelmet.

Mógor Tamásné tudományos értekezésében megállapította, hogy megfelelő szintű képzés és oktatás nélkül az információbiztonság-tudatosság nem alakítható és fejleszthető. [50] Prof. Dr. Rajnai Zoltán Magyarország kiberkoordinátora, az Óbudai Egyetem általános Rektorhelyettese és a Biztonságtudományi Doktori Iskola egykori Vezetője, az Óbudai Egyetemen a Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar dékánja is többször hangoztatta, hogy kiemelt feladatnak tartja, hogy a kormányzat megfelelő figyelmet fordítson a gyermekek kibervédelmének oktatására. Illetve, hogy a kibervédelmi szempontból történő oktatást már óvodáskortól kell elkezdeni és a probléma megoldása társadalmi érdek. [84] [85] [5] [86]

Rajnai professzor szerint a biztonságtudatosság egy olyan erős követelmény ma már, aminek meg kell felelni életkori sajátosságoktól függetlenül. Fontos, hogy biztonságtudatos szinten üzemeltessük és használjuk a kiberteret. [87]

3.1 Különböző digitális órák a közoktatásban évfolyamonkénti bemutatásban

A teljesség igényére törekedve a következőkben részletesen bemutatom, hogy a Nemzeti Alaptantervben hogyan jelenik meg a digitális ismeretek, az online élet, a világháló minden aspektusával kapcsolatos tanítás és ezzel szoros kapcsolatban lévő kiberbiztonság oktatása (illetve annak hiánya) évfolyamokra bontva.

Először az 3-4. évfolyamban találkozunk bármilyen jellegű IKT tárgy oktatásával Digitális kultúra néven. [88] A Nemzeti Alaptantervben a további évfolyamokban is kizárólag Digitális kultúra néven történik IKT tárgy oktatása. Az alapóraszáma: 68 óra egy tanévre vonatkozóan. A tantárgy témaköreit az alábbi, 20. ábra szemlélteti:

A 3–4. évfolyamon a digitális kultúra tantárgy alapóraszáma: 68 óra.

A témakörök áttekintő táblázata:

Témakör neve	Javasolt óraszám
A digitális világ körülöttünk	6
A digitális eszközök használata	14
Alkotás digitális eszközökkel	18
Információszerzés az e-Világban	8
Védekezés a digitális világ veszélyei ellen	6
A robotika és a kódolás alapjai	16
Összes óraszám:	68

17. ábra A 3-4. évfolyam Digitális kultúra tantárgy: témakörök és óraszám
Oktatás. hu Digitális kultúra 3-4. évf.

Az egy tanévre vonatkozó teljes tanítási óraszám jelentős részét (16 óra), közel egy negyedét „A robotika és a kódolás alapjai” című témakör öleli fel. Ez az első olyan évfolyam, ahol a gyerekeknek tanmenetbe integráltan jelenik meg az online élet, a digitális világ, a világháló oktatásával kapcsolatos mindennemű fogalom, amelyet meg kell ismertetni a gyerekekkel. Az alapokat kezdjük el lehelyezni, amire a továbbiakban építeni lehet a tudást. A robotika egy nagyon fontos helyet foglal el a fiatal nemzedék oktatásában már a tantárgy bevezetésétől kezdődően, gyakorlatilag a teljes oktatásban eltöltött időre (a 12. évfolyamig) ez a struktúra a jellemző. Ezt a továbbiakban részletesen látni fogjuk.

A Nemzeti Alaptantervben 6 óra van meghatározva „védekezés a digitális világ veszélyei ellen” témakörben. Ez a következőket tartalmazza:

FEJLESZTÉSI FELADATOK ÉS ISMERETEK

- A személyes adat fogalmának értelmezése
- Az online zaklatás felismerése, a segítségkérés lehetőségeinek bemutatása és gyakorlása
- Közvetlen tapasztalatok szerzése az álhírekkel, manipulált képekkel, videókkal kapcsolatban
- Az online kommunikáció etikai és biztonsági szabályrendszerének bemutatása
- Az online függőség jellemzőinek ismerete
- A személyes adatok védelme
- A mobileszközök alkalmazásának előnyei és veszélyei

FOGALMAK

internetes zaklatás, internetfüggőség, játékfüggőség, álhír, blokkolás, kizárás, jelentés, bizalmas információk, jelszó, személyes adat

JAVASOLT TEVÉKENYSÉGEK

- Érvelés egy információ hitelességével kapcsolatban
- Példák gyűjtése az internetes zaklatások néhány megjelenési formájáról
- Szituációs játék eljátszása az internetes támadások, zaklatások esetén történő segítségkérés néhány formájáról
- Tanácsok megfogalmazása, napirend készítése a túlzott digitáliseszköz-használat ellensúlyozására, kiküszöbölésére
- Olyan érzékeny, személyes adatok megnevezése, melyeket fokozottan óvni szükséges a digitális kommunikáció során

18. ábra NAT témakörök részletezése 3-4. évfolyam
Oktatás. hu Digitális kultúra 3-4. évf

A Digitális kultúra tárgy a 3. évfolyamban jelenik meg először a kerettantervben. A magyarországi oktatási rendszerben egy harmadik osztályos tanuló általában 8-9 éves. Ennyi idős korukra a gyerekek már több száz vagy több ezer órát eltöltenek az online térben [89] [90] és ennyi idős korukban is csak 6 órát áldoznak a „digitális világ veszélyei”-nek az oktatásával kapcsolatban, ahol az internetes függőség, az online zaklatás, a személyes adat fogalmának a tisztázása foglal el 3 órát a 6 órából. Ezenkívül a fennmaradó 3 órában az online kommunikáció szabályrendszere, a mobileszközök alkalmazásának előnyei és hátrányai és az álhírek, manipulált képek és videók „közvetlen tapasztalat szerzése” áll.

Ezek valóban fontos témakörök. Ugyanakkor felmerül a kérdés, hogy elegendő-e és megfelelő-e ez a tanmenet egy 8-9 (gyakran 10) éves gyermek számára és valóban ezek-e a legfontosabb témakörök, amelyeket elsősorban meg kell ismertetni mindössze 6 órában egy tanév alatt. És ugyanennyi óraszámban jelenik meg, ugyanezzel a tantárgy címmel a 4. évfolyamban is az IKT oktatása. Amit fontos lenne tanítani azokat nem tartalmazza a tanmenet. Gondolok például a jelszóhasználatra, jelszavak cseréjének gyakoriságára, jelszóvédelemre, eszközvédelemre a vírusokra és egyéb kártevőkre, a

klónozott oldalak felismerésére, az internetes csalások és social engineer technikák egyéb módjaira.

A legutolsó 2020-as Nemzeti Alaptantervben az 5-6. évfolyamon az IKT oktatása továbbra is Digitális kultúra című tantárgyként kerül oktatásra és alapóraszáma: 68 óra egy tanévben. [91] A témaköröket és a javasolt óraszámokat a következő, 22. ábra szemlélteti:

Az 5–6. évfolyamon a digitális kultúra tantárgy alapóraszáma: 68 óra.

A témakörök áttekintő táblázata:

Témakör neve	Javasolt óraszám
Algoritmizálás és blokkprogramozás	14
Online kommunikáció	5
Robotika	11
Szövegszerkesztés	12
Bemutatókészítés	8
Multimédiás elemek készítése	8
Az információs társadalom, e-Világ	6
A digitális eszközök használata	4
Összes óraszám:	68

19. ábra Az 5-6. évfolyam Digitális kultúra tantárgy: témakörök és óraszám
Oktatás. hu Digitális kultúra 5-6. évf.

Az 5-6. évfolyamban már nem kap egyetlen óraszámot sem a kiberbiztonság, a digitális adatok védelme, a tudatos online jelenlét vagy bármi ehhez kapcsolódó témakör. Ugyanakkor olyan témakörök jelennek meg benne, mint az algoritmizálás és blokkprogramozás, ami a legmagasabb óraszámot kapta egy tanév során, összesen 14-et, illetve a Robotika évi 11 tanórával.

Ezt értelmezvén és némileg sarkítva elmondhatjuk, hogy a 11-12 éves kortól 13-14 éves korig a gyerekek a Nemzeti Alaptantervet követve semmilyen oktatásban nem részesülnek a kiberbiztonsággal kapcsolatban, ugyanakkor robotikát már tanítunk nekik (rendszerszinten). És, hogy valójában mit takar a robotika, az algoritmizáls és blokkprogramozás, illetve a táblázatban található többi témakör oktatása, a lényeget kiemelve és rövidítve, szemléltetem a következő ábrákon. (23. 24. 25. ábra)

TÉMAKÖR: Algoritmizálás és blokkprogramozás
JAVASOLT ÓRASZÁM: 14 óra

TANULÁSI EREDMÉNYEK

A témakör tanulása hozzájárul ahhoz, hogy a tanuló a nevelési-oktatási szakasz végére:

- érti, hogyan történik az egyszerű algoritmusok végrehajtása a digitális eszközökön;
- egyszerű algoritmusokat elemez és készít;
- ismeri a kódolás eszközeit;
- adatokat kezel a programozás eszközeivel.

A témakör tanulása eredményeként a tanuló:

- megkülönbözteti, kezeli és használja az elemi adatokat;
- ismeri és tanári segítséggel használja a blokkprogramozás alapvető építőelemeit;
- ismeri és használja a programozási környezet alapvető eszközeit;
- a probléma megoldásához vezérlési szerkezetet (szekvencia, elágazás és ciklus) alkalmaz a tanult blokkprogramozási nyelven;
- tapasztalatokkal rendelkezik az eseményvezérlésről;
- mozgásokat vezérel szimulált vagy valós környezetben.

FOGALMAK

algoritmus, folyamat, adat, adattípus, szöveges adatok, számok, bemenet, kimenet, problémamegoldó tevékenység, változó, algoritmus leírása, szekvencia, elágazás, ciklus, ciklusok fajtái, feltétel, algoritmustervezés, lépésenkénti finomítás elve, fejlesztői felület, blokkprogramozás, kódolás, tesztelés, elemzés, hibajavítás

20. ábra Algoritmizálás és blokkprogramozás témakör részletezése
Oktatás. hu Digitális kultúra 5-6. évf.

Az adatokat biztonságosan kezelni, kártevőket felismerni az online térben és egyéb, a hétköznapi tevékenységek során nélkülözhetetlen tudás átadására nem kerül sor, de algoritmus leírásra, szekvenciára, elágazásra és hasonlókra figyelmet fordítunk az Alaptantervben, tanévenként 14 órában. A témakörök súlyozását tekintve az online kommunikáció 5 tanóra, míg az algoritmizálás és blokkprogramozás 14 tanóra az 5-6. évfolyamban tanévenként. Ha jól tanultam statisztikából, akkor a súlyok nagysága egyenes arányban van a témák fontosságával. Itt elmondhatjuk, hogy 5 aránylik a 14-hez. Az online kommunikáció csúfos vereséget szenvedett az algoritmizálás és blokkprogramozás témakörével szemben, ami közel 3-szor annyi tanórán át kerül oktatásra a NAT alapján. Az egy másik vizsgálat tárgyát képzi, hogy egy 6. évfolyamot elvégzett fiatal, aki 28 órán tanulta az algoritmizálást és blokkprogramozást, vajon mennyi tudásra tett szert ebben a témakörben, melyre elég nagy hangsúlyt fektet a NAT.

Az online kommunikációra 5 tanórát szán a NAT egy tanév során. A témakör részletes bemutatása a következő:

TÉMAKÖR: Online kommunikáció

JAVASOLT ÓRASZÁM: 5 óra

TANULÁSI EREDMÉNYEK

A témakör tanulása hozzájárul ahhoz, hogy a tanuló a nevelési-oktatási szakasz végére:

- ismeri, használja az elektronikus kommunikáció lehetőségeit, a családi és az iskolai környezetének elektronikus szolgáltatásait;
- ismeri és betartja az elektronikus kommunikációs szabályokat.

A témakör tanulása eredményeként a tanuló:

- tisztában van a hálózatokat és a személyes információkat érintő fenyegetésekkel, alkalmazza az adatok védelmét biztosító lehetőségeket;
- önállóan kezeli az operációs rendszer mappáit, fájljait és a felhőszolgáltatásokat.

FEJLESZTÉSI FELADATOK ÉS ISMERETEK

- Online kommunikációs csatornák önálló használata, online kapcsolattartás
- Etikus és hatékony online kommunikáció a csoportmunka érdekében
- Online identitás védelmében teendő lépések, használható eszközök
- Adattárolás és -megosztás felhőszolgáltatások használatával

FOGALMAK

online identitás, e-mail, chat, felhőszolgáltatások, adattárolás, megosztás

JAVASOLT TEVÉKENYSÉGEK

- Elektronikus levél írása, üzenetküldő és csevegőprogram használata az elektronikus kommunikáció szabályainak betartásával
- Etikus és hatékony online kommunikáció az iskolai élethez és más tantárgyakhoz kapcsolódó csoportmunka érdekében
- Az adatok védelmét biztosító lehetőségek használata az online kommunikációs alkalmazásokban
- Személyes adatok, az iskolai élethez és más tantárgyakhoz kapcsolódó projektben adatok tárolása és megosztása a családi és az iskolai környezet elektronikus szolgáltatásai, felhőszolgáltatások segítségével

21. ábra Online kommunikácó témakör részletezése
Oktatás. hu Digitális kultúra 5-6. évf.

Az online kommunikácó témaköre az alábbiakat tartalmazza: Az adattárolás és -megosztás felhőszolgáltatások használatával, illetve az operációs rendszer mappáinak, fájljainak helyes kezelése, továbbá (a tanuló) ismeri és használja a családi és az iskolai környezetének elektronikus szolgáltatásait. Felmerült bennem a kérdés, hogy ezek a témák hogyan kapcsolódnak a kommunikáció címhez? Illetve online kommunikáció, mint fő témakör oktatása során ezek-e a legfontosabb területek? A NAT válasza erre egyértelműen az igen. Azt zárójelben jegyzem meg, hogy a 9. évfolyamba lépő fiatalok jelentős hányada nem tud önállóan mappát készíteni és elnevezni a Windows operációs rendszer asztalára.

A harmadik témakör a Digitális kultúra oktatásában az 5-6. évfolyamban a Robotika, melyre 11 óra a javasolt óraszám minden tanévben. A témakör részletes bemutatása a következő:

TÉMAKÖR: Robotika
JAVASOLT ÓRASZÁM: 11 óra

TANULÁSI EREDMÉNYEK

A témakör tanulása hozzájárul ahhoz, hogy a tanuló a nevelési-oktatási szakasz végére:

- ismeri és használja a blokkprogramozás alapvető építőelemeit;
- adatokat gyűjt szenzorok segítségével;
- mozgásokat vezérel szimulált vagy valós környezetben.

A témakör tanulása eredményeként a tanuló:

- ismeri és használja a blokkprogramozás alapvető építőelemeit.

FEJLESZTÉSI FELADATOK ÉS ISMERETEK

- Az algoritmikus gondolkodás fejlesztése
- Algoritmus készítése lépésekre bontással
- Algoritmusok megvalósítása, modellezése egyszerű eszközök segítségével
- A gyakorlati életből vett egyszerű problémák megoldása algoritmusok segítségével
- Robotvezérlési alapfogalmak
- Szenzorok, robotok vezérlésének kódolása blokkprogramozással
- Az együttműködési készség fejlesztése csoportos feladatmegoldások és projektmunkák során

FOGALMAK

robot, szenzor, algoritmus, blokkprogramozás, kódolás, vezérlés

JAVASOLT TEVÉKENYSÉGEK

- Alapszolgáltatásokat nyújtó program előállítása blokkprogramozás segítségével
- Blokkprogramozás használatával az események és azok kezelésének megismerése egyszerű játékok készítése kapcsán
- Robotok vezérlése blokkprogramozással
- Geometrikus ábrák útján mozgó robot programozása
- A környezeti akadályokra reagáló robot programozása

22. ábra Robotika témakör részletezése
Oktatás. hu Digitális kultúra 5-6. évf.

A kiberbiztonság oktatására ebben a témakörben sem kerül sor egyetlen tanóra keretéig sem. A robotokat vezérelni blokkprogramozással, geometrikus ábrák útján mozgó robot programozását, környezeti akadályokra reagáló robot programozását azonban évenként 11 órában tanítunk az 5-6. évfolyamba járó gyerekeknek. Ha egy pillanatra el tudunk vonatkoztatni attól, hogy mennyire fontos témákat előz meg ez a témakör és ha már ilyen témában szeretnénk, hogy a 12-13 évesek jártasak legyenek, akkor miért csak évi 11 órában tanítjuk nekik? Ha nagyon szeretnénk programozó zseniket nevelni, akik robotokat tudnak vezérelni, amik akadályokon átugranak és geometrikus ábrákon tudnak mozogni, akkor erre elég a 11 óra egy év alatt?

A Doktori Disszertációm terjedelmére vonatkozó korlátozásra való tekintettel, a következő 3 témakört, amely a Nemzeti Alaptanterv követelményében szerepel az 5-6. évfolyam oktatásában nem szemléltetem külön ábrán, csak felsorolás szintjén kívánok kitérni rá.

Ez a 3 témakör a következő:

- Szövegszerkesztés: 12 óra

- Bemutatókészítés: 8 óra

- Multimédiás elemek készítése: 8óra

Ezen témakörök oktatása kiemelten hasznos, bár a primer kutatásom során készített interjúalanyaim szerint a 9. évfolyamba érkező diákok gyakorlati tudása ezen témakörökben erősen hiányos. Úgy gondolom, célszerű lenne ezen témakörökre nagyobb hangsúlyt helyezni a közoktatás során. Több gyakorlatra szert tenni és ezen programok készségszintű használtát megtanítani, mert ezek a témakörök: Szövegszerkesztés, Prezentáció, Multimédiás anyagok készítése a tanulók életének további szakaszaiban (akár egyetemi tanulmányai tekintetében, akár munkavállalás tekintetében) is feltehetően nagy szerepet kapnak majd az Alfa és a Z generáció életében.

A legtöbb munkakör betöltéséhez már elengedhetetlenül fontos a Word, Power Point, Excel és hasonló szoftverek készségszintű használata. Ma már egy dokumentum elkészítése és formázása rutin műveletnek számít a legtöbb szakmai területen.

Az egyetemi szintű képzés során egyenesen elengedhetetlen ezen programok gyakorlati alkalmazása. Egy szakdolgozatot elkészíteni Word vagy egyéb szövegszerkesztő programok használata nélkül, mondhatni elképzelhetetlen. Ugyanez igaz a Power Point vagy egyéb prezentáció készítő szoftver használatával kapcsolatban. A szakdolgozat védéséhez is kell valamilyen „bemutató” program rutinszerű használata.

Ezen témakörök oktatása kiemelten hasznos és üdvözlendő.

A következő témakör a Digitális kultúra című tantárgy oktatásában az 5-6. évfolyamban: Az információs társadalom, e-Világ címet kapta, melyet tanévenként 6 órában kell tanítani a Nemzeti Alaptanterv előírása alapján. A témakör részletes bemutatását a következő ábra szemléltei:

TÉMAKÖR: Az információs társadalom, e-Világ
JAVASOLT ÓRASZÁM: 6 óra

A témakör tanulása eredményeként a tanuló:

- önállóan keres információt, a találatokat hatékonyan szűri;
- az internetes adatbázis-kezelő rendszerek keresési űrlapját helyesen tölti ki;
- ismeri az információs társadalom múltját, jelenét és várható jövőjét;
- védekezik az internetes zaklatás különböző formái ellen, szükség esetén segítséget kér.

FEJLESZTÉSI FELADATOK ÉS ISMERETEK

- Az információ szerepe a modern társadalomban
- Információkeresési technikák, stratégiák
- Adatok biztonságos kezelése, technikai és etikai problémák
- Az informatikai eszközök használatának következményei a személyiségre és az egészségre vonatkozóan

FOGALMAK

e-Világ; e-ügyintézés; virtuális személyiség; információs társadalom; adatbiztonság; adatvédelem; digitális eszközöktől való függőség

JAVASOLT TEVÉKENYSÉGEK

- Elektronikus levél írása hivatalos, iskolai, családi és baráti címzettnek
- Nyilvános és baráti fórumba hozzászólás, posztolás, mások hozzászólásának értékelése
- A családi és iskolai kapcsolatokban az elektronikus kommunikációs szabályok értékelése
- Az elektronikus kommunikáció gyakorlatában felmerülő problémák megismerése, valamint az ezeket megelőző vagy ezekre reagáló biztonságot szavatoló beállítások megismerése, használata
- Megfigyelések végzése és értelmezése a közösségi portálokon, keresőmotorok használata közben rögzített szokásokról, érdeklődési körökről, személyes profilokról
- Érdeklődési körnek, tanulmányoknak megfelelően információk keresése valamelyik keresőmotorban, és a találatok hatékony szűrése

23. ábra Az információs társadalom, e-Világ témakör részletezése
Oktatás. hu Digitális kultúra 5-6. évf.

Ez a témakör 6 órát kapott egy tanév során. Ebben a témakörben már szerepel az adatbiztonság és adatvédelem, olyan fogalmak mellett, mint a digitális eszközöktől való függőség, e-ügyintézés, virtuális személyiség, információs társadom. Mindezt évi 6 órában. És a NAT-ban rögzítették, hogy a témakör tanulása eredményeként a tanuló ismeri az információs társadalom múltját, jelenét és várható jövőjét. Az életünk minden területe hoz elképzelhetetlen változásokat. A digitális világ turbulens és elképesztő fejlődésének megjósolására azonban a NAT-ban meghatározott oktatás alapján külön tanórát kell szentelni.

Az utolsó nagy témakör az 5-6. évfolyamban A digitális eszközök használata, melyre 4 órát javasol a Nemzeti Alaptanterv. A Doktori Disszertációm terjedelmére vonatkozó korlátozásra való tekintettel, ezt a témakört nem szemléltetem külön ábrán, csak felsorolás szintjén kívánok kitérni rá. Operációs rendszer felhasználói szintű ismerete, mappa, fájl és felhőszolgáltatás kezelése, digitális hálózatok alapszolgáltatásai. A fogalmak között szerepel az adat, információ, hír, helyi hálózat, mappaműveletek, mobileszközök rendszere a teljesség igénye nélkül.

A Nemzeti Alaptanterv az 5-6. évfolyamban nem tartalmaz alapvetően fontos fogalmakat a kiberbiztonság oktatásával kapcsolatban. A kiberbiztonság nem is kapott helyet a 8 témakör között, amely szerepel a NAT-ban 2 tanéven át. Ezzel szemben az egyáltalán nem hétköznapi és gyakorlati haszonnal mérsékelten kedvező témakörök, mint a robotika, az algoritmizálás vagy a blokkprogramozás, elég jelentős óraszámot képvisel az 5. és 6. osztályban.

A legutolsó 2020-as Nemzeti Alaptantervben a 7-8. évfolyamon az IKT oktatása továbbra is Digitális kultúra című tantárgyként kerül oktatásra és alapóraszáma itt is: 68 óra. [91] A témaköröket és a javasolt óraszámokat a következő, 27. ábra szemlélteti:

7.-8. evf.

A 7–8. évfolyamon a digitális kultúra tantárgy alapóraszáma: 68 óra.

A témakörök áttekintő táblázata:

Témakör neve	Javasolt óraszám
Algoritmizálás és blokkprogramozás	15
Online kommunikáció	4
Robotika	8
Szövegszerkesztés	8
Bemutatókészítés	6
Multimédiás elemek készítése	6
Táblázatkezelés	12
Az információs társadalom, e-Világ	5
A digitális eszközök használata	4
Összes óraszám:	68

24. ábra Az 7-8. évfolyam Digitális kultúra tantárgy: témakörök és óraszám
Oktatás. hu Digitális kultúra 7-8. évf.

A Nemzeti Alaptantervben a 7-8. évfolyamban ugyanannyi óraszámban tanulnak Digitális kultúra tantárgyat a gyerekek, mint 5-6. évfolyamban. Az óraszámok elosztása változott és egy új témakör is szerepel a Táblázatkezelés 12 óra évenként. A továbbiakban a 7-8. évfolyam részletes bemutatásától eltekintek a nagyfokú egyezőségre való tekintettel.

A 8. évfolyamot követően a diákok különböző szakirányoknak megfelelően tudnak továbbtanulni. A különböző szakokon eltérőek az IKT tárgyához köthető tantárgyak nevei, témakörei és ajánlott óraszámai. A kutatás további részében a gimnáziumokra vonatkozó Kerettantervet mutatom be a 9-12. évfolyamok számára. [92]

Gimnáziumban továbbra is Digitális kultúra a tantárgy elnevezése amely kapcsoldóik a kiberbiztonság és az online jelenlét témájához.

A legutolsó 2020-as Nemzeti Alaptantervben az 9-10. évfolyamon az IKT oktatása továbbra is Digitális kultúra című tantárgyként kerül oktatásra és alapóraszáma: 102 óra. [92] A témaköröket és a javasolt óraszámokat a következő, 28. ábra szemlélteti:

A 9–10. évfolyamon a digitális kultúra tantárgy alapóraszáma: 102 óra.

A témakörök áttekintő táblázata:

Témakör neve	Javasolt óraszám
Algoritmizálás, formális programozási nyelv használata	25
Információs társadalom, e-Világ	3
Mobiltechnológiai ismeretek	4
Szövegszerkesztés	11
Számítógépes grafika	14
Multimédiás dokumentumok készítése	4
Online kommunikáció	4
Publikálás a világhálón	14
Táblázatkezelés	12
Adatbázis-kezelés	5
A digitális eszközök használata	6
Összes óraszám:	102

25. ábra Az 9-10. évfolyam Digitális kultúra tantárgy: témakörök és óraszám
Oktatás. hu Digitális kultúra 9-10. évf.

A Digitális kultúra tantárgyra, a korábbi évfolyamokból már ismerős témakör felosztás megmaradt, a javasolt óraszámok tekintetében történt változás és néhány új témakör került bevezetésre: Az Algoritmizálás témaköre megmaradt, de kiegészült a programozási nyelv használatával és 10-el több óraszámot kapott, mint 7-8. évfolyamban. Új témakör a Mobiltechnológiai ismeretek (4 óra), a Számítógépes grafika (14 óra), a Publikálás a világhálón (14 óra) és az Adatbázis-kezelés (5 óra). A továbbiakban ezt a 4 teljesen új témakört mutatom be. Az első ilyen bemutasára kerülő témakör a Mobiltechnológiai ismeretek, melynek javasolt óraszáma 4 óra tanévenként. A témakörök részletes leírását a következő, 29. ábra szemlélteti.

TÉMAKÖR: Mobiltechnológiai ismeretek
JAVASOLT ÓRASZÁM: 4 óra

TANULÁSI EREDMÉNYEK

A témakör tanulása hozzájárul ahhoz, hogy a tanuló a nevelési-oktatási szakasz végére:

– ismeri és használja a mobiltechnológiát, kezeli a mobileszközök operációs rendszereit és használ mobilalkalmazásokat.

A témakör tanulása eredményeként a tanuló:

– az applikációkat önállóan telepíti;
– céljainak megfelelően használja a mobileszközök és a számítógépek operációs rendszereit;
– az iskolai oktatáshoz kapcsolódó mobileszközökre fejlesztett alkalmazások használata során együttműködik társaival.

FEJLESZTÉSI FELADATOK ÉS ISMERETEK

– A mobiltechnológia körébe tartozó eszközök ismerete
– Mobileszközök kezelése, alkalmazások futtatása, telepítése, eltávolítása
– Mobileszközökre tervezett oktató- és oktatást segítő programok használata
– Mobiltechnológiai eszközök segítségével megvalósított együttműködés

FOGALMAK

mobiltechnológia, mobileszköz, alkalmazás, applikáció, alkalmazás telepítése, alkalmazás eltávolítása, kezelőfelület, oktatóprogramok, oktatást segítő programok, hálózati kapcsolat

JAVASOLT TEVÉKENYSÉGEK

– Tanulást segítő mobilalkalmazás választása, telepítése, eltávolítása
– Tantárgyi mobilalkalmazás indítása, használata, beállítása, paraméterek módosítása
– Projektfeladatok megoldása során a csapaton belüli kommunikáció megvalósítása mobileszközökkel

26. ábra Az 9-10. évfolyam Digitális kultúra tantárgy: Mobiltechnológiai ismeretek témakör részletezése
Oktatás. hu Digitális kultúra 9-10. évf.

Ez a témakör 4 órában kerül megtartásra a 9-10. évfolyamban a Nemzeti Alaptanterv előírása alapján. Ennek a tárgynak a segítségével képes lesz a tanuló önállóan telepíteni mobil applikációkat, céljainak megfelelően használja a mobileszközök és a számítógépek operációs rendszereit. A tanulási eredmény pedig, hogy kezeli a mobileszközök operációs rendszereit és használ mobilalkalmazásokat.

A Nemzeti Alaptanter a 15-16 éves korosztálynak tanítja meg a mobileszközök használatát és az appok letöltését. Ez a generáció már a kezében a telefonnal nő fel. Egészen kisded koruktól kezdődően ott van a kezükben a mindenféle okoseszköz. Ezt a tudást autodidakta módon már 1-2 éves korukban elsajátították, miközben az új és újabb játékokat töltötték le. Mikor még tisztán és érthetően beszélni sem tudtak, a telefonok és tabletek operációs rendszereit már készségszinten használták.

A kibervédelem továbbra sem szerepel a témakörök között, amelyről az oktatásban eddig egyetlen tanóra erejéig sem esett szó. A kiberbiztonság témaköre nem a napi szintű használat közben válik készségszintű tudássá. Ezért meg kell dolgozni, tenni kell a tudásért és a naprakész jelenlétért. Ez nem úgy működik, mint a játékok az appokban, hogy csak csinálom és valahogy továbbjutok a következő pályára és a sok gyakorlásnak köszönhetően egy idő után már profi játékossá válok. A kiberbiztonságról hallanunk kell. Foglalkoznunk kell vele. Sajnos egy nyűg. Oda kell figyelni, hogy milyen jelszavakat használunk, azokat cserélni kell bizonyos időközönként, önfegyelem kell hozzá, hogy mely linkekre ne kattintsunk rá azonnal bármilyen kecsegtető ígérettel bír is. Ezt mindenképpen tanítani kellene évről évre ismételni, frissíteni és átbeszélni a kiberbiztonsági óvintézkedéseket.

15-16 évesen már nagy hangsúlyt kellene kapnia a banki applikációs, a netes vásárlás, a biztonságos online banki tevékenységek témakörének is. Ebben a korosztályban (a felnőttkor küszöbén) már egyre gyakrabban fordul elő az online vásárlás önállóan. Többnyire már nem a szülők vásárolnak az ennyi idős fiataloknak, ezt már intézik ők maguk. És külön óraszámot vagy témakört szentelve ennek az oktatására sem kerül sor a Nemzeti Alaptantervben.

A következő új témakör amely megjelenik a Nemzeti Alaptantervben a 9-10. évfolyamban, a Számítógépes grafika oktatása évenként 14 órában. A tantárgy témaköreinek részletes bemutatását a következő, 30. ábra szemlélteti:

TÉMAKÖR: Számítógépes grafika
JAVASOLT ÓRASZÁM: 14 óra

TANULÁSI EREDMÉNYEK

A témakör tanulása hozzájárul ahhoz, hogy a tanuló a nevelési-oktatási szakasz végére:

- létrehozza az adott probléma megoldásához szükséges rasztergrafikus ábrákat;
- létrehoz vektorgrafikus ábrákat.

A témakör tanulása eredményeként a tanuló:

- tisztában van a raszter-, a vektorgrafikus ábrák tárolási és szerkesztési módszereivel.

FEJLESZTÉSI FELADATOK ÉS ISMERETEK

- Digitális képek jellemzőinek és tárolásának megismerése
- A rasztergrafikus kép jellemzői: felbontás, színmélység
- Rasztergrafikus rajzolóprogram használata
- Színrendszerek, alakzatok színezése, átlátszóság, takarás, vágás
- Dokumentumszerkesztő program alakzataival ábra készítése minta vagy leírás alapján
- Rasztergrafikus és vektorgrafikus ábra tárolási módszerének ismerete
- Alakzatok egymáshoz képest történő elrendezése: igazítás, elosztás, rétegek, transzformációk
- Vektorgrafikus szerkesztőprogram használata
- Alakzatok rajzolása: rajzolóeszközök, pont, szakasz, ellipszis, kör, téglalap
- Vektorgrafikus ábra elkészítése minta vagy leírás alapján
- Vektorgrafikus ábrakészítés algoritmikus tervezése
- Alakzat tulajdonságainak módosítása: méret, szegély, kitöltés, feliratozás, átlátszóság, transzformációk: elforgatás, tükrözés
- Alakzatok egymáshoz viszonyított elrendezése: igazítás, elosztás, rétegek, eltolás, forgatás, csoportosítás, kettőzés, klónozás
- Görbék, csomópontok felhasználása rajzok készítésében. Csomópontműveletek
- Raszter- és vektorgrafikus ábrák konverziója
- Elemi műveletek 3D-s modellel

27. ábra Az 9-10. évfolyam Digitális kultúra tantárgy: Számítógépes grafika témakör részletezése
Oktatás. hu Digitális kultúra 9-10. évf.

A NAT nem oktatja a kiberbiztonság témakörét, de a rasztergrafikus és vektorgrafikus rajzolómprogram használatát évi 14 órában 2 éven keresztül igen.

A következő új témakör a Publikálás a világhálón című témakör oktatása évi 14 órában. A tantárgy témaköreinek részletes bemutatását a következő, 31. ábra szemlélteti:

TÉMAKÖR: Publikálás a világhálón
JAVASOLT ÓRASZÁM: 14 óra

TANULÁSI EREDMÉNYEK

A témakör tanulása hozzájárul ahhoz, hogy a tanuló a nevelési-oktatási szakasz végére:

- ismeri a HTML formátumú dokumentumok szerkezeti elemeit;
- érti a CSS használatának alapelveit.

A témakör tanulása eredményeként a tanuló:

- dokumentumokat szerkeszt és helyez el tartalomkezelő rendszerben;
- több lapból álló webhelyet készít.

FEJLESZTÉSI FELADATOK ÉS ISMERETEK

- Egy webes tartalomkezelő rendszer önálló használata
- Webdokumentum szerkezetének és alapelemeinek ismerete
- Webdokumentum tartalmának és stílusának szerkesztési lehetőségei, szétválasztásuk jelentősége
- Közlésre szánt szöveges és képi információval kapcsolatos elvárások, kiválasztási szempontok, fájlformátumok
- Az internetes publikálás módszereinek megismerése, szabályai
- Szövegek, képek, fotóalbumok, hang- és videoanyagok, weblapok publikálása tartalomkezelő rendszerben
- Weblapkészítés HTML nyelven weblapszerkesztővel
- Stíluslap csatolása weblaphoz, és a benne lévő stílusok használata a dokumentum formázásához
- Összetett webdokumentum készítése

JAVASOLT TEVÉKENYSÉGEK

- Webes publikálásra szánt szöveges és képi információk előkészítése a tanuló érdeklődésének megfelelően választott témában
- Saját weboldal készítése webes tartalomkezelő rendszerben a tanuló érdeklődésének megfelelően választott témában
- Stílusokra épülő weboldalak szerkezetének közös elemzése
- Stíluslapot használó weboldal kinézetének módosítása a stíluslap cseréjével
- Az iskolai élethez vagy más tantárgyakhoz kapcsolódó, részletes feladatleírásnak megfelelő weboldal szerkezetének kialakítása kész stílusok felhasználásával
- Elkészített weblap internetes publikálása

28. ábra Az 9-10. évfolyam Digitális kultúra tantárgy: Publikálás a világhálón témakör részletezése
Oktatás. hu Digitális kultúra 9-10. évf.

Ebben a témakörben sem kapott semmilyen óraszámot a kiberbiztonság. Több lapból álló webhelyet tud készíteni a tanuló és ismeri a HTML formátumú dokumentumok szerkezeti elemeit, érti a CSS használatának alapelveit (mindezt 14 óra alatt!), de még ehhez a témakörhöz kapcsolatosan sem tartozik a kiberbiztonság -akár említésre méltóan- témaköre.

A utolsó új témakör az Adatbázis-kezelés évi 5 órában. A tantárgy témaköreinek részletes bemutatását a következő, 32. ábra szemlélteti:

TÉMAKÖR: Adatbázis-kezelés

JAVASOLT ÓRASZÁM: 5 óra

TANULÁSI EREDMÉNYEK

A témakör tanulása hozzájárul ahhoz, hogy a tanuló a nevelési-oktatási szakasz végére:

– strukturáltan tárolt nagy adathalmazokat kezel, azokból egyedi és összesített adatokat nyer ki.

A témakör tanulása eredményeként a tanuló:

– ismeri az adatbázis-kezelés alapfogalmait;
– az adatbázisban interaktív módon keres, rendez és szűr.

FEJLESZTÉSI FELADATOK ÉS ISMERETEK

– Strukturált adattárolás
– Adattípusok: szöveg, szám, dátum és idő, logikai
– Közérdekű adatbázisok elérése, adatok lekérdezése
– Szűrési feltételek megadása
– Hozzáférési jogosultság szerint adatlekérés, módosítás, törlés

FOGALMAK

adatbázis, adattábla, sor, rekord, oszlop, mező, adattípus, lekérdezés, jelentés; adattípusok: szöveg, szám, dátum, idő, logikai; szűrés, szűrési feltétel, logikai műveletek; hozzáférési jogosultság

JAVASOLT TEVÉKENYSÉGEK

– Adatok lekérdezése, szűrése és nyomtatása közérdekű adatbázisokból, például menetrendekből, kulturális műsorokból, védett természeti értékekből
– A hozzáférési jogosultságok elemzése az adatbázisokban, például az iskolai elektronikus naplóban, digitális könyvtárban, online enciklopédiában
– Az adatbázisokra épülő online szolgáltatások, például az e-kereskedelem lehetőségeinek kipróbálása, vita azok biztonságos használatának lehetőségeiről
– A biztonsági beállítások lehetőségeinek elemzése, azok hatása, majd vizsgálata a különböző közösségi médiumok mint online adatbázisok esetén

29. ábra Az 9-10. évfolyam Digitális kultúra tantárgy: Adatbázis-kezelés témakör részletezése
Oktatás. hu Digitális kultúra 9-10. évf.

Az Adatbázis-kezelés mely évi 5 órában történik, egy ennyi idős korosztálynak fontos tanulmánya a szövegszerkesztéshez és a táblázatkezeléshez hasonlóan. Bár évente 5 óra alatt nem lehet elsajátítani készség szinten még az alapokat sem.

A Nemzeti Alaptantervben továbbra sincs előírás a kiberbiztonság témájának oktatásával kapcsolatban.

A digitális adatok védelme, az adathalászat, a körültekintő online fizetés, a banki applikációk tudatos használata, álweboldalak felismerése, social engineer technikák ismertetése elengedhetetlenül fontos lenne. Ez a korosztály jelenti a tanköteles kor végét. Ideális esetben természetesen a fiatalok nem fejezik be a tanulást 10. osztályban, de ez nem egy ritka vagy példanélküli esemény. És úgy engedjük a felnőttkorba belépni a következő generációkat, hogy nem tanítjuk meg nekik az alapvető biztonsági lépéseket és óvintézkedéseket egy olyan területen, ahol szinte egész nap aktívan vannak jelen. Ezzel szemben rengeteg olyan dologra fordít időt a NAT, amely nemhogy nem a napi tevékenységük részét nem képezi, de sok esetben egész életük során nem lesz rá szükségük például algoritmizálás, weboldal készítés, rasztergrafikus és vektorgrafikus ábrázlási mód satöbbi.

A legutolsó 2020-as Nemzeti Alaptantervben a 11. évfolyamon az IKT oktatása továbbra is Digitális kultúra című tantárgyként kerül oktatásra és alapóraszáma: 68 óra. [92] A témaköröket és a javasolt óraszámokat a következő, 33. ábra szemlélteti:

A 11. évfolyamon a digitális kultúra tantárgy alapóraszáma: 68 óra.

A témakörök áttekintő táblázata:

Témakör neve	Javasolt óraszám
Algoritmizálás, formális programozási nyelv használata	20
Információs társadalom, e-Világ	4
Mobiltechnológiai ismeretek	4
Szövegszerkesztés	4
Online kommunikáció	2
Táblázatkezelés	12
Adatbázis-kezelés	20
A digitális eszközök használata	2
Összes óraszám:	68

30. ábra A 11. évfolyam Digitális kultúra tantárgy: témakörök és óraszám
Oktatás. hu Digitális kultúra 11. évf.

A Nemzeti Alaptantervben a 11. osztályban szerepel utoljára a Digitális kultúra című tantárgy oktatása. A 12. évfolyamban már nem szerepel.

A Digitális kultúra oktatása a 10. évfolyamban még 102 órában történt tanévenként. A 11. osztályban már csak 68 órát kapott a Digitális kultúra.

A tanmenet tükrözte az óraszám csökkenést: 3 témakört kivettek a tanmenetből.

Ez a 3 témakör a következő:

- Számítógépes grafika

- Multimédiás dokumentum készítése

- Publikálás a világhálón

A korábbi tanmenetekhez illeszkedve a 11. évfolyamban sem tanítják a kiberbiztonság témakörének bármely aspektusát. Az algoritmizálás és formális programozási nyelv használatának a tanítása közel a harmadát teszi ki a 11. osztályosok tananyagának a Nemzeti Alaptanterv szerint. A 11. évfolyam végeztével a fiatalok a 12. osztályban már nem tanulnak Digitális kultúrát, hanem készülnek az érettségire.

A 12. évfolyamot befejezvén megszerzik az érettségi bizonyítványukat és belépnek a felnőttkorba. Innentől a fiatalok egy része továbbmegy egyetemi képzésre, de nagyobb részük nem tanul tovább. Egyetemi oktatás során sem részesül a hallgatók többsége kibervédelmi oktatásban. Kizárólag azok tanulnak a továbbiakban a kiberbiztonság témájáról, akik ilyen irányú egyetemi képzésre jelentkeznek. És ott már nem az alapvető információkat oktatják, amelyeket a közoktatásnak kellett volna. A felsőoktatási színvonal már nem arról szól, hogy a jelszavad ne legyen 1234 vagy a kisállatod neve.

A közoktatásból kikerülő fiatalok úgy hoznak döntéseket, úgy válnak szülőkké vagy esetleg pedagógusokká, hogy semmilyen oktatásban nem részesültek kibervédelemmel kapcsolatban. És így kell majd tanácsot adniuk, felelősségteljes digitális életre nevelniük a gyermekeiket, a következő generációt. És így kerültek ki a közoktatásból a mai szülők és pedagógusok is.

Fejezet végi összefoglalás

Ebben a fejezetben részletesen bemutattam a Magyarországon érvényes Nemzeti Alaptantervben azt a tantárgyat, melynek keretében a kiberbiztonság oktatását lehetne és kellene oktatni. Ez az egyetlen tantárgy amely digitális és online élettel kapcsolatban oktatást biztosít 1-12-ig évfolyamig a gimnazista fiatalok számára. Digitális kultúra címmel került a NAT-ba.

Továbbá bemutattam, hogy hányadik osztályban milyen témaköröket ír elő a Nemzeti Alaptanterv a digitális tárgyak oktatásával kapcsolatban és hány órát szánnak az egy-egy adott témakörre. Részletesen rávilágítottam, hogy a kiberbiztonság, mint minden fontos ehhez kapcsolódó fogalmat felölelő témakör egyetlen évfolyamon sincs jelen a tanmenetben. A kiberbiztonság oktatására külön önálló tanórát nem biztosít a NAT egyetlen évfolyamban sem. Kizárólag a 3-4. évfolyamban jelenik meg a kiberbiztonság témájának néhány aspektusa, összesen 6 tanórát szánnak rá egy tanév alatt és elsősorban a netfüggőségre és az internetes zaklatásra helyezi a hangsúlyt a Nemzeti Alaptanterv. Egyetlen definíció a „személyes adatok védelme” jelenik meg a „védekezés a digitális világ veszélyei ellen” címet viselő témakörben. Jelszóvédelem, jelszavak kiadása-, tárolása- és cseréjével kapcsolatban itt sem történik rendszerszintű oktatásra való előírás, illetve ajánlás. Az üzenetben kapott linkekre való kattintás veszélyei, az áloldalak felismerése, a kétlépcsős azonosítás, a megfelelő eszközvédelem, a felelősségteljes online jelenlét, a biztonságos netbank használat, az óvintézkedések, a figyelmeztető jelek, a kibertámadás eseténi teendők még említés szintjén sem jelennek meg a NAT-ban. A rendszeres digitális jelenlét, az okoseszközök napi, rutinszerű használata életünk minden területét átszövik. Ez a jelenség bár napról napra fokozódik, nem újszerűen keletkezett. Már több, mint 2 évtizede életünk szerves részét alkotja. Ennek ellenére a Nemzeti Alaptantervben még mindig nincs egyetlen témakör sem, mely a kiberbiztonsággal foglalkozna széleskörűen, strukturáltan, naprakész információkkal.

A 9. évfolyamtól kezdődően nem tértem ki külön a szakgimnáziumok és szakiskolák által nyújtott digitális oktatásra, csak a gimnazisták tanmenetét vizsgáltam a Nemzeti Alaptanterv tükrében. Ennek oka azzal magyarázható, hogy nagyon sokféle szakirány oktatása történik napjainkban Magyarországon és a kifejezetten digitális irányultságú oktatástól eltekintve a többi középszintű oktatás feltételezhetően alacsonyabb színvonalat biztosít a tanulók számára, mint a gimnázium oktatás.

A Nemzeti Alaptanterv tanulmányozása során, az is említésre méltó jelenség számomra, hogy mennyire sajátos módon került meghatározásra a különböző témakörök oktatása. Nem találtam magyarázatot arra vonatkozóan, hogy miért kell ilyen magas óraszámban oktatni az algoritmizálást, a programozási nyelveket, a robotikát, blokkprogramozást, a kódolást, a számítógépes grafikát. Ezek a témakörök igen magas óraszámban szerepelnek szinte minden évfolyamon a tanmenetben. Úgy gondolom, hogy egy nagyon erős alapozást kellene adni a fiataloknak az eszközhasználat és a felelősségteljes digitális élet tekintetében. Akit érdekel a programozás, annak pedig számos lehetősége van, ilyen irányú továbbtanulásra, illetve fakultatív órákra. Egy kicsit számomra ez olyan érzést kelt, mintha egy írni-olvasni nem tudó gyermekkel elemeznénk egy szakirodalmi alkotást.

Disszertációm témája a kiberbiztonság tudatosításának az oktatása az Alfa és a Z generáció korosztályában, ugyanakkor meg kell jegyeznem, hogy a 9. évfolyamba lépő gyerekek jelentős hányada nem tud olyan alapvető dolgokat önállóan megcsinálni a digitális térben, mint egy üres mappát létrehozni az asztalra és elnevezni megadott névre. Ezek a fiatalok, 9-es évfolyamba lépésükkör már 408 órát (6x68 óra a 3-tól 8-ig évfolyamig) töltenek el Digitális kultúra című tanórán. Mégis az egészen minimális szintű tudásuk terén is aggasztóan magas arányban vannak jelen hiányosságok. Ehhez kapcsolódóan felmerül bennem a kérdés, mely természetesen költői, hogy nem lenne-e célszerűbb, ha a Nemzeti Alaptantervben az igazán fontos alapok oktatására fordítanánk a hangsúlyt. Egy 9. évfolyamba lépő fiatalnak már ne kelljen ott kezdeni az oktatását, hogy hogyan készítünk mappát, nevezünk el egy fájlt, illetve, hogyan kell felelősségteljesen bánni (és kezelni) a digitális adatainkkal az online térben. Hiszen ennyi idősen már komoly tapasztalat áll a hátuk mögött, melyet a digitális világban töltöttek el és ahol rengeteg információt tárolnak és osztanak meg privát életükről.

ÖSSZEGZETT KÖVETKEZTETÉSEK

A HOLNAP SZAKEMBEREIT A MA OKTATÁSA BIZTOSÍTJA

A mostani Alfa és Z generáció szülöttei – azok, akik jelenleg is a közoktatás résztvevői – kezében lesz néhány évtizeden belül az országunk, nemzetünk jövője. Vajon mennyire erős alapot kapnak a jelenlegi fiatal generáció tagjai kiberbiztonság tudásuk tekintetében?

Több éve foglalkozom oktatóként és anyaként Alfa és Z generációba tartozó fiatalokkal. Személyes tapasztalataim alapján, alapvető hiányosságokra lettem figyelmes.

A személyes adatvédelem és információmegosztás több aspektusa tekintetében is magas fokú hiányosságok és alapvető biztonsági óvintézkedések hiányát állapítottam meg.

A doktorandusz éveim során, az elmúlt években több irányból is végeztem kutatásokat arra vonatkozóan, hogy az Alfa és a Z generáció milyen mélységben tanul a kiberbiztonság fontosságáról. Azt feltételeztem, hogy az adatvédelemmel és a kiberbiztonsággal kapcsolatban nem tanulnak kellő mélységben a fiatalok általános és középszintű oktatásuk során. A feltételezésem beigazolódott, sőt mondhatni igazán elszomorító tényekkel szembesültem.

A Nemzeti Alaptantervben egyetlen évfolyamban sem szerepel a kiberbiztonság témaköre. Tovább súlyosbítja a helyzetet, hogy egyetlen külön tanórát sem szentelnek a NAT-ban a kiberbiztonság oktatására a teljes középszintű oktatás befejezéséig, azaz a 12. évfolyamig. Nincs olyan tanóra, amikor strukturáltan végig vezetnék a fiatalokat a megfelelő erősségű jelszavak, a jelszavak időszakos cseréjének fontossága, a jelszavak megfelelő tárolása, az ál weboldalak felismerése, a biztonságos online banki tevékenységek, a biztonságos online vásárlás, az elektronikus eszközök védelme és egyéb kibervédelemhez köthető témákon.

Nincsen megfelelő tananyag, sőt leginkább semmilyen tananyag a 12 év alatt, amit a közoktatásban eltöltenek. További nehezítő körülmény, hogy turbulens változásoknak köszönhetően nagyon nehéz az ilyen irányú tudást naprakészen tartani. Ugyanakkor fontos kiemelni, hogy az alapvető biztonságtudatos és felelősségteljes viselkedés szabályai sincsenek oktatva, sem pedig tananyagban rögzítve, ezek az alapvetések pedig nem változnak az évek múlásával.

Fontosnak tartom, hogy a különböző digitális jellegű tárgyak oktatására szakosodott pedagógusok is naprakész információkkal rendelkezzenek. Ehhez fontos lenne egy rendszerszinten bevezetett edukáció, mely kifejezetten a IKT tárgyakat oktató szakemberek továbbképzésére alakítottak ki.

Ezeken túlmenően fontosnak tartom, hogy minden egyes oktató részesüljön kifejezetten kibervédelemmel kapcsolatos edukációban legalább 2-3 évenként.

Ez az intézkedés egyrészről azt szolgálná, hogy a kiberbiztonság témáját napirenden tartaná, másrészt a pedagógusok felkészültebbek lennének kibervédelmi kérdések tekintetében. Ez azért is annyira jelentős, mert a fiatalok elsősorban olyan felnőttől fogadnak el intelmet, akiben bízni tudnak, akihez érzelmileg közelebb állnak és ez a személy nem feltétlenül a Digitális kultúra tárgyat oktató személy.

Ehhez elengedhetetlen lenne, hogy az oktatásban minden résztvevő megfelelő, naprakész tudással rendelkezzen a kiberbiztonság legfontosabb aspektusainak a tekintetében. Amíg az oktatók jelentős hányada nem rendelkezik az online adatok védelmével kapcsolatos alapvető jártassággal és tudással, addig nem tudnak érdemben segíteni a fiataloknak ebben a témakörben. És nulladik lépésként kiemelten fontos lenne az osztályfőnökök számára kibervédelmi edukálást biztosítani.

Az osztályfőnökök személye az, aki jobban részese tud lenni egy gyermek magánéletének. Ők azok, akik jobban belelátnak a gyermekek családi életébe is. Ezért gondolom, hogy hasznos lenne mindenekelőtt az osztályfőnököket felkészíteni, hogy hasznos segítséget tudjanak nyújtani egy fiatalnak, ha esetlegesen kibertámadás áldozatává válnak. A digitális adatok védelméről, a felelősségteljes online jelenlétről, a biztonságtudatos felhasználói magatartásról osztályfőnöki óra keretén belül is kellene tanórát elkülöníteni.

SUMMARY

TOMORROW'S PROFESSIONALS ARE PROVIDED BY TODAY'S EDUCATION

The current generation of Z and Alpha - those who are currently participating in public education - will have the future of our country and nation in their hands in a few decades. How strong a foundation will the members of the current young generation receive in terms of their cybersecurity knowledge?

I have been working with young people belonging to the Z and Alpha generations as an educator and mother for several years. Based on my personal experience, I have become aware of fundamental shortcomings.

I have identified a high degree of shortcomings and a lack of basic security precautions in several aspects of personal data protection and information sharing.

During my doctoral studies, I have conducted research from several directions in recent years on the depth of understanding of the importance of cybersecurity among Generation Z and Alpha. I assume that young people do not learn enough about data protection and cybersecurity during their primary and secondary education. My assumption was confirmed, and I was confronted with some truly sad facts.

The National Core Curriculum does not include cybersecurity in any grade. The situation is further aggravated by the fact that not a single lesson is dedicated to cybersecurity education in the NAT until the completion of the entire secondary education, i.e. until the 12th grade. There is no lesson that would guide young people in a structured way through the use of passwords of appropriate strength, the importance of periodically changing passwords, proper storage of passwords, recognizing fake websites, safe online banking, safe online shopping, protecting electronic devices and other topics related to cybersecurity.

There is no adequate curriculum, or rather no curriculum at all, during the 12th grade that they spend in public education. Another complicated factor is that due to turbulent changes, it is very difficult to keep such knowledge up to date. At the same time, it is important to highlight that the basic rules of safety-conscious and responsible behavior are neither taught nor recorded in the curriculum, and these fundamentals do not change over the years.

I believe it is important that teachers specializing in teaching various digital subjects also have up-to-date information. For this, it would be important to introduce education at a systemic level, specifically designed for the further training of professionals teaching ICT subjects.

In addition to this, I consider it important that each instructor receives specific cyber security-related education at least every 2-3 years.

This measure would, on the one hand, serve to keep the topic of cybersecurity on the agenda, and on the other hand, teachers would be better prepared regarding cybersecurity issues. This is also so significant because young people primarily accept advice from adults they can trust, to whom they are emotionally closer, and this person is not necessarily the person teaching the Digital Culture subject.

To achieve this, it would be essential for all participants in education to have adequate, up-to-date knowledge about cybersecurity. As long as a significant proportion of educators do not have the basic skills and knowledge related to online data protection, they will not be able to help young people in this area in a meaningful way. And as a zero step, it would be particularly important to provide cybersecurity education for class teachers.

Class teachers are the ones who can be more involved in a child's private life. They are the ones who can also see into the children's family life better. That is why I think it would be useful, above all, to prepare class teachers so that they can provide useful help to a young person if they become a victim of a cyberattack. A separate lesson should be given within the class teacher's lesson on the protection of digital data, responsible online presence, and safety-conscious user behavior.

Új tudományos eredmények

Kutatásomban **igazoltam**, hogy a magyar közoktatás nem fordít elegendő figyelmet a kiberbiztonság tudatosításának témájára, **illetve azt is bizonyítottam**, hogy a magyar közoktatásban nincs megfelelően felépített, naprakész tananyag kiberbiztonság témájában.

Ennek a két hipotézisnek a vizsgálatához először szekunder adatgyűjtést végeztem és törekedtem arra, hogy minden releváns és naprakész publikációt felleljek a témához kapcsolódóan. Számos kiemelkedő kutató értékes munkáját tanulmányoztam munkám során. Kutatást végeztem a különböző generációk tekintetében, megfogalmaztam hasonlóságokat és különbséget és magyarázatul szolgáltam arra vonatkozóan, hogy miért éppen az Alfa és a Z generáció áll a kutatásom fókuszában. Megvizsgáltam az online tér biztonságos alkalmazására bevezetett jogszabályokat hazai és nemzetközi kitekintésben is.

A szekunder kutatás után primer kutatást végeztem, ahol a teljesség igényét szem előtt tartva minden érintett oldalról megvizsgáltam a kiberbiztonság oktatását. Először kvalitatív kutatást készítettem. Egyrészt mélyinterjúk keretein belül oktató szakembereket kérdeztem a kiberbiztonság oktatásával kapcsolatos személyes tapasztalataikról, másrészt Alfa és Z generációba tartozó fiatalokkal készítettem fókuszcsoportos megkérdezést a kiberbiztonság oktatásával kapcsolatban.

A kvalitatív kutatás eredményeire alapozva készítettem kvantitatív kutatást, kérdőíves megkérdezés formájában. A kérdőívben szélesebb körben értem el a kutatásom célcsoportjába tartozó Alfa és Z generációs fiatalokat. Így nagyobb mintaelemszám alapján tudtam vizsgálni a véleményüket és tapasztalataikat a kiberbiztonság tudatosításának oktatásával kapcsolatban. A kitöltés hólabda mintavételi eljárással, önkéntes kitöltési alapon történt Google Forms felületen.

A kutatásom következő fázisában a Nemzeti Alaptantervet vizsgáltam meg, kiberbiztonság oktatása szempontjából. Évfolyamonkénti felosztásban **bemutattam**, hogy mely nagy témakörökre bontva, hány órát áldoz a NAT a Digitális kultúra oktatására. Azért csak ezt a tantárgyat vizsgáltam, mert ez az egyetlen olyan tárgy, amelynek keretein belül a kiberbiztonság tudatosítása, illetve oktatása alapot képezhetne. A vizsgálat során fény derült rá, hogy a kiberbiztonság témaköre egyáltalán nem szerepel

egyetlen évfolyam tanmenetében sem, elsőtől tizenkettedik évfolyamig. Nem csak témakörként, de egyetlen konkrét órai tananyagként sem szerepel a kiberbiztonság a Nemzeti Alaptantervben.

A primer kutatás eredményeként megállapítottam, hogy a fiatalok nem részesültek megfelelő közoktatásban a kiberbiztonság témakörében. Tananyagot nem kaptak kiberbiztonság témájához kapcsolódóan. A fiatalokban hiányérzet van, szerettek volna intézményesített keretek között szakoktatásban részesülni kibervédelem témájában. Szerettek volna tanyagot kapni akár elearning, akár nyomtatott könyv formájában. Érzik a hiányt, amelyet a közoktatásnak a felelőssége lenne kitölteni. Sok esetben a felnőttek megfelelő edukálása sem történt meg kiberbiztonsági vetületben, ez további nehezítő tényezőt jelent a fiatalok számára.

A jövőre vonatkozóan a kutatásomra alapozottan szívesen részt vennék egy konkrét, jól strukturált, átfogó tananyag kidolgozásában 1-12. évfolyamig, ahol az IKT tantárgy innovatív tantervét kidolgozhatnám, elérhető és naprakész tananyagot állíthatnék össze más kollégákkal közösen. Úgy gondolom, hogy az elmúlt években szerzett tapasztalataim segítségével mélyebb bepillantást nyerhettem az Alfa és a Z generáció életébe, egyetemi és középszintű oktatási tapasztalataim alapján egy gazdagabb, gyakorlatibb tanmenet kialakítását segíthetném elő és igazán szívügyemnek tekintem a kiberbiztonságot éppúgy, mint a fiatal nemzedékek tudásának bővítését.

Ajánlások

Ajánlom kutatásomat leginkább olyan szakembereknek, akik érdemben tehetnek a magyar közoktatás színvonalának emelése érdekében, kifejezetten a digitális oktatásra való tekintettel. Nagyon szívesen adom át a tapasztalataimat és örömmel részt veszek bárminemű fejlesztéssel kapcsolatban, melynek segítségével hasznos, naprakész és valóban gyakorlat orientált képzésben részesíthetjük a mai fiatalokat, akik a holnap szakemberei lesznek. Hiszem, hogy Nemzetünk jövője nagyban függ a közoktatásunktól. Ahogy többször is leírtam disszertációmban, hiszem, hogy **a holnap szakembereit a ma oktatása biztosítja**.

Kutatásomat ajánlom továbbá a közoktatásban minden szakembernek, aki érintett a digitális oktatásban bármely évfolyamon. Hasznos lehet, ha a Digitális kultúra tárgyat oktató pedagógus tisztában van a Nemzeti Alaptantervben meghatározott témakörökkel és óraszámokkal minden évfolyam tekintetében. Ez talán némi magyarázattal szolgálhat arra vonatkozóan, hogy miért lehet létező jelenség az alaptudás hiánya a fiatal korosztályban.

A közoktatásra nem csak, mint rendszerszinten jelenlévő jelenségre és a Nemzeti Alaptantervre, hanem mint Emberekre gondolok, nagy „E” betűvel, akik munkájuk során kapcsolatba kerülnek a fiatalokkal és akik kezében van a mentális jól-létük, melyet nem kizárólag kibervédelemi aspektusok tekintetében értek.

Véleményem szerint a gyakori dicséret, az önbizalom növelése egy mentálisan egészségesebb társadalmat eredményez, mint a poroszos jellegű oktatásra jellemző megszégyenítés, megfélemlítés vasökle. Ebben segíteni nem a NAT módosításával, nem új törvények vagy szabályok alkalmazásával lehet, hanem kizárólag az emberi értékek tiszteletben tartásával, egymás iránti figyelmességgel és a fiatalokkal, mint egyenrangú partnerekkel való bánásmóddal lehet. Ez kizárólag az oktatók személyes attitűdjén múlik. És úgy tapasztalom, hogy felsőoktatásban, az egyetemi közegben már sokkal jellemzőbb jelenség a tisztelet és egyenlő bánásmód, mint az egyetemi éveket megelőzően.

Kutatásom eredményeit ajánlom továbbá minden kutatónak, aki az Alfa és / vagy a Z generációt kutatja. Disszertációmban hasznos adatokra lelhet e két generáció digitális oktatásával, online életük bizonyos aspektusaival kapcsolatban.

Azon kutatóknak is ajánlom, akik a kiberbiztonság témájában végeznek vizsgálatokat. A szakirodalmi kutatásom kiterjed a kibervédelem hazai és nemzetközi jogszabályainak vizsgálatára és számos social engineer technikát bemutattam.

Kutatómunkám eredményeit jó szívvel ajánlom minden egyes hétköznapi embernek, aki élete során kapcsolatba kerül fiatalokkal akár mint szülő, akár mint oktató. Ha rendszerszinten lassabban is megy végbe a változás, hiszem, hogy magánemberként nagyon sokat segíthetünk a körülöttünk élőkön. Bátorkodom a korábbi kijelentésemet fokozni azzal, hogy nem csak a fiatalokkal kapcsolatban segíthetünk egymásnak a digitális adataink magasabb fokú védelmének kialakítása során. A disszertációmban mutattam be olyan esettanulmányt is, ahol felnőtt, nem mellesleg diplomás, értelmiségi felnőttnek voltak komoly hiányosságai alapfokú adatvédelemmel kapcsolatban. Ha vesszük a fáradságot és a körülöttünk élőkre nagyobb figyelmet fordítunk, feltételezem, hogy találunk olyat személyes ismerőseink között is, aki hálás szívvel hallgatna meg, néhány alapvető biztonsági óvintézkedésre intő tanácsot.

IRODALOMJEGYZÉK

[1] C. Skouloudi és E. Kantas, „Cybersecurity education maturity assessment,” ENISA, EU, 2024.

[2] ENISA, „Network Information Security in Education,” ENISA, EU, 2012.

[3] P. Anderson, S. DE Paoli és D. CATALUI, „Status of privacy and NIS course curricula in Member States, published education,” ENISA, EU, 2015.

[4] K. R. Szűcs, „Biztonsági kockázatok csökkentése a mindennapokban,” in *Kiberbiztonság - Cybersecurity 2.*, R. Zoltán, Szerk., Budapest, Biztonságtudományi Doktori Iskola, 2019, pp. 82-94.

[5] P. D. R. Zoltán, Interviewee, *Prof. Dr. Rajnai Zoltán - interjú.* [Interjú]. 09 2017.

[6] C. Bakewell és W. Mitchell, „Generation Y female consumer decision-making styles,” *International journal of retail & distribution management,* %1. kötet31 (2), pp. 95-106, 2003.

[7] N. Howe és W. Strauss, Millenial rising: The next great generation, Vintage, 2009.

[8] M. Törőcsik, K. Szűcs és D. Kehl, „Generációs gondolkozás a Z és az Y generáció életsítlus csoportjai,” *Marketing & Menedzsment,* %1. kötetII. különszám, pp. 3-15, XLVIII. évfolyam 2014.

[9] M. Törőcsik, K. Szűcs és D. Kehl, „How generation think: research on generation Z.,” *Acta universitatis Sapientiae,* pp. 23-45, 2014.

[10] V. Tamás, Érzelmi biztonság, Budapest: Kulcslyuk Kiadó, 2011.

[11] V. Tamás, Jól szeretni Tudod-e, hogy milyen a gyereked?, Budapest: Kulcslyuk Kiadó, 2013.

[12] S. Krisztián, „Mindent a generációkról 1. rész,” Friderikusz podcast, 2025.

[13] N. Howe és W. Strauss, „The new generation gap,” *Atlantic Boston ,* %1. kötet270, pp. 67-67, 1992.

[14] I. Agárdi és M. Alt , „A mobiltárca elfogadásának generációs különbségei: az X és Z generáció összehasonlítása,” *Statisztikai szemle,* %1. kötet90 (11), pp. 1049-1079, 2021.

[15] H. Schuman és J. Scott, „Generations and collective memories,” *American Sociological review,* pp. 359-381, 1989.

[16] A. Bencsik, G. Horváth-Csikós és T. Juhász, „Y and Z generations at Workplaces,” *Journal if Competitiveness,* %1. kötet8.3, 2016.

[17] A. Joshi, J. Dencker és G. Franz, „Generations in organisations,” *Research in organisational behavior 31.,* pp. 177-205, 2011.

[18] B. Meretei, „Generációs különbségek a munkahelyen - Szakirodalmi áttekintés,” *Vezetéstudomány-Budapest Management Review,* pp. 10-18, 2017.

[19] T. Juhász, C. Czeglédi és E. Varga, „Különböző generációk a munkahelyeken,” *Közösségi kapcsolódások-tanulmányok kultúráról és oktatásról,* %1. kötet3 (2), pp. 74-83, 2023.

[20] Z. Kőműves, L. Palmai, P. Kovács-Kósa és G. Szabó-Szentgróti, „Generációs különbségek elemzése a versenyszférában,” *Új Munkaügyi Szemle,* %1. kötet4, 2023.

[21] G. Callanan és J. Greenhaus, „The baby boom generation and career management: A call to action,” *Advances in Developing Human Resources,* %1. kötet10 (1), pp. 70-85, 2008.

[22] J. Westerman és J. H. Yamamura, „Generational preferences for work environment fit: effects on employee outcomes,” *Career Development International,* %1. kötet12(2), pp. 150-161, 2007.

[23] B. Kupperschmidt, „Multigeneration employees: Strategies for effective management,” *The healt care manager,* %1. kötet19(1), pp. 65-76, 2000.

[24] A. Tari, Y generáció, Budapest: Jaffa, 2010.

[25] R. Rodriguez, M. Green és M. Ree, „Leading Generation X: Do the old rules apply?,” *Journal of Leadership & Organizational Studies,* %1. kötet9(4), pp. 67-75, 2003.

[26] J. Vázquez de Príncipe, Resilience of Multicultura and Multigenerational Leadership and Workplace Experience, IGI Global, 2024.

[27] M. Prensky, „Digital natives, digital immigrants part 2: Do they really think differently?,” *On the horizon,* %1. kötet9(6), pp. 1-6, 2001.

[28] A. Tari, Y generáció. Klinikai pszichológiai jelenségek és társadalomlélektani összefüggések az információs korban, Budapest: Jaffa, 2010.

[29] S. P. Eisner, „Managing Generation Y,” *SAM Advanced Management Journal (Society for Advancement of Management,* p. 70, 2005.

[30] A. Tari, Z generáció, Budapest: Tercium, 2011.

[31] L. Székely, „A multitasking generáció nyomában,” *Kultúra és közösség IV. folyam,* %1. kötet2017/II., pp. 29-40, 2017.

[32] J. Steyer, Szólj vissza a facebooknak!, Gabo, 2012.

[33] M. Klausz, Megosztok, tehát vagyok, Budapest: Athenaeum, 2017.

[34] E. Pais, *Alapvetések a Z generáció tudománykommunikációjához,* Pécs: PTE, 2012.

[35] K. Steigervald, Generációk harca, Budapest: Partvonal, 2020.

[36] A. Tari, Bátor Generációk, Budapest: Tercium, 2017.

[37] K. Mitnick és S. William, A legendás hacker a behatolás művészete, Budapest: Perfact, 2006.

[38] K. Mitnick és S. William, A legendás hacker A megtévesztés művészete, Budapest: Perfact, 2003.

[39] „New York Times,” 07 2023. [Online]. Available: https://www.nytimes.com/2023/07/20/technology/kevin-mitnick-dead-hacker.html. [Hozzáférés dátuma: 08 08 2025].

[40] „HVG.hu,” 20 07 2023. [Online]. Available: https://hvg.hu/tudomany/20230720_Kevin_Mitnick_meghalt_hekker_amerika. [Hozzáférés dátuma: 08 08 2025].

[41] H. Márk, „444.hu,” 21 07 2023. [Online]. Available: https://444.hu/2023/07/21/meghalt-kevin-mitnick-a-korai-internet-legendas-hackere. [Hozzáférés dátuma: 08 08 2025].

[42] „Mitnick Security,” [Online]. Available: https://www-mitnicksecurity-com.translate.goog/about-kevin-mitnick-mitnick-security?_x_tr_sl=en&_x_tr_tl=hu&_x_tr_hl=hu&_x_tr_pto=sc. [Hozzáférés dátuma: 08 08 2025].

[43] R. Bilton, „BBC,” 07 2025. [Online]. Available: https://www.bbc.com/news/articles/cx2gx28815wo. [Hozzáférés dátuma: 08 08 2025].

[44] „HVG,” 07 2025. [Online]. Available: https://hvg.hu/tudomany/20250727_zsarolovirus-csod-knp-logistics-gyenge-jelszo. [Hozzáférés dátuma: 08 08 2025].

[45] „Economx,” 07 2025. [Online]. Available: https://www.economx.hu/gazdasag/kibertamadas-zsarolovirus-kartevo-pszichologiai-manipulacio.813363.html. [Hozzáférés dátuma: 08 08 2025].

[46] „Kürt,” 07 2025. [Online]. Available: https://kurt.hu/2025/07/31/eset-kiberfenyegetettsegi-jelentes-robbanasszeruen-terjed-a-hamis-hibauzenetekkel-tamado-clickfix-kartevo/. [Hozzáférés dátuma: 08 08 2025].

[47] C. D. István, „Antivirus Blog,” 07 2025. [Online]. Available: https://antivirus.blog.hu/2025/07/24/hamis_hibauzenetekkel_tamad_a_clickfix_kartevo. [Hozzáférés dátuma: 08 08 2025].

[48] „Haszon,” 08 2025. [Online]. Available: https://haszon.hu/piacok/szamitogepek-reme-clickfix/. [Hozzáférés dátuma: 08 08 2025].

[49] „ESet,” 08 2025. [Online]. Available: https://www.eset.com/sg/business/threat-report/?srsltid=AfmBOor7teB_8Ixjw2Ar_zNbc1TG9Fpbr7QEf5GfwOyeop_Jb2XizB83).. [Hozzáférés dátuma: 08 08 2025].

[50] T. Mógor, *Az emberi tényező szerepe az információbiztonság megvalósítása és erősítése terén. Az információbiztonsági kultúra fejlesztésének lehetőségei a Magyar Honvédségben,* Budapest: Óbudai Egyetem, 2017.

[51] R. Edit, *A felhasználók biztonságtudatosságának jelentősége a publikus felhőszolgáltatások nagyvállalatoknál történő bevezetésekor,* Budapest: Óbudai Egyetem, 2019.

[52] É. Beke, *A mérnök hallgatók foglalkoztathatósági kompetenciái az Ipar 4.0 tükrében,* Budapest: Óbudai Egyetem, 2023.

[53] R. Számadó, *Önkormányzatok kiberbiztonságának és online képességének vizsgálata, figyelemmel az emberi tényező fejlesztésének kérdéseire,* Budapest: Óbudai Egyetem, 2018.

[54] I. Psenakova, „Ne hagyd magad becsapni!," *Lélektan és hadviselés - Interdiszciplináris folyóira,* %1. kötetII. évfolyam, pp. 55-65, 2020.

[55] A. Bodó, T. Marsi, V. Sebők és N. Zámbó, Célzott kibertámadások - Éves továbbképzés az elektronikus információs rendszerek védelméért felelős vezető számára, D. Veronika, Szerk., Budapest: Nemzeti Közszolgálati Egyetem, 2022.

[56] A. Bodó, O. Cser, R. Gyaraki, G. Kaczur , T. Lattmann, Á. Solymos, Z. Szabó, A. Tikos , D. Váczi és N. Zámbó, Célzott kibertámadások Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára 2018, D. Veronika, Szerk., Budapest: Nemzeti Közszolgálati EGyetem, 2018.

[57] C. Kollár és Á. Zakar, „A social engineering és a manipulációs technikák és módszerek – kutatási jelentés," *Biztonságtudományi Szemle,* %1. kötetII.év. 2.sz., pp. 23-38, 2020.

[58] L. Kovács és E. Terták, „A kiberbűnözés legjobb ellenszere a pénzügyi műveltség," *Gazdaság és Pénzügy ,* pp. 6-29, 2024.

[59] J. P. Albrecht, „How the GDPR will change the world," *European Data Protection Law Review,* p. 287, 2016.

[60] C. Tankard, „What the GDPR means for businesses," *Network Security,* pp. 5-8, 2016.

[61] M. Gal és O. Aviv, „The competitive effects of the GDPR," *Journal of Competition Law & Economics,* %1. kötet16(3), pp. 349-391, 2020.

[62] S. Sharma, Data privacy and GDPR handbook, New Jersey: John Wiley & sons, 2019.

[63] „ENISA,” 10 2024. [Online]. Available: https://www.enisa.europa.eu/sites/default/files/2025-02/A%20Trusted%20and%20Cyber%20Secure%20Europe%20-%20ENISA%20Strategy.pdf. [Hozzáférés dátuma: 10 08 2025].

[64] ENIA, „Public Privat Partnerships PPP Cooperative models,” ENISA, EU, 2017.

[65] ENISA, „Cooperative Models for Effective Public Private Partnerships Good Practice Guide,” ENISA, Luxembourg, 2011.

[66] ENISA, „Cooperative Models for Effective Public Private Partnerships Desktop Research Report,” ENISA, Luxembourg, 2011.

[67] „ENISA Good Practice Guide,” [Online]. Available: https://www.enisa.europa.eu/sites/default/files/publications/Final_NSIE.pdf. [Hozzáférés dátuma: 10 08 2025].

[68] ENISA, „Information Sharing and Analysis Centres (ISACs),” EU, EU, 2017.

[69] A. Sarri és G. Fernandez, „A governance framework for national cybersecurity strategies NCCS,” ENISA, EU, 2023.

[70] A. Sarri és G. Fernandez, „Building effective governance frameworks for the implementation of national cybersecurity strategies NCSS,” ENISA, EU, 2023.

[71] A. Sarri és P. Kyranoudi, „Good practices in innovation under NCSS,” ENISA, EU, 2019.

[72] ENISA, „Cross sector exercise requirements,” EU, EU, 2022.

[73] A. Drougkas, U. Komzaite, E. Philippou, P. Abel, F. Gratiolet és E. Maaskant, „NIS Investments 2024,” ENISA, EU, 2024.

[74] ENISA, „Gaps in NIS standardisation Recommendations for improving NIS in EU standardisation policy,” ENISA, 2016.

[75] L. Dupré, „EP3R 2010-2013 Four years of Pan-European Public Private Cooperation,” ENISA, EU, 2014.

[76] E. c. policies, „NIS2 Directive: Securing network and information systems,” Digital-strategy.ec.europa.eu, [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive?utm_source=chatgpt.com. [Hozzáférés dátuma: 24. 10. 2025.].

[77] K. Adamos, F. DI Franco és S. Leventopoulos, „Cybersecurity roles and skills for NIS2 essential and important entities,” ENISA, EU, 2025.

[78] ENISA, „NIS2 Technical Implementation Guidance,” EU, Luxembourg, 2025.

[79] Ö. Vásárhelyi, „Magyarország kiberbiztonságának jövője az európai uniós NIS2 irányelv tükrében,” *Nemzetbiztonsági Szemle,* pp. 18-35, 2024.

[80] „NiS 2 irányelv: Hálózati és információs rendszerek biztosítása,” ENISA, EU, 2022.

[81] Z. N. Sik, „Elektronikus információbiztonság és közigazgatás előadás”.

[82] A. Pallagi, „A biztonságtudatosság fejlesztésének szerepe az oktatási rendszerben,” in *Kiberbiztonság - Cybersecurity*, R. Zoltán, Szerk., Budapest, Biztonságtudományi Doktori Iskola, 2019, pp. 71-81.

[83] J. Bognárné Dr. Kocsis, „Általános iskolás tanulók kutatásra nevelésének szerepe a tudásalapú fejlődésben,” in *Bárhory-Brassai Tanulmánykötet 1. rész*, F. B. O. J. Rajnai Zoltán, Szerk., Budapest, Óbudai Egyetem, 2014, pp. 62-69.

[84] K. Csercsa és Z. Rajnai, „Covid járvány utáni tapasztalatok vizsgálata kiberbiztonsági vetületben a Z generáció tagjai között,” Marcelová, Szlovákia, 2025.

[85] Z. Márton és Z. Rajnai, „A social engineering fejlődése és jövője a pszichológiai sebezhetőségek kihasználása a digitális korban,” *Biztonságtudományi Szemle,* %1. kötet6(4), pp. 45-56, 2024.

[86] N. G. Szolgálat, Szerző, *Prof. Dr. Rajnai Zoltán - Kiberbiztonság, gyermekvédelem.* [Performance]. 2017.

[87] P. D. R. Zoltán, Interviewee, *Szemtől szemben 2024.04.12.*. [Interjú]. 2024.

[88] O. Hivatal, „Kerettanterv 1-4. évfolyam,” 2020.

[89] Eduline.hu, „Mennyit telefonoznak a magyar diákok,” 2025.

[90] N. M. é. H. Hatóság, „Napi 4 órát játszik a gyermek a telefonjával Veled mennyit?,” 2025.

[91] O. Hivatal, „Kerettanterv az általános iskola 5-8. évfolyam számára,” 2020.

[92] O. Hivatal, „Kerettanterv a gimnáziumok 9-12. évfolyama számára,” 2020.

[93] I. E. Allen és J. Seaman, Staying the Course: Online Education in the United States, Newburyport: Eric, 2008.

[94] „Public Private Partnerships PPP Cooperative models,” ENISA, EU, 2017.

RÖVIDÍTÉSJEGYZÉK

IKT Információs és Kommunikációs Technológia

NAT Nemzeti Alaptanterv

ÁBRAJEGYZÉK

KÖSZÖNETNYILVÁNÍTÁS

Abban a hihetetlen megtiszteltetésben volt részem, hogy a doktori disszertációm témavezetését elvállalta **Prof. Dr. Rajnai Zoltán**, aki nemcsak szakmailag, hanem emberileg is kimagasló személy és nagyon sokat köszönhetek neki. Súlyos betegségem alatt is mellettem állt és mind szakmailag, mind emberségben nagy segítséget nyújtott az elmúlt több, mint 4 során. Nincsenek rá szavak, mennyit jelentett nekem, hogy együtt dolgozhattunk.

Nagyon köszönöm lányomnak **Csercsa Emmának** azt a végtelen hitet, amit irányomban tanúsít a mai napig. Ha Ő nem hiszi el rólam azt, hogy mindenre képes vagyok, biztosan nem tudtam volna végig csinálni ezeket az éveket. Köszönöm, hogy akkor is türelmes volt és megértő, amikor reggeltől estig csak a gépem előtt ültem és dolgoztam. Hihetetlen nagy kincs adatott nekem személyében Istentől.

Köszönöm szépen a bátyámnak **Csercsa Tamásnak**, aki mindig a segítségemre siet és mindig támogat és felvidít. Köszönöm az édesapámnak **Csercsa Józsefnek**, hogy a feltaláló vénájából rám is örökített és annyira szeretett, ami soha el nem múlik. Köszönöm családom minden tagjának, hogy mindig mellettem állnak.

Köszönöm **Kuripla Istvánnak**, aki sokat hozzátett az életemhez szakmailag és magánemberként egyaránt. Megtisztelő, hogy barátságát élvezhetem.

Köszönöm **Varga Győzőné Tündének** és **Papp Zsuzsannának** az elmúlt évek közös munkáját. Sokszor nyújtott támaszt a segítségük.

Köszönöm **Dr. Keszthelyi Andrásnak**, aki szakmailag és emberileg sokat hozzátett az életemhez.

Köszönöm az Óbudai Egyetemnek, hogy 7+4+8 féléven keresztül lehettem a hallgatója, az oktatója és azt a színvonalat és légkört, amit az elmúlt évek során megtapasztalhattam. Csodálatos emberekkel kerülhettem kapcsolatba.

Köszönöm szépen az Óbudai Egyetemen dolgozó minden oktatónak, hallgatónak és dolgozónak, aki bármilyen módon segített az elmúlt évek során. A teljesség igénye nélkül szeretném kiemelni **Lévay Katalint, Farkasné Hronyecz Erikát, Mondics-Kurmay Líviát, Feketéné Gyarmati Andreát,** akik szakértelmükkel rendszeresen segítették a munkámat. Külön köszönöm az Óbudai Egyetem Biztonságtudományi Doktori Iskola támogatását és kiemelkedő szakmai színvonalát.