Óbudai Egyetem

Doktori (PhD) értekezés

Az információbiztonság növelése a felhasználó támogatásának lehetőségeivel

Nyikes Zoltán

Témavezető

Dr. habil Kerti András

Biztonságtudományi Doktori Iskola

Budapest, 2019

Szigorlati Bizottság:

Elnök:

Prof. Dr. Rajnai Zoltán egyetemi tanár ÓE

Tagok:

Prof. Dr. Berek Lajos egyetemi tanár ÓE

Dr. Szenes Katalin c. egyetemi docens ÓE

Nyilvános védés bizottsága:

Elnök:

Prof. Dr. Berek Lajos egyetemi tanár ÓE

Titkár:

Dr. Szűcs Endre egyetemi adjunktus ÓE

Tagok:

Prof. Dr. Pokorádi László egyetemi tanár ÓE

Dr. habil. Michelberger Pál egyetemi docens ÓE

Dr. habil. Farkas Tibor egyetemi docens NKE

Bírálók:

Dr. Kiss Gábor egyetemi docens ÓE

Dr. Magyar Sándor egyetemi adjunktus NKE

Nyilvános védés időpontja

2019.

TARTALOMJEGYZÉK

„…az olyan ember, aki nem ért a számítógéphez,
a XXI. században analfabétának fog számítani…”

Teller Ede

BEVEZETÉS

Az internet az informatika és a digitalizáció korában az élet megváltozott. A világ kitárult és az élet felgyorsult az információ gyors és szabad áramlásának hatására. Az információ áradat hatása mindenkit érint, szinte függői lettünk az internetnek. Az informatika robbanásszerű fejlődése mindenki számára érezhető. A mai társadalom tagjai többségének van internet hozzáférése. Az informatikai eszközök és az internet a használata sok esetben csak a szórakozásra és a kapcsolattartásra szorítkozik. A kommunikáció is megváltozott, sokan közösségi oldalakon is megosztják életeseményeiket. Gyermekektől az idősebb korosztályon keresztül mindenki használhatja és használja is az internetet.

Az ember túlélését, az evolúciós fejlődés során a biztonságtudatossága, a védelmi reflexeinek működése, valamint az eszközök használatának magasszintű kompetenciája biztosította. A kiber világának nincs évezredekre visszanyúló története, csak az utóbbi évszázad végén alakult ki és vált egyre népszerűbbé. A kibertérben új lehetőségek és veszélyek várják a felhasználókat, ezért itt is szükség van a digitális kompetenciára és a fokozott biztonságtudatosságra, mivel itt még nem alakultak ki a védelmi reflexek.

A tudományos probléma megfogalmazása

Doktori értekezésem az információbiztonság növelésének, erősítésének felhasználói vonatkozásaival foglalkozik, különös tekintettel a biztonságtudatosság[1] és a digitális kompetencia[2] [114] fejlesztésének, valamint támogatásának lehetőségeire. Disszertációmban vizsgálom a felhasználó szerepét az információbiztonság kialakításában és erősítésében. Többéves szakmai tapasztalatomra és az összegyűjtött információkra alapozva megállapítom, hogy a felhasználó – mint az egyik alappillére az információbiztonságnak – nagyobb támogatást igényel.

[1] Solymos Ákos, információbiztonsági szakértőnek a WITSEC 2016.10.06-i szakmai napján elhangozott előadásában megfogalmazottak szerint: „A biztonságtudatosság kialakítása olyan ismeretek, gondolkodásmód és viselkedésminták átadása a munkatársak és az ügyfelek részére, amelyek alkalmazásával csökkenteni tudják a maguk és a szervezet kockázati szintjét, a kockázatokból fakadó költségeket és veszteségeket a munkahelyen és otthon, saját informatikai környezetükben is.”

[2] Az Európai Parlament 2006/962/EC ajánlása alapján - A digitális kompetencia az információs társadalom technológiáinak magabiztos és kritikus használatára való képesség a munkában, a szabadidőben, és a kommunikációban [114].

A témaválasztás indoklása

Mesterszakos (MSc) tanulmányaimat a Zrínyi Miklós Nemzetvédelmi Egyetem Biztonságtechnikai mérnöki szakán kezdtem és a jogutód egyetemen, a Nemzeti Közszolgálati Egyetemen szereztem diplomát 2012-ben. Diplomamunkám „Az információbiztonság megteremtésének vizsgálata egy fiktív katonai szervezet esetében, különös tekintettel a minősített adat védelme vonatkozásában" címet viselte.

Témaválasztásom egyik oka a felhasználók biztonságára irányuló érdeklődésem. A közelmúltban számos komoly káresemény származott a felhasználók alacsony biztonságtudatossága és digitális kompetenciája miatt, például kórházak, közintézmények adatbázisai sérültek vagy lettek zsarolás áldozatai. Felvetődött az a kérdés, hogy a felhasználók kiszámíthatatlan, sztochasztikus viselkedését, mely biztonsági kockázatot okozhat, hogyan lehetne kiszámíthatóbbá tenni, ezzel pedig az információs rendszerek biztonságát növelni. Kutatásomban tehát a felhasználó viselkedését vizsgálom, mivel a felhasználó a digitális rendszer része, így kockázati tényező is. Az információs társadalomban nagyon fontos kérdés a felhasználók széleskörű digitális intelligenciája és ezáltal biztonságtudatossága és digitális kompetenciája is, ezért a téma rendkívül aktuális.

Célkitűzések

Célként fogalmaztam meg, hogy

1. olyan értekezést készítsek, kutatási eredményekkel megalapozva, amely az információs társadalom digitális kompetenciájának növelésére, valamint biztonságtudatosságának fejlesztésére ajánlásokat ad az adott csoportok számára, melyekbe a felhasználók kompetenciájuk szerint besorolhatók.

2. értekezésemben a kutatási eredmények felhasználásával elkészítsek egy olyan, a felhasználók digitális kompetenciájának felmérésére szolgáló keretrendszert, amely tartalmazza a biztonságtudatosságra vonatkozó osztályokat és szinteket is. Ennek a keretrendszernek az alkalmazásával mind a felhasználó, mind a munkaadó, továbbá az iskolák is fel tudják mérni a felhasználó aktuális képességszintjét. Mindezt annak érdekében szükséges megtenniük, hogy a digitális kompetencia és a biztonságtudatosság szintjének növelése minél hatékonyabban valósulhasson meg.

3. a 2.pontban ismertetett keretrendszer alkalmas legyen a felhasználók képességszintjének felmérésére széleskörűen. A keretrendszer a „kezdő" szinttől kiindulva az „alacsony" és a

„közepes” szintű felhasználók képességszintjének besorolásán keresztül egészen a „magas” szintű felhasználók minősítésére is megfelelő legyen.

4. egy olyan digitális akadálymentesítő rendszer kidolgozására és szabványosítására tegyek javaslatot, amelynek alkalmazása azon felhasználók részére nyújthatna nagyobb biztonságot, akik koruknál fogva még vagy már (gyermek és időskorúak) nem rendelkeznek magas digitális kompetenciaszinttel.

A téma kutatásának hipotézisei

1. Feltételezem, hogy a társadalom különböző életkorú és különféle infrastrukturális lehetőségekkel rendelkező csoportjai esetében a digitális kompetencia és biztonságtudatosság eltérő lehet. Ennek a feltételezésemnek az az alapja, hogy a digitális technika gyors fejlődése és a benne rejlő lehetőségek miatt a társadalom egyes rétegei digitális kompetencia és biztonságtudatosság szempontjából eltérő ütemben fejlődtek.

2. Feltételezem, hogy egy viselkedésspecifikus szempontrendszer felállításával a felhasználók kockázati szempontból besorolhatók lehetnek az eltérő digitális kompetenciájuk és biztonságtudatosságuk szerint. Mivel a felhasználó viselkedése nem meghatározható és ezáltal kockázati tényezőt jelent.

3. Feltételezem, hogy kompetencia és biztonságtudatosság szempontjából a társadalom egészét besorolni kell egy már meglévő keretrendszerbe vagy amennyiben szükséges egy új Digitális Kompetencia Keretrendszert kell kialakítani, ami össztársadalmi jelentőséggel bírna a biztonságtudatosságra és a digitális kompetenciára vonatkozóan, mivel a felhasználók eltérő kockázati tényezőt jelenthetnek.

4. Feltételezem, hogy ugyanúgy, mint az élet gyors döntéseket megkövetelő más területein (pl. közlekedés) egyezményes jelrendszert alkalmazunk, ez a módszer digitális környezetben is alkalmas lehet (nevezhető akadálymentesítésnek is) a biztonság növelésére főként a gyors döntéseket igénylő esetekben.

Kutatási módszerek

A kutatási módszereket tekintve szükségszerű az komplex megközelítés alkalmazása a téma jellegéből, összetettségéből adódóan. Ez abból következik, hogy kutatásom során az információbiztonság más területeit is vizsgáltam, mint például a technikai megvalósítás lehetőségeit vagy a szabályozottság kérdését. A fenti témákban számos publikációm is megjelent. Áttekintettem Magyarország információbiztonságának szabályozottságát, a

mobiltelefonok biztonságát, a wifi hálózatok biztonsági kérdéseit, a létfontosságú rendszerek biztonságát a BigData lehetőségeivel, az ügyviteli rendszer modernizálásának lehetőségeit. A lefolytatott vizsgálatok során arra a megállapításra jutottam, hogy a magyarországi információbiztonság szabályozott, valamint a technikai kérdések esetében a szükséges technológia rendelkezésre áll a megfelelő szintű biztonság megteremtéséhez. Azonban egy tényező minden esetben megoldandó biztonsági kihívást jelentett. Ez pedig maga a felhasználó volt. Amennyiben a felhasználó alacsony digitális intelligenciával rendelkezik, abban az esetben a rendszereink lehetnek a legkorszerűbb technikai védelemmel ellátva és a szabályzók mindenre kiterjedően lefedhetnek minden biztonsági rést, akkor is a leggyengébb láncszemen fog múlni a biztonság. Legyen ez egy létfontosságú rendszer, vagy akár a felhasználó saját tulajdonú okostelefonja. Kutatómunkám során törekedtem az elméleti összefüggések és a gyakorlati alkalmazás komplex vizsgálatára. Elméleti kutatásomban a hatályos jogszabályok figyelembevételével közelítettem meg a kérdéseket, amelyek végén a gyakorlati megvalósíthatóság elvét tekintettem célként. A forrásanyagok feldolgozása, saját kutatásomban történő felhasználása, integrálása, tapasztalatainak leszűrése érdekében felhasználtam az analízis és a szintézis nyújtotta módszereket. A dokumentum – és kutatáselemzéseket minden esetben saját kutatási témámhoz kapcsolódóan végeztem. Célom volt egy – az ok-okozati összefüggéseket láttató – átfogó munka megalkotása. A felmérések és megfigyelések hozzájárultak ahhoz, hogy a végkövetkeztetések tükrözzék a felhasználók digitális intelligenciájának jelenlegi helyzetét. Kérdőívet készítettem a felhasználók részére, amelynek tapasztalatai és a válaszok korrelációs értékeléséből kapott eredmények a kutatásomhoz kiindulási alapot nyújtottak. A kérdőívek kiértékelése során alkalmaztam a Pearson korrelációs együttható értékének meghatározását. A teszt annál jobban méri a mérni kívánt tulajdonságot, minél jobban összefügg a valódi érték a mért értékkel, vagyis a két érték minél jobban korrelál. Ez a tulajdonság, a teszt megbízhatósága, reliabilitása. Gyakorlati feladatokat dolgoztam ki, melyeket a kísérletben önkéntesen résztvevők hajtottak végre valós időben. Különös figyelmet fordítottam a gyakorlati tapasztalatok elemzésére, az értékelhető következtetések megfogalmazására.

A disszertációm irodalomkutatását 2018. július 18-án fejeztem be.

1 AZ INFORMÁCIÓBIZTONSÁG BÁZISPONTJAI

Korunkban, amikor az internet és az informatika fejlődése megváltoztatta életünket és annak mindennapjait, kitárult a világ. Az információ gyors és szabad áramlása az életünket is felgyorsította [1]. Gyorsabban „élünk”, több információ, több impulzus ér minket. Ennek már akkora a befolyásoló hatása, hogy már-már függők lettünk az információáradattól. A társadalom ebből a szempontból kettészakadt, a fiatalabb és az idősebb generációk között éles a kontraszt. A 35 évnél idősebbek számára az informatikai eszközök és alkalmazások használata kihívást jelent. Az informatikai robbanást mindenki megérezte, a többség rendelkezik internethozzáféréssel, annak használata a funkcióját tekintve inkább csak a szórakoztatást és a kapcsolattartást szolgálja. Az internet és az informatikai eszközök adta lehetőségek nem, vagy csak nagyon korlátozott számban kerülnek kihasználásra. Ez különösen nagy veszélyt rejteget, mert ezek a korosztályok így leszakadnak, és saját magukat rekesztik ki a digitális jólétből[3]. Ezzel szemben a 35 évnél fiatalabbak már teljes természetességgel használják és alkalmazzák a digitális világ adta lehetőségeket [2]. Használják az internetet és a különböző informatikai eszközöket. Itt is jellemző a szórakozás és a kapcsolattartási funkciók elsődleges használata, de sokkal szélesebb körben alkalmaznak egyéb, az internet és az informatikai eszközök által biztosított más lehetőséget is [3]. Nem okoz problémát elsajátítani egy-egy új funkcióval bíró alkalmazást. Ez azért alakulhatott így ki, mert ezek a korosztályok vagy már nagyon kicsi gyerekkoruk óta ebben a digitális világban élnek, vagy már eleve ebbe születtek bele és teljesen természetes számukra a digitális jelenlét. Azonban minden esetben elmondható, hogy a digitális világ számtalan veszélyt rejteget a számunkra. Elsősorban azokra, akik használják azt, de másodsorban azokra is, akik nem túl aktívak a digitális világban, vagy egyáltalán nem is használják. Mivel életünk és a társadalmunk működésének döntő többsége már a digitális térbe tevődött át, és kikerülhetetlenül azon keresztül zajlik, ezért annak a biztonsága rendkívüli fontossággal kell, hogy bírjon mindenki számára. A biztonságtudatosság és a védelmi reflexeink még nem alakultak ki úgy, mint ahogy az a fizikai, valós térben, az evolúciós fejlődés és az évezredek során már biztosította az ember túlélését [4]. A kibertérben[4] zajló élet nem nyúlik vissza évezredekre, de még évszázadokra sem. Az elmúlt negyed évszázadban alakult ki és vált egyre népszerűbbé a digitális világ, azonban annak felfedezése nem szorítkozott kizárólag biztonságos tevékenységekre [5]. Ahogy egyetlen új dolognak és térnek a feltárását sem a biztonságos megközelítés jellemezte, úgy a digitális tér felfedezését

[3] Digitális jólét – részletesen kifejtve a 2.2.2 pontban
[4] Kibertér – részletesen kifejtve a 1.3.1 pontban

sem. Ha a digitális tér és a kibervilág megismerését összevetjük a fizikailag valós terek felfedezésével, mint a tengerek, a légtér vagy akár a világűr feltérképezése, akkor megállapíthatjuk, hogy az első használók számára ott sem a biztonság volt az elsődleges szempont [6]. De miután széles körben elterjedt azok használata, egyrészt kialakult valamilyen biztonsági reflex, másrészt számos, a biztonságot érintő szabályozás történt az adott területeken. A digitális térre vonatkozó biztonsági reflexek kialakulása és a biztonsági szabályozások még nem túl régóta kezdődtek meg. De mit sem ér a szabályozás, hogyha az csak követi az eseményeket, bonyolult és egyébként sem tartják be, mert adott személyre az internet világában már nem érvényes. Gondolok itt arra az anomáliára, hogy a törvények és jogszabályok csak a fizikális világban létező, földrajzilag elkülönített közigazgatási egységekre vonatkoznak, mint például különböző szintű önkormányzatok, országok vagy szövetségi egységek. Ezzel szemben például a magyar szabályok már nem vonatkoznak az ellenünk más országból elkövetett kiberbűntények[5] idegen állampolgáraira [7]. Egy ázsiai hackert nem tart távol egy uniós- vagy magyar szabályozás attól, hogy feltörje a közösségi profilunkat és visszaéljen adatainkkal. Ennek ellenére hiszem és vallom, hogy márpedig a társadalmi rend alapja maga a törvénykezés, mely nélkül anarchia uralkodna. A törvénykezés viszont kevésnek bizonyul, ha az emberek nem a törvény szellemében élnek és önmaguk nem tesznek a saját biztonságuk érdekében sem a fizikai valóságban, sem a kibertérben [8]. Teljesen alapvető dolog, hogy az emberek a lakásuk ajtaját becsukják, és kulccsal bezárják, ha riasztójuk van, azt is élesítik. Az autóban, ha beszállnak, bekapcsolják a biztonsági övet és betartják a közlekedési szabályokat, ha pedig az út- és látási viszonyok romlanak, akkor csökkentik a sebességet és fokozottabban figyelnek vezetés közben [9]. Az is teljesen természetes, hogy nem mennek egyedül éjszaka olyan környékre, ahol tudvalevő a bűncselekmények magas száma, és nem vásárolnak az utcán kétes kinézetű személyektől értékes dolgokat. Tehát a fenti példák azt tükrözik, hogy az emberek tisztában vannak a fizikai tér biztonsági elvárásaival. Kutatásom során ennek mintájára a kibervilágban zajló életünk biztonsági kihívásaira keresek választ. Arra, hogyan előzhetőek meg a káresemények, mert a prevenció sokkal kevesebbe kerül, mint például az egészségügyben is, az elvesztett egészség visszaszerzésénél. Ebben az esetben is magát az embert kell meggyőzni arról, hogy tegyen az egészségéért még a betegséget megelőzően. Ugyanígy a kiberbiztonság tekintetében is magának az embernek a biztonságtudatosságát kell növelni az elkerülhető incidensek megelőzésének érdekében. A biztonságtudatosság növekedése akkor érhető el a felhasználók körében, ha tudják és értik,

[5] Kiberbűntény – részletesen kifejtve az 1.3.1 pontban

hogy mit is csinálnak az interneten az informatikai eszközeikkel különböző alkalmazások segítségével, egyszóval magas a digitális kompetenciájuk és a digitális kulturáltságuk [10].

1.1. Az Európai Unió törekvései a digitális kompetencia és biztonságtudatosság növelése érdekében

Az Európai Unió felismerve a digitális kor beköszöntének kihívásait, számos, a digitális felzárkózást érintő területen új szabályozást és nagyszámú innovációt indított el. Sarkallva mindezzel az Uniós államokat, melyeket az ilyen irányú törekvéseikben erkölcsileg és anyagilag is jelentős támogatásban részesít.

1.1.1 Az Európai Parlament és Tanács ajánlása a digitális kompetencia növelésére

Az Európai Parlament és Tanács ajánlása (EPT 2006/962/ EK) [114] szerint az egész életen át tartó tanuláshoz szükséges kulcskompetenciák jelentős fontossággal bírnak. Ennek alapján a magyar Nemzeti alaptantervben is meghatározásra kerültek az úgynevezett kulcskompetenciák, ezek között a digitális kompetencia is szerepel. Ugyancsak az Európai Parlament és Tanács ajánlásában szerepelnek a szükséges készségek és attitűdök, melyek elengedhetetlenek a digitális kompetencia fejlesztéséhez.

EPT 2006/962/EK:7 A digitális kompetencia a természetnek, az IST (Information Society Technology – információs társadalmi technológiák, a továbbiakban: IST) szerepének és lehetőségeinek alapos értése és ismerete a mindennapokban: személyes és társadalmi életünkben és a munkában. Ez nem más, mint a fő informatikai alkalmazások, valamint az internet lehetőségeinek és veszélyeinek megértése és az elektronikus kommunikáció, az információ megosztása a tanulás és kutatás számára.

1.1.2 Az Európai Digitális Menetrend

Az Európai Digitális Menetrendet az Európai Bizottság 2010 májusában mutatta be. Ennek az akciótervnek és stratégiának az a feladata, hogy 2010 és 2020 között előmozdítsa az EU gazdaságának fellendülését és elterjessze a digitális korszak vívmányait a társadalom minden szintjén. A digitális menetrend célja általánosságban, hogy a nagy sebességű és szupergyors internetre és interoperábilis alkalmazásokra épülő egységes digitális piac révén fenntartható gazdasági és szociális előnyöket teremtsen.

Az Európai Digitális Menetrend célja az infokommunikációs technológiák alkalmazásának minél szélesebb körű elterjesztése. Azokra az IT-technológiákra és internetes szolgáltatásokra összpontosít, amelyek elősegítik a munkahelyteremtést, a gazdasági növekedést, és ezáltal

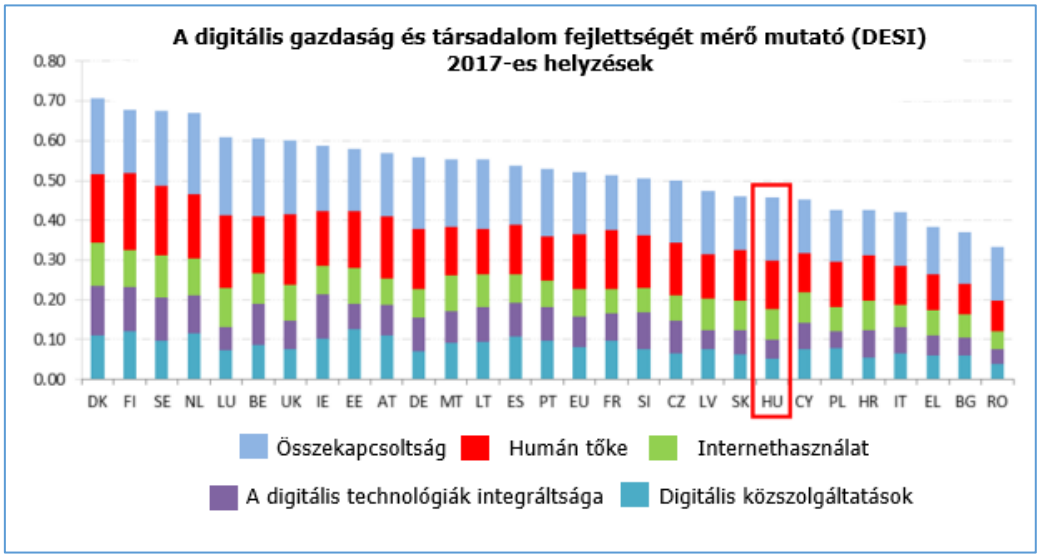
jelentősen hozzájárulnak az uniós polgárok életminőségének és a vállalkozások versenyképességének javításához.

A gazdaság többi részéhez képest a digitális gazdaság hétszer gyorsabban növekszik, a páneurópai szakpolitikai keretrendszer egyenetlensége miatt viszont a benne rejlő lehetőségek kiaknázását korlátozza. A gyors, megbízható és összekapcsolt digitális hálózatok terén Európa lemaradt a legfejlettebb országoktól, pedig ezek a hálózatok nemcsak a gazdaság gerincét adják, hanem az üzleti és a magánéletet is átszövik.

Naponta 250 millióan használják az internetet Európában. Azoknak az uniós polgároknak a száma azonban még mindig több millióra tehető, akik életük folyamán sohasem használták az internetet. Különösen az alacsony digitális kompetenciájú emberek vannak kitéve olyan nehézségeknek, amelyek nagymértékben megnehezítik azt, hogy élni tudjanak az új elektronikus tartalmak és szolgáltatások adta lehetőségekkel. Mindenkinek rendelkeznie kell fejlett digitális készségekkel ahhoz, hogy az egyre nagyobb számú napi feladatot elvégezze az internet használatával [11].

Európa digitális fejlődéséről szóló jelentés (EDPR[6]), 2017 – Országprofil Magyarországról

A digitalizálás tekintetében a tagállamok által elért előrehaladást az Európa digitális fejlődéséről szóló jelentés (EDPR) követi nyomon.



1. ábra A digitális gazdaság és társadalom fejlettségét mérő mutató (DESI) – 2017-es helyezések (forrás: EDPR, 2017) [12]

[6] EDPR - European Digital Progress Report (Európa digitális fejlődéséről szóló jelentés)

Egyesíti a digitális gazdaság és társadalom fejlettségét mérő mutató (DESI)[7] alapján nyert mennyiségi adatokat és az országspecifikus szakpolitikákra vonatkozó minőségi információkat [12].

Magyarország 2017-ben a 28 uniós tagállam közül a 21. helyen állt, ami átlagos ütemű fejlődést jelent az elmúlt évekhez képest. Az összekapcsoltság területén Magyarország jól teljesít, ami a nagysebességű vezetékes szélessáv (NGA[8]) és a 4G elterjedtségének és a vezetékes hálózatok szélessávú internethasználati növekedésének tudható be. Továbbra is lassan terjed a mobil szélessáv (1. ábra). A digitális készségein javított Magyarország, de elmarad az átlagtól, ezért ebből a szempontból Magyarország sajnos a gyengén teljesítő országok csoportjába tartozik.[9]

Magyarország 2017-ben a humán tőkéjét tekintve 18. helyen állt az uniós országok között. Ez elmarad az uniós átlagtól, de jobb előrehaladást ért el, mint az Unió átlagban. Magyarország a 2016 évi 18. helyről a 15. helyre került 2017-ben az EU-n belül, mert az internet felhasználók száma 6 százalékponttal nőtt. Így, jelentősen megközelítette az uniós átlagot [12].

1.1.3 Az Európai Unió hálózati és információs rendszerek biztonságáról szóló irányelve

A hálózati és információs rendszerek biztonságáról szóló irányelv, vagyis az úgynevezett NIS irányelv 2016. július 19-én megjelent az Európai Unió hivatalos lapjában. Ez az Európai Parlament és a Tanács (EU) 2016/1148 számú irányelve. A NIS irányelv az első közösségi szintű szabályozás az információbiztonság területén. Korábban önkéntesen és bizalmi alapon valósult meg a tagállamok intézményei között az együttműködés. Az irányelv célja, hogy megfogalmazzon egy közös intézmény és eszköztárat a tagállamok számára, illetve egy európai szintű együttműködés alapjait fogalmazza meg. Így elkülöníthetők a nemzeti szinten végrehajtandó és a közösségi szinten végrehajtandó feladatok [115].

1.1.4 Az ENISA[10] éves jelentés biztonságtudatosságra vonatkozó részei

Az Európai Unió Hálózati és Információbiztonsági Ügynöksége által a 2016 évre kiadott Fenyegetettségi helyzetkép című jelentés kiemeli, hogy az informatikai biztonsági oktatás, képzés és tudatosság növelése területén bevált gyakorlatokkal (best practices[11]), a szakemberek

[7] DESI - The Digital Economy and Society Index (A digitális gazdasági és társadalom fejlettségmérő mutató)
[8] NGA - Next generation access (Újgenerációs hozzáférés)
[9] Gyengén teljesítő országok (digitális készségek terén): Románia, Bulgária, Görögország, Olaszország, Horvátország, Lengyelország, Ciprus, Magyarország és Szlovákia.
[10] The European Union Agency for Network and Information Security – az Európai Unió Hálózati és Információbiztonsági Ügynöksége
[11] best practise – bevált gyakorlat

fejlesztésével és a fiatalok tudatosításával kapcsolatos szerepvállalások nagyban növelik a kiberfenyegetések megelőzését. Az oktatással és a tudatosság szintjének emelésével jelentősen csökkenthetők a biztonsági költségek, valamint a felhasználók biztonsági kockázatai is. A 2016 évi jelentés kimondja, abban az évben kimutatható az, hogy a felhasználók magas biztonságtudatosságából adódóan jelentősen, több mint 50%-kal csökkenti a rendszeres és a hatékony képzés az adathalászat, a ransomware[12] és más hasonló támadásokkal szembeni kitettséget [13]. A 2017 évi jelentésben az ügynökség arról számol be, hogy az adathalász támadások 90-95%-a sikeres volt, amit a végpont védelemnövelése mellett a felhasználók tudatosságának növelésével kell csökkenteni. A kiberbiztonsági szakemberek a körében végzett felmérések alapján kimutatták, hogy a bennfentes támadások (insider atacks[13]) bekövetkezésének több más ok mellett, - 31%-ban oka a felhasználók biztonságtudatossága vagy az oktatás hiánya okozza [14].

1.2 Magyarország digitális fejlesztése

Magyarország, ahogy az Európai Unió is, felismerte az új társadalmi rend kialakulásában rejlő kiaknázatlan lehetőségeket. Továbbá azt, hogy társadalmi szinten az erőforrásokat és infrastruktúrákat, valamint az állampolgároknak, mint felhasználóknak a készségeit sürgősen javítani és fejleszteni kell. Ahhoz, hogy versenyképességünket megtartani és nem utolsó sorban, akár növelni is tudjuk, az ország számára kiemelt fontosságú a digitalizáció széleskörű elterjesztése.

1.2.1 Magyarország digitális fejlesztésére tett kormányzati intézkedések

A Nemzeti Infokommunikációs Stratégia (illetve az erről szóló 1069/2014. (II.19.) Korm. határozat) [116] és Zöld Könyv [15] jelöli ki a 2014-20-as időszakra vonatkozóan az uniós elvárásokkal is összehangolt hazai informatikai és távközlési szektor fejlesztésének stratégiai irányait, fejlesztési súlypontjait. A Digitális Nemzet Fejlesztési Program (1631/2014. (XI. 6.) Korm. határozat) [117] rögzíti a stratégia megvalósításának akciótervi kereteit. A Digitális Magyarország küldetése, hogy a digitális környezet kiegyensúlyozottan fejlődjön az összehangolt kormányzati fejlesztési programoknak köszönhetően. Az infokommunikációs eszközök és szolgáltatások pozitív lendülete segítségével megvalósuljon a versenyképes, fenntartható gazdasági növekedés, foglalkoztatás és társadalmi esélyegyenlőség. Célja, hogy

[12] ransomware - zsarolószoftver / zsarolóprogram, olyan kártékony szoftver, amely valamilyen fenyegetéssel próbál pénzt kicsikarni a felhasználóból.
[13] insider attacks - A bennfentes támadás, olyan incidens, ami a szervezeten belüli emberekből induló (munkavállalók, a korábbi alkalmazottak, stb) csalással, bizalmas vagy kereskedelmi szempontból értékes információ lopásával, a szellemi tulajdon lopásával vagy a számítógépes rendszerek szabotálásával járhat.

növekedjen és javuljon az állampolgárok és a vállalkozások elektronikus szolgáltatásokhoz való hozzáférési lehetősége, valamint ezen szolgáltatások igénybevételének aránya, azaz a készségfejlesztés.

A kormány elkészítette a Digitális Jólét Programot (DJP[14]), amelyet 2012/2015. (XII. 29.) határozatával [118] fogadott el. A Digitális Jólét Programot a Nemzeti Infokommunikációs Stratégiával (NIS[15]) és a NIS akciótervi kibontását tartalmazó „Zöld könyv az infokommunikációs szektor 2014-2020 között fejlesztési irányairól" című dokumentummal összhangban, a Digitális Nemzet Fejlesztési Programban (DNFP[16]) elért eredményekre, illetve megvalósítás alatt álló fejlesztésekre építve valósítja meg [16].

A Digitális Magyarország főbb céljai:

- szupergyors internet elérhetővé tétele, azaz, hogy a háztartások legalább 30 Mbps-os sebességgel csatlakozzanak a világhálóra 2020-ig. A kormány célja, hogy (az Európai Unióban) már 2018-ra biztosítsa az egész országot lefedő, nagy sávszélességet (legalább 30 Mbps) biztosító infrastruktúra megépítését, a nagysebességű szélessávú hálózatot,
- a helyi közösségek, valamint a teljes magyar közösség összetartozásának erősítése a digitális technológia révén,
- az állam által nyújtott szolgáltatások fejlődése; eszközbeszerzések; intelligens városi szolgáltatások bevezetése; a térségi gazdaságfejlesztési programok lebonyolítása; a helyi KKV-k informatikai fejlesztése,
- digitális infokommunikációs alkalmazások, szolgáltatások elterjesztésének támogatásán keresztül az életminőség javítása minden élethelyzetben. Azaz, hogy 2020-ra az állampolgárok számára biztosított közszolgáltatások minél szélesebb köre legyen elérhető elektronikusan, és a vállalkozások számára valósuljon meg a szolgáltatások elektronizálása,
- az ország versenyképességének növelése a digitális szolgáltatások, valamint a digitális készségek fejlesztése által. A digitális készségek fejlesztése kulcsszerepet játszik a fenti célok eredményeinek hasznosulásában, így kiemelten fontos e terület integrált fejlesztése, amely magában foglalja a köznevelés, valamint a felsőoktatás rendszerére irányuló, illetve a különböző hátrányos helyzetű célcsoportokat megcélzó összehangolt akciókat egyaránt [17].

[14] DJP – Digitális Jólét Program
[15] NIS - Nemzeti Infokommunikációs Stratégia
[16] DNFP - Digitális Nemzet Fejlesztési Program

1.2.2 Magyarország Digitális Gyermekvédelmi Stratégiája

A 1488/2016. (IX. 2.) Korm. határozat [119] rendelkezik a Gyermekek Számára Biztonságos Internetszolgáltatás megteremtéséről, a tudatos és értékteremtő internethasználatról és Magyarország Digitális Gyermekvédelmi Stratégiájáról.

A stratégia kiemelt célja a tudatos, értékteremtő internethasználat támogatása mellett, hogy érvényesüljenek a gyermekek védelmét szolgáló szabályok és intézkedések. Ezért elengedhetetlen a gyermekekre leselkedő veszélyek, kockázatok azonosítása, azok kiküszöbölése az internethasználat során, ezáltal a káros hatások megelőzése, illetve lehető legnagyobb mértékű csökkentése. A stratégia további célkitűzése, hogy a rendelkezésre álló védelmi mechanizmusok megfelelőképpen, hatékonyan töltsék be funkciójukat [18].

1.2.3 Magyarország Digitális Oktatási Stratégiája (DOS)

„Magyarország Digitális Gyermekvédelmi Stratégiájának megalkotását (…) elengedhetetlenné tette (…), hogy olyan új típusú veszélyforrások, fogalmak jelentek meg az elmúlt években a gyermekek internethasználatával összefüggésben, amelyek új megoldásokat, bizonyos körben új állami eszközrendszert igényelnek [19].”

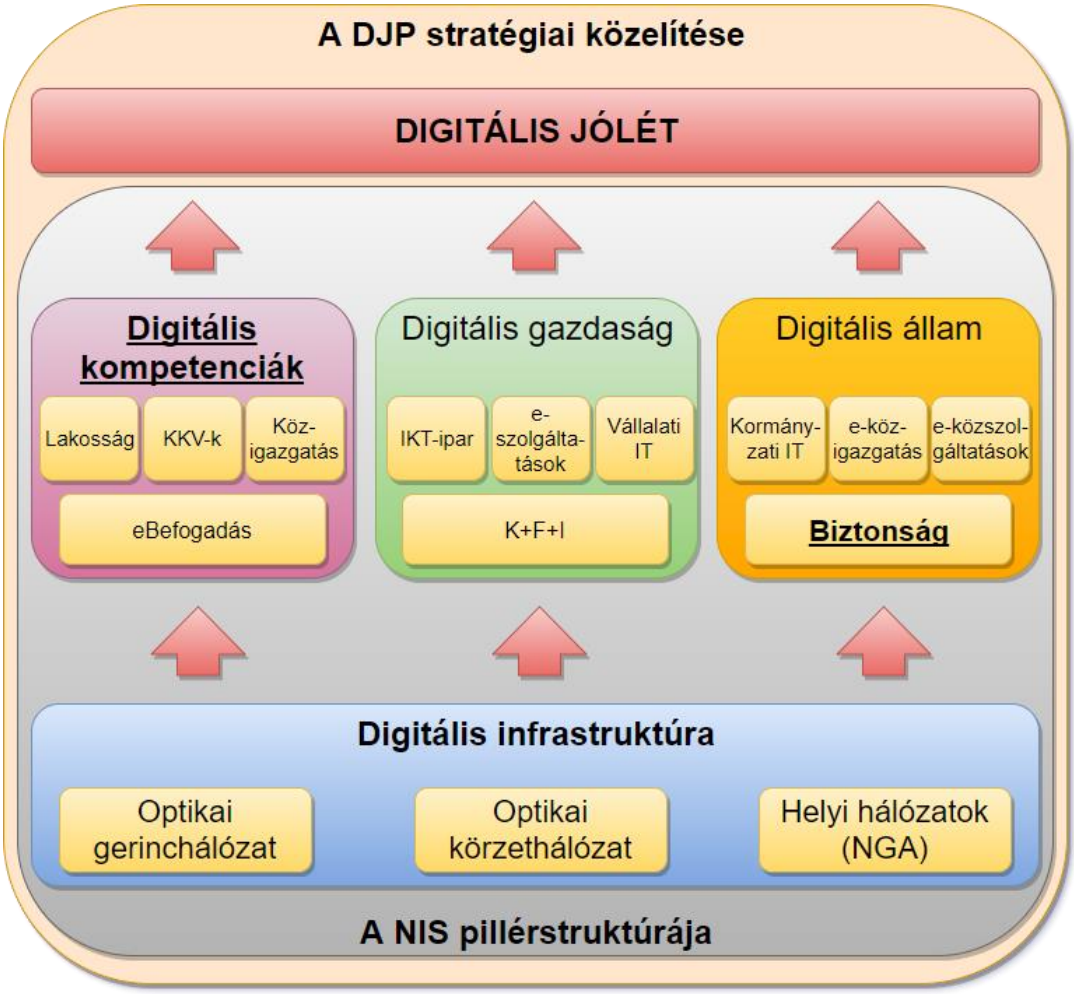
A stratégia „kiemelt célja a tudatos, értékteremtő internethasználat támogatása mellett, hogy az eddigieknél hangsúlyosabban érvényesüljenek a gyermekek védelmét szolgáló szabályok és intézkedések. Ennek érdekében fontos az internethasználat során a gyermekekre leselkedő veszélyek, kockázatok azonosítása, azok kiküszöbölése, ezáltal a káros hatások megelőzése, illetve lehető legnagyobb mértékű csökkentése. A stratégia további célkitűzése, hogy a rendelkezésre álló védelmi mechanizmusok megfelelőképpen, hatékonyan töltsék be funkciójukat [19].”

„A stratégia középpontjában a gyermekek állnak, de ezzel együtt a társadalom szinte valamennyi csoportja érintettnek tekinthető, ezért az állami eszközrendszer meghatározása mellett a kölcsönös tudásmegosztás és tanítás, valamint a társadalom különböző szereplőinek összefogása együttesen tehetik sikeressé a stratégia gyakorlati megvalósítását [19].”

1.2.4 A Digitális Jólét Program (DJP) 2.0

A társadalmi és közigazgatási egyeztetést követően 2017. július 19-én jelent meg a Kormány 1456/2017. (VII. 19.) határozata a DJP2.0 elfogadásáról [120]. A dokumentum nem csak azokat a pontokat, szakmai javaslatokat tartalmazza, amelyek vonatkozásában a kormányhatározat feladatokat jelöl ki az egyes minisztériumok számára, hanem további olyan elképzeléseket is, amelyek későbbi intézkedések alapját képezhetik. A DJP2.0 elkészítése során arra törekedtek,

hogy egyetlen fontos, a kormányzat közpolitikai, szabályozási vagy fejlesztéspolitikai figyelmét igénylő terület se maradjon ki. A rendkívül gyorsan változó digitális ökoszisztéma természetesen bármikor mutathat olyan új jelenségeket, amelyek beavatkozást igényelnek.



2. ábra A DJP stratégiai közelítése és a NIS pillérstruktúrája, benne kiemelve a digitális kompetencia és a biztonság elhelyezkedése (forrás: DJP 2.0; készítette a szerző) [16]

A digitális kompetenciák fejlesztésének elsődleges célja, hogy a magyar munkavállalók megfeleljenek a digitális kor elvárásainak, mert az elkövetkező években dől el, hogy milyen szerepet töltenek majd be az európai munkaerőpiacon. Az érintett magyar polgárok munkaerő-piaci kilátásait folyamatosan, komoly mértékben rontja a digitális kompetenciák hiánya. A digitális kompetenciák fejlesztése ugyanakkor a teljes digitális ökoszisztémára pozitív hatást gyakorol. A magyar nemzetgazdaságból több százezer digitálisan felkészült munkavállaló hiányzik, ami nélkül az Irinyi Terv és az IPAR 4.0 megvalósítása és a hazai KKV-k technológiai fejlesztése hatalmas gondot jelent.

A kormányzat a NIS és a DJP2.0 dokumentumokban azt a célt tűzte ki maga elé, hogy a digitalizáció minél több dimenziójában váljon Magyarország a régió vezető szereplőjévé váljon. Ennek érdekében számos stratégiát alkotott meg (2. ábra) szakértők segítségével [16].

1.2.5 Az Új Nemzedék Jövőjéért Program

Az Új Nemzedék Jövőjéért Program a kormány ifjúságpolitikai keretprogramja, amelyet 2012-ben alkotott az akkori Közigazgatási és Igazságügyi Minisztérium, valamint a Nemzeti Erőforrás Minisztérium által felkért szakértői csoport. Az Új Nemzedék Jövőjéért Program nem stratégia, nem cselekvési terv, hanem egy keretprogram, amely meghatározza a kormány ifjúságpolitikai céljait, a szükséges beavatkozási területeket, és a kívánt hatás eléréséhez nélkülözhetetlen intézkedések sorát. A Program részletesen foglalkozik a digitális felzárkóztatással és annak kihívásaival. Fontos megemlíteni, hogy az ifjúságpolitika elsődleges célcsoportjának a 14-től 35 éves korig tartó korosztályt tekinti. Mindezt a fiatalok egyre későbbi munkaerőpiac szereplőivé válása és az elhúzódó családalapításuk alapján teszi [20].

1.2.6 Magyarország nemzeti stratégiái az élethosszig tartó tanulásra

Szent-Györgyi Albert, a Nobel-díjas magyar tudós mondta 1937-ben, hogy „A holnap olyan lesz, amilyen a ma iskolája.” Ezt a tanácsot alapul véve a kormányzat megalkotta „Az egész életen át tartó tanulás szakpolitikájának keretstratégiáját”, a „Köznevelés-fejlesztési stratégiát”, valamint a „Végzettség nélküli iskolaelhagyás elleni középtávú stratégiát.” Ezeket a stratégiákat a Kormány 1603/2014. (XI. 4.) számú, a Magyar nemzeti társadalmi felzárkózási stratégia II.-ről szóló Korm. határozat [121] alapján, valamint a 1672/2015. (IX. 22.) számú, a magyar nemzeti társadalmi felzárkózási stratégia II. végrehajtásának a 2015-2017. évekre szóló kormányzati intézkedési tervéről szóló Korm. határozat [122] alapján hajtotta végre. A magyar kormány korábban már 2005-ben is fogadott el nemzeti stratégiát az élethosszig tartó tanulásról. Különösen indokolja ezt, hogy az oktatás világában a korábbi stratégiai dokumentum elfogadása óta olyan jelentős változások történtek, amelyek miatt ez a dokumentum már nem tölthette be azon szakpolitikai lépések orientálójának a szerepét, amelyek a digitális kompetencia fejlesztéséről is intézkednek [21].

1.2.7 Magyarország szakpolitikai stratégiája a foglalkoztatáspolitika fejlesztésére

A kormányzat számára a Nemzetgazdasági Minisztérium 2013-ban ugyan előkészítette „A 2014-2020 közötti időszak foglalkoztatáspolitikai célú fejlesztéseinek megalapozása” című szakpolitikai stratégiát, azonban a Kormány nem tárgyalta meg, ezért az nem tekinthető a Kormány álláspontjának. Ez a szakpolitikai stratégia viszont, más kompetenciák növelése

mellett, kiemelten foglalkozik a digitális kompetencia, mint kulcskompetencia fejlesztésének szükségességével [22].

1.2.8 Digitális Munkaerő Program

A kormányzat a digitális gazdaság fejlődését fenyegető legfőbb korlátozó tényezőként azonosította az informatikai és digitális munkaerőhiányt. A problémát folyamatosan és egyre határozottabban jelezte a kormányzat a közvélemény felé is, és számos olyan egyeztetésen és projektben vett részt, amely a munkaerőhiány egyes tényezőit volt hivatott orvosolni. Az azonosított probléma több elemére kiterjedő átfogó programként pedig elkészítette és a döntéshozók figyelmébe ajánlja a Digitális Munkaerő Program (DMP) elnevezésű javaslatcsomagját. A DMP természetesen nem oldhatja meg a digitális átalakulással összefüggő valamennyi munkaerőpiaci problémát: szándéka szerint az IKT ágazat, illetve az IPAR 4.0 körébe tartozó és a digitális átalakulásban leginkább érintett ágazatok számára kíván hozzájárulni a digitálisan felkészült munkavállalók biztosításához. A program segíthet annak megelőzésében is, hogy az egyébként is szűkösen rendelkezésre álló informatikai szakemberekkel töltsenek be olyan munkaköröket, amelyekben egy magas digitális kompetenciákkal rendelkező, de az adott ágazatot is jól ismerő szakember is foglalkoztatható volna [23].

1.3 A magyarországi információbiztonsági helyzet változásának előzményei

A következő részben a digitális kompetencia és a biztonságtudatosság azon megjelenési formájának a jogszabályi környezetét vizsgálom, ami nélkül az előbb említett képesség és készség nem is létezne, ez pedig nem más, mint a kibertér.

Magyarországon egy jelentős információbiztonsági szabályozási és korszerűsítési folyamat vette kezdetét a 2009. évi CLV. törvény 2010. április 1-i hatályba lépését követően. Ez a törvény a minősített adat védelméről rendelkezik. A korábban érvényes nemzeti és külföldi minősített adatok védelméről szóló rendelkezéseket hatálytalanította, és azonos szintre emelte a nemzeti minősített adatok védelmét a NATO vagy az EU minősített adatainak védelmi szintjével. Ezt követően jelentek meg és a törvénnyel egy időben léptek hatályba a törvény végrehajtási rendelkezései. Az egyik a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Kormányrendelet. A másik az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairól szóló 92/2010. (III. 31.) Kormányrendelet. Majd ezt követte a minősített adat elektronikus

biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V. 6.) Kormányrendelet [123][124][125][126].

A fenti szabályzók megalkotását és életbeléptetését az tette szükségessé, hogy Magyarország 1999-ben a NATO tagjává vált, valamint 2004-ben az Európai Unió közösségébe lépett. Mind a két szövetségi rendszerhez történő csatlakozás feltétele volt a szövetségesek és a közösség által ránk bízott minősített adatok védelmének a garantálása, amelyeket az akkori kormányzatok meg is tettek. A nemzeti minősített adatok védelme viszont méltatlanul el volt hanyagolva és a külföldi minősített adatokhoz képest alacsony védelmet kapott [24].

1.3.1 Az elektronikus információbiztonság jogszabályi háttere

Felgyorsult életünk megkerülhetetlen eleme az elektronikai területen elért vívmányoknak a mindennapokban történő alkalmazása. Az internet által nyújtott szolgáltatások ma már nagyon sok ember zsebében ott lapulnak okostelefonok formájában. Az emberek többsége az otthonában, és a munkahelyen a számítógépek segítségével éli mindennapjait. A munkahelyek többsége ma már elképzelhetetlen az informatikai rendszerek hálózatának alkalmazása nélkül. Teljes életünket behálózzák azon infrastruktúrák, amelyeket összekötnek, de akár működtetnek is az infokommunikációs[17] rendszerek és technológiák. Természetesen ezeknek a vívmányoknak is vannak sérülékeny pontjai, amelyeket védeni kell, mert mint az élet minden területének, ezeknek is megvannak a maguk bűnelkövetői csoportjai. Ezek a bűnözők ma már a világon bárhonnan összehangolt támadásokat képesek végrehajtani akár az internet felhasználói ellen, akár különböző infrastruktúrák, akár közigazgatási és gazdasági intézmények ellen az internet felhasználásával.

A mai világunkban, amikor az információs vagy tudás alapú társadalom korát éljük, a legfontosabb erőforrások egyikévé lépett elő az információ. A továbbítására, tárolására szolgáló új közegen, a kibertéren keresztül is egy ország ugyanolyan sérülékeny és kiszolgáltatott, mint amikor egy ország légtere nincs megfelelően védve. Ezért tehát ezt a közeget is sajátosságainak megfelelően kell védeni, sőt a katonai alkalmazhatóságáról, védelméről sem szabad megfeledkezni.

[17] Az információ- és kommunikációtechnológia (Information and Communications Technology, ICT) alatt az egységes kommunikáció szerepét, a telekommunikáció integráltságát, a számítógépekre és az audiovizuális rendszereket értjük. Ezen eszközök felhasználói képesek hozzáférni, tárolni, továbbítani, valamint kezelni az információkat [25].

1.3.2 Az kibertér védelmének jogszabályi háttere

Azokat az elektronikus információs rendszereket, amelyek összekapcsoltan és decentralizáltan biztosítják az adatok és információk továbbítását a gazdasági és társadalmi folyamatokhoz, kibertérnek nevezik.

Magyarország kibervédelmi stratégiája a Magyarország Alaptörvényében megfogalmazott alapértékek leképezése egy külön biztonság- és gazdaságpolitikai területre, az Alaptörvény 38. cikkéből levezetett, a nemzeti vagyon részét képező nemzeti adatvagyon, valamint a kapcsolódó létfontosságú rendszerek és létesítmények kiberbiztonságának dokumentuma. A stratégia összhangban van az 1035/2012. (II. 21.) Korm. határozattal [127] elfogadott Magyarország Nemzeti Biztonsági Stratégiájával. Társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme. Továbbá elfogadásra került a 1139/2013. (III.21.) Korm.határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. Ezen stratégia célja az Alaptörvény elveivel összhangban, többek között a nemzetgazdaság és társadalom szabad tevékenységének védelme és biztonságának garantálása [128].

1.3.3 Törvény az elektronikus információbiztonságról

A Magyar Országgyűlés 2013-ban egy korszakalkotónak mondható törvényt (2013. évi L. törvény) fogadott el, az állami és önkormányzati szervek elektronikus információbiztonságáról (a továbbiakban: IBTV). A törvény 2013. július 1-jén lépett hatályba. A napjaink információs társadalmát érő fenyegetések, miatt a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, továbbá az ezt kezelő információs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága a nemzet érdekében kiemelten fontos. A törvény úgy definiálja a felhasználót, mint egy adott elektronikus információs rendszert igénybe vevők köre. Meghatározza továbbá az elektronikus információs rendszert is, mint az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese. Tehát a törvény a felhasználó személyt a rendszer részének tekinti, mint „humán interfészt” [129].

1.3.4 Az Ibtv végrehajtásának szabályozása

Az Ibtv végrehajtására a hatályba lépését követően számos jogszabály lépett életbe és került visszavonásra. A disszertáció készítésekor a hatályban lévő jogszabályok a következők a megalkotásuk szerinti időrendben:

- 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról [130].
- 484/2013. (XII.17.) Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről [131].
- 185/2015. (VII. 13.) Korm. rendelet a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól [132].
- 186/2015. (VII. 13.) Korm. rendelet a központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről [133].
- 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról [134].
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről [135].

A 185/2015. (VII. 13.) Korm. rendelet a disszertáció témáját tekintve azért különösen fontos, mert kimondja, hogy „a sérülékenységvizsgálat tárgya az adatok, információk kezelésére használt elektronikus információs rendszerek, rendszerelemek, eszközök, eljárások és kapcsolódó folyamatok vizsgálata, valamint az ezeket kezelő személyek általános informatikai felkészültségének, és az érintett szervezetnél használt informatikai és információbiztonsági előírások, szabályok betartásának vizsgálata.” Tehát, mint ahogy azt már korábban a törvényi

részben is megfogalmaztam, a felhasználó, mint „humán interfész” a rendszer részét képezve ebben az összefüggésben már a sérülékenységvizsgálat elhagyhatatlan része.

1.3.5 Összegzés

Magyarország információbiztonsági helyzete szabályozott, törvényei és a végrehajtó rendeletei az Európai Uniós és a NATO szabályzásaival harmonizálnak, azoknak megfelelnek. Az új kor társadalmi berendezkedéséből adódó kihívásoknak a szabályozások eleget tesznek. Természetesen, ezen a ponton nem szabad hátradőlni és elégedetten szemlélni a folyamatokat. Az információbiztonsággal foglalkozó szakmai társadalomnak igenis kötelessége a jogszabályalkotók figyelmét felhívni az újabbnál újabb kihívásokra, fenyegetettségekre, valamint az olyan korszerű eljárások bevezetésére, amelyek az információ – mint érték, és erőforrás – biztonságát szolgálják, garantálják.

1.4 Összefoglalás

A fentiekben a kutatásomat megalapozó irodalmi és szabályzói háttér áttekintésével bemutattam témaválasztásom aktualitását és fontosságát, ami a felhasználók digitális kompetenciájának és biztonságtudatosságának növelése. A törvényi szabályozás igen széleskörűen lefedi az elektronikus információbiztonság és a kibervédelem kérdéseit. Ismertettem az Európai Uniónak a digitális kompetencia és a biztonságtudatosság növelésére vonatkozó törekvéseit, azon belül az Európa Parlament és Tanács ajánlását a digitális kompetencia növelésére, mely meghatározó fontosságú hazánk számára is. Vázoltam továbbá az Európai Digitális Menetrendet is, amelynek keretében az európai digitális fejlődésről szóló jelentés, 2017. évi Magyarországot bemutató országprofilja reális képet ad jelenlegi helyzetünkről a többi uniós ország viszonylatában. Nem kezelhető Magyarország az EU-ból kiszakítva a törvényi szabályozás tekintetében, hiszen azzal összhangban kell lennie. A megismert kutatási eredmények is azt mutatják, hogy az EU nem különbözteti meg az egyes tagállamok felhasználóit lakóhelyük szerint, annak ellenére, hogy eltérő politikai és kulturális múlttal rendelkeznek. Az EU minden állampolgárt azonos elvek alapján rendszerez és törvényeit mindenkire azonos módon értelmezi.

A magyarországi digitális fejlesztések keretében a digitális fejlődésre irányuló kormányzati intézkedések is alátámasztják a kutatásaim társadalmi fontosságát és aktualitását. A magyarországi információbiztonsági helyzet és annak változása, valamint előzményei, a törvényi és jogszabályi háttér is jól mutatja, hogy a kormány a minősített adatok védelme tekintetében is elkötelezett az információbiztonság megteremtésében. Ezen belül jelentőséggel

bír az elektronikus információbiztonság- és a kibertér védelmét biztosító jogszabályi hátterének megteremtése. Az informatika, a digitalizáció, a kibertér kialakulása és egyre szélesebb körben való használatának gyors terjedése szükségessé teszi, hogy a jogszabályi háttér ezt kövesse és a fejlődésnek megfelelően szabályozza az információk védelmét érzékenységük szerint.

A kormányzat által készített a Magyarország Digitális Gyermekvédelmi Stratégiája, a Magyarország Digitális Oktatási Stratégiája és a Digitális Jólét Program 2.0, mind azt szolgálják, hogy Magyarország gazdasága és lakossága mielőbb váljon versenyképessé a digitális korban. Ez a stratégia főként a munkavállalókra, valamint a majdani munkavállalókra (gyermekek és fiatalok) koncentrál. A kapcsolódó Új Nemzedék Jövőjéért Program, Magyarország nemzeti stratégiái az élethosszig tartó tanulásra, Magyarország szakpolitikai stratégiája a foglalkoztatáspolitika fejlesztésére, valamint a Digitális Munkaerő Program keretében is a kormány számára az előzőekben megfogalmazottak megteremtése a cél. A magyar kormányzat törekszik a Magyarországon élők és a határon túli magyarság digitális kompetenciaszintjének felzárkóztatására, valamint biztonságtudatosságuk növelése is stratégiai célja.

2 A KÜLÖNBÖZŐ GENERÁCIÓK DIGITÁLIS KOMPETENCIÁJÁNAK ÉS BIZTONSÁGTUDATOSSÁGÁNAK VIZSGÁLATA

A digitális kompetencia a 20. század végétől egyre nagyobb társadalmi és egyéni fontossággal bír. Napjainkban a digitális eszközök és az internet elterjedése miatt elengedhetetlen a legalább alapszintű informatikai ismeret mindenki számára.

A materiális világ veszélyeivel szemben már kialakultak a különböző védekező mechanizmusok. A kiberkorszak csak néhány évtizedre nyúlik vissza. A kibertérben megjelenő támadásokra, a hétköznapi emberek nincsenek felkészülve és nem tudják felmérni azoknak a veszélyességét.

Az alábbi fejezetben kutatásaim eredményeként a vizsgált korosztályok szintjeinek felmérését és a felhasználók ezen szintekhez történő besorolását mutatom be [156][157][158][159].

Magyarországon az informatika és az internet rohamos elterjedése az elmúlt évtizedekre tehető. Az X és az azt megelőző generációkhoz tartozó magyar felhasználók csak felnőtt korukban találkoztak digitális eszközökkel és azok használatával. Az 1965 és 1979 között születetteket nevezi a szociológia X generációnak. Ezen korosztályok munkába állásához nem volt elvárás a digitális kompetencia, hiszen sem az eszközök, sem a digitális infrastruktúra nem volt mindenki számára elérhető. Mindezeken túl ennek a korosztálynak nem volt megfelelő motivációja arra, hogy fejlessze a digitális kompetenciáját és ezzel együtt fejlődjön digitális biztonságtudatossága.

Az említett korosztályok ezért jelentős segítségre szorulnak abban, hogy napjaink digitális kihívásainak megfeleljenek. A digitális kompetencia és ezzel együtt a biztonságtudatosság képzéssel fejleszthető. Az ismeretek szintje jelentős eltérést mutat az azonos korú felhasználók között, amit számos más felmérés és saját kutatásom is alátámaszt. Ennek felmérése, a szintek meghatározása összetett feladat. Kérdőíves felméréssel a felhasználók készségük és jártasságuk szerint különböző szintű csoportokba oszthatók. A különböző szinten lévő felhasználók digitális kompetenciájának és biztonságtudatosságának fejlesztése eltérő ismeret átadásával valósítható meg [156][157][158][159].

2.1 Amit tudni kell a generációkról

A 20. század első harmadában még 33-35 évben határozták meg egy nemzedék biológiai élettartamát. A család életén belül volt nagy jelentőségű a nemzedékváltás időtartama. A szülők

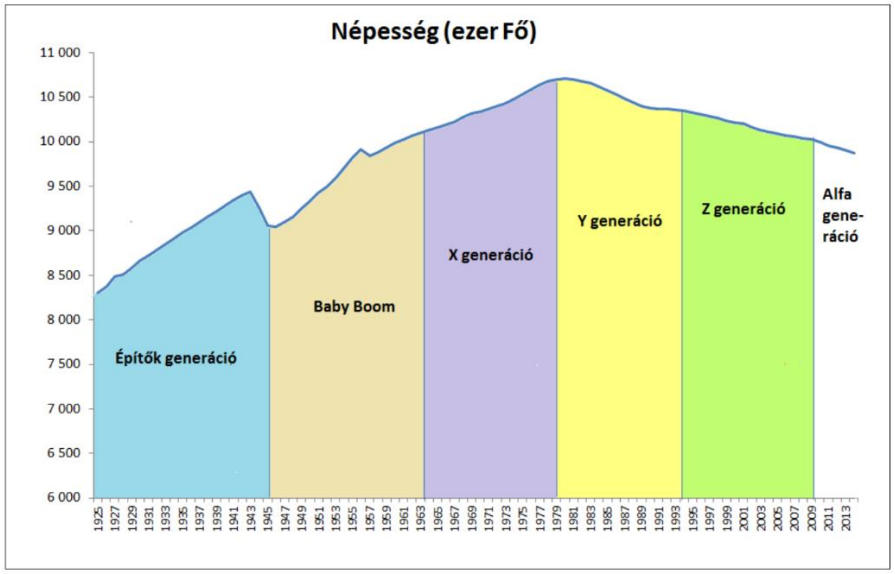
és gyermekeik közötti korkülönbséget 20-25 évben jelölték meg [26]. A mai generáció viszont jóval később vállal gyereket, mint szüleik. Így a szülők és gyermekeik közötti 20 év akár 30 évnél is többre nőhet. Az elmúlt fél évszázad változásaiból eredően nincs még egy olyan fontos generáció, mint az 1980 előtt születettek, akiknek ezt a nagyszámú technikai újdonságot kellett, kell megismernie és használnia [27]. Új kihívásokkal szembesülünk minden nap. Kimondható, hogy a generációs szakadék egyre jobban tátongó mélység [28].

2.1.1 Építők / veteránok – a csendes generáció

Az építő generáció tagjait veteránoknak is nevezik, ők a jelenlegi idős nemzedék. Ez az a korosztály, melynek nagy többsége már nagyszülő, de akadnak olyan szerencsések, akik dédunokájuk cseperedését is megérték, megérik [27]. A válság és a II. világháború idején születtek, a szüleik túlságosan védelmezve nevelték őket, így fiatal szülőként ők már sokkal kevésbé voltak oltalmazók. Azonban csúcsidőszakot élhettek meg már fiatal felnőttként. Jellemző rájuk, hogy ügyesek és nyitottak a világra, alkalmazkodóak, de érzelgősek és határozatlanok is [28].

2.1.2 A Baby boom generáció

Ők a Rock' n' roll korszak gyermekei, azaz a Baby boom, boomerek elnevezést kapták. Ők már a háború után születtek, életüknek meghatározó eseménye volt a háborút követő válság, a gazdasági növekedés, a technológiai fejlődés [29].



3. ábra A magyar népesség alakulása generációk tükrében (forrás: KSH[18]) [28]

[18] KSH – Központi Statisztikai Hivatal

Az amerikai angol ezt a szemléletes kifejezést használja a kor szülötteire, mert a születések száma ekkor robbanásszerűen megugrott [30]. Még Magyarországon is több mint 12 %-kal nőtt a népesség száma (3. ábra). A gyermekkoruk által megalapozott kíváncsiság jellemző a korszak elején születettekre, mert fontos számukra a tisztesség, az emberiesség és a szeretet. Az 1956 után születettekre inkább a kiábrándultság és a cinizmus jellemző, az optimista szemléletből sokat veszítettek. Ennek a korosztálynak az idősebbjei már nyugdíjban vannak, a fiatalabbak még aktív keresők [26][28].

2.1.3 Az X generáció

Az X generáció elnevezést először Robert Capa (Fiedmann Endre), magyar származású fotós használta egy 1953-as, II. világháború után születettek szereplésével készült fotósorozatának elnevezésére. Az X az ismeretlent jelöli, ami később Douglas Coupland „X generáció" című regénye nyomán került a köztudatba. Az X generáció a szellemi, spirituális ébredés alatt születetteket jelöli, akiknek szülei már kevésbé óvták, védelmezték gyermekeiket, mint az őket megelőző generáció. Az X generáció eszes, gyakorlatias és jó ítélőképességű [31]. A korosztály többsége szüleinél iskolázottabb, és már nem csak a kötelező orosz nyelvet tanulta. A hetvenes évek végétől születettek már kamaszként is használják a számítógépet, és mindenki saját tempójának megfelelően elkezdi használni a technika legújabb vívmányait. A munka területén a pénz, a karrier és a státus a motiváló erő. Marc Prensky (2001) találóan digitális bevándorlóknak címkézi ezt a nemzedéket [32]. Az elnevezés találó metafora, hiszen sokan nem a mai modern világban születtünk, hanem gyorsabban vagy lassabban, bosszankodva vagy lenyűgözve használni kezdtük a digitális világ új vívmányait [28][156][157][158][159].

2.1.4 Az Y generáció

A bennszülött, őslakos kifejezést használják erre a generációra. Mert minden bennszülött rendelkezik a saját terepén valami olyan tudással, ami a „civilizált" ember számára ismeretlen. Egyes források szerint az elnevezés a fiatal (az angol Youth - fiatalság, ifjúság) szó rövidítése, mások szerint egyszerűen az Y az X betűt követi az ABC-ben [30]. Ők a mai 20 – 30 évesek. Nevezik őket millenáris vagy ezredfordulós generációnak, net-generációnak is, és rengeteg más címkét is kaptak jellemzőként. Magyarországon még szocializmus volt, amikor megszülettek, de már demokráciában nőttek fel. A szüleik védelmezve nevelték őket, mindent megadva gyermekeiknek az anyagiakat tekintve [33]. Ők sokszor a számítógépekkel együtt nőttek fel, és nem a közös családi társasjátékozással [27]. Irigylésre méltó képességük, kompetenciájuk, hogy mesterei az internetnek, a számítástechnikának, az információs technológiának [28].

2.1.5 Az Z generáció

A Z generáció (az 1994 és 2010 között születettek) a világ első globális nemzedéke. Jellemző rájuk, hogy érzékenyek és okosak, legalábbis a digitális világ területén. Ők már teljes egészében beleszülettek a különböző digitális technológiák világába. Természetes számukra, hogy állandó kapcsolatban vannak egymással, virtuálisan naponta rengeteg emberrel kommunikálnak, a közösségi oldalakon több száz baráttal rendelkezhetnek [34]. Kábítószerként hat rájuk a digitális tér, ahol minden megvalósulhat. A Z generáción belül a legfiatalabbakat már C generációként[19] emlegetik [28].

2.1.6 Az Alfa generáció

Azért nevezik őket a társadalomkutatók, szociológusok "alfa" generációnak (2011. után születettek), mert remélik, hogy velük újra kezdődik minden, új lehetőséget kapnak, amivel élni is tudnak majd [30]. Bízni kell abban, hogy képesek lesznek a kihívásokkal megbirkózni. Ügyesebbek, gazdagabbak, egészségesebbek és magányosabbak lesznek a legfiatalabb generáció tagjai [32]. A legtovább fognak élni az emberiség történetében, a legmagasabb iskolai képzettséggel rendelkeznek majd és teljes mértékben a világháló részei lesznek [28][36].

2.2 A digitális korszak

Az Európai Uniós elvárásoknak megfelelően a magyar kormányzat által kitűzött célnak, a lakosság digitális kompetenciaszint-növelésének fontossága mostanára már nem lehet kérdés. A felhasználók digitális kompetenciaszintjének növelése képzéssel valósítható meg. A célzott kutatási eredmények elemzésével és felhasználásával hatékonyabbá tehetőek ezek a képzések. A digitális tudás olyan növekedését kell elérni, amelynek eredményeképpen a digitális javak közel azonos módon elérhetővé válhatnak mindenki számára. Ez azért fontos, mivel a kutatásom is alátámasztja azt, hogy a megkérdezettek szinte mindegyike használja az internetet, de eltérő készségekkel, képességekkel. A munkahelyek és a szakmák döntő többségéhez szükséges valamilyen mértékben a digitális írástudás képessége, melyet a későbbiekben a kutatásom is bizonyít, tehát nem mindegy a munkavállalók és a cégek számára sem, hogy az alkalmazottak milyen szintű digitális ismeretekkel rendelkeznek, illetve fognak rendelkezni.

Magyarország kormánya, mint minden más fejlett világbeli állam kormánya, felismerte azt a fontos problémát, amely az elmúlt húsz évben generálódott és gyorsult fel, ami nem más, mint a digitális kompetencia hiánya a magyar lakosság körében. Az internet, mint infrastruktúra

[19] Az angol „connecting” (folyamatosan kapcsolatban lévő) szóból ered a megjelölés, utalva arra, hogy a közösségi oldalhoz kapcsolódva, kezükben telefonnal alszanak el és kelnek fel.

fejlődésének hatására a gazdasági szereplők is egyre nagyobb hangsúlyt fektetnek a digitális fejlesztésre. Az elmúlt 20 évben nagyszámú olyan új iparág fejlődött ki, amely kimondottan a digitalizációra épül. Gondoljunk itt a web-áruházakra, a digitális geopozíció meghatározásra épülő szolgáltatások terjedésére, de akár az egész online világra. Az infokommunikáció adta lehetőségek egyre népszerűbbek és nagy a penetrációjuk. Az ipar esetében beszélhetünk az ipar digitális transzformációjáról, a 4. Ipari forradalomról, ami Ipar 4.0 néven ismert, és napjainkban is zajlik. Tehát belátható, hogy egy új képesség elsajátítására van szüksége a mai kor dolgozó és felnövekvő generációinak, mégpedig a digitális kompetenciára [160].

2.2.1 A digitális javak

Az információ, avagy tudás alapú társadalom résztvevői részéről az egyik legalapvetőbb elvárása a társadalom irányába, hogy biztosítsa számukra a javakat. Ezek a javak jelen esetben digitális javak, mint például az elektronikus kereskedelem, a banki ügyintézés, az oktatás, egyéb ügyintézések és még sorolhatnánk. A társadalom részéről viszont alapvető elvárás az egyes tagjaival szemben, hogy azok a részükre biztosított digitális javakat elérjék, használják, és boldoguljanak vele, tegyék jobbá az életüket. Természetesen mindezt úgy, hogy az mindenki számára megnyugtatóan biztonságos legyen. Az egyén ugyanolyan felelős azért, hogy a részére biztosított javakat el tudja érni, mint maga a társadalmat irányító vezetés. Tehát nem mondható el az, hogy kizárólagosan az állam feladata a lakosság ilyen irányú képességének növelése, mert a kormányzati törekvések mind hiábavalóak a társadalmi elvárások teljesítése érdekében, hogyha az egyén nem tesz semmit azért, hogy a célját elérje [161][162].

2.2.2 A digitális jólét

Az egyén jól felfogott érdeke, hogy megtanulja használni azokat a közműveket, amelyek a jólétét szolgálják. A 20. században az iparosításnak köszönhetően az emberek számára elérhetővé vált a villamos hálózat, a vezetékes ivóvíz, a vezetékes földgáz, a csatornahálózat, a telefonhálózat. Majd a 20. század végén megjelent a legnagyobb közcélú informatikai hálózat, az internet. Az internet infrastruktúráján pedig a 20 éve nagy penetrációval bíró világháló mindenki rendelkezésére áll.

Az elmúlt fél évszázadban, ami az informatika igazi robbanásszerű fejlődését hozta magával, amely az információs rendszerek terjedését generálta, az emberek egyre szélesebb tábora találkozott a mindennapjaiban a számítógép-rendszerekkel. Szélesedett az oktatási paletta is ezen a területen. Az internet terjedését a már korábban említett világháló, az úgynevezett WorldWideWeb megjelenése segítette. Aztán a kétezres évek elején, közepén megjelentek az első okos (smart) telefonok, melyek alkalmasak voltak az internetelérésre. Természetesen

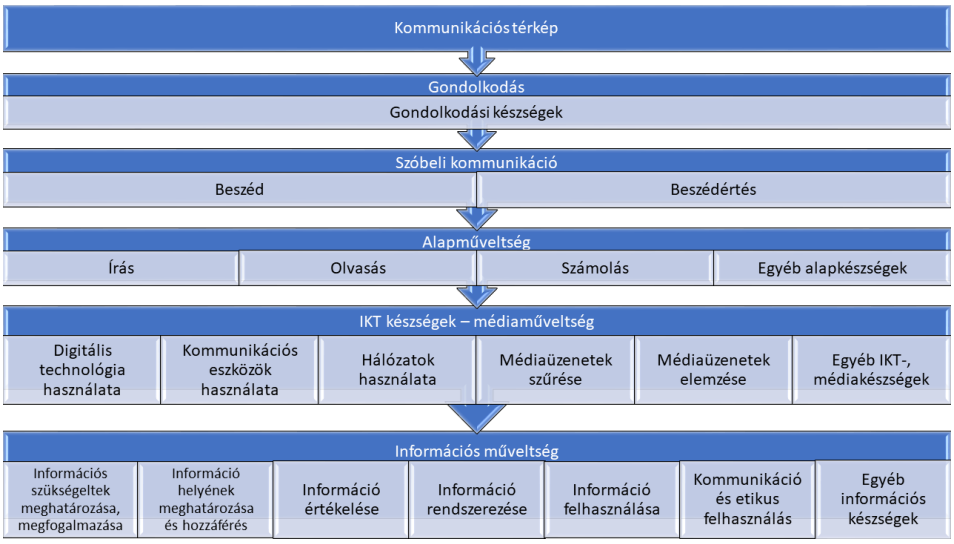
ehhez a mobil szolgáltatók és a kábel tv szolgáltatók hatalmas fejlesztésére is szükség volt. Azzal, hogy mindenütt megjelent az informatika, az életünk könnyebbé vált. Gyorsabban, olcsóbban, egyszerűbben tudunk ügyintézni, vásárolni, bankolni, kapcsolatot tartani távoli és közeli ismerőseinkkel, családunkkal, barátainkkal [156][159].

2.3 A digitális kompetencia

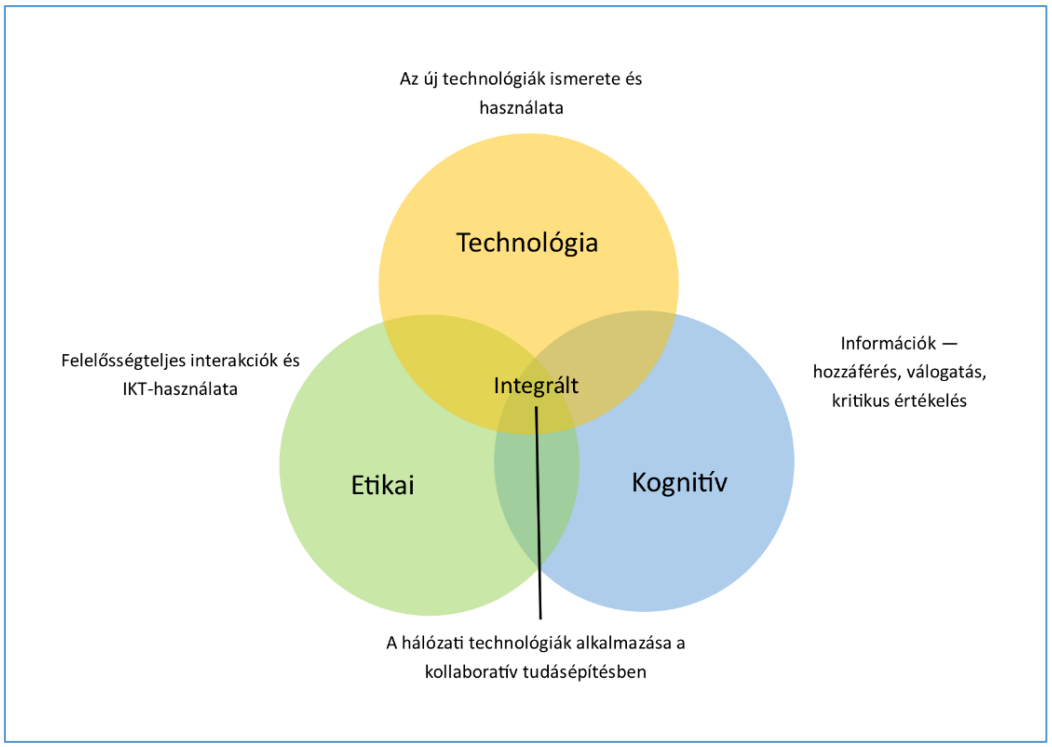
Az 1980-as években, illetve az 1990-es évek elején a szakirodalomban jellemzően még a számítógépes műveltség fogalommal találkozhattunk, amely a számítógép-használathoz szükséges alapismeretek meglétére, illetve az alkalmazásukban való jártasságra utalt. Ezen eszköztudást méri az 1996-ban útjára indított, és a mai napig népszerű ECDL (European Computer Driving Licence – Európai Számítógép-használói Jogosítvány) vizsga, amelynek keretében többféle tanúsítványt is lehet szerezni. Ezen vizsgát eddig közel 13 millió ember (Magyarországon 440 ezer fő) tette le sikeresen. Az ECDL követelmények és a modulok is jelentős változásokon mentek keresztül az évek során, például 2013 októberében megjelent az *IT biztonság* ECDL modul is, és több modul elnevezése is megváltozott, a korábbi *Internet és kommunikáció* modul új neve *Online alapismeretek* (online essentials) lett [36].

2.3.1 A digitális kompetencia dimenziói

Az információs és kommunikációs technológiák alkalmazásával kapcsolatos készségek a legalapvetőbb szinten a multimédiás technológiájú információk keresését, értékelését, tárolását, létrehozását, bemutatását és átadását, valamint az internetes kommunikációt és a hálózatokban való részvétel képességét foglalják magukban [36].



4. ábra Az UNESCO kommunikációs készségtérképe (forrás: DJP 2.0; készítette a szerző) [37]



5. ábra A digitális kompetencia dimenziói (forrás: Calvani és tsai, 2008) (Készítette a szerző) [35][160]

A lakosság, a vállalkozások és a közigazgatás digitális kompetenciájának fejlesztése, a digitális írástudás növelésével és a digitális megosztottság mérséklésével valósítható meg úgy (4. ábra), hogy képessé teszi a felhasználókat az infokommunikációs rendszerek bevezetése által előálló üzleti lehetőségek felismerésére és kihasználására, valamint a tartósan leszakadókat a digitális ökoszisztéma előnyeiben való részesedésre, azaz az e-befogadásra [34][160].

Antonio Calvani és társai (Calvani és tsai, 2008) tanulmányukban a digitális kompetenciát három dimenzió együtteseként definiálják (5. ábra). Az egyik technológiai dimenzió, amelyben a problémamegoldás képessége és a változó technológiai környezethez való rugalmas alkalmazkodás kap elsősorban szerepet, a másik a kognitív dimenzió, melynek lényege az információk „olvasása”, szelekciója, értelmezése, értékelése és bemutatása, valamint egy etikai dimenzió, a másokkal való kapcsolattartás és kommunikáció a technológia felelősségteljes alkalmazásával [35][160].

Továbbá fontos még a digitális kompetencia, a digitális média magabiztos és kritikus alkalmazása munkában, szabadidőben és a kommunikáció során. Ez a képesség, a logikus és kritikus gondolkodáshoz, a magas szintű információkezelési és fejlett kommunikációs készségekhez kapcsolódik. Az infokommunikációs technológiák felhasználásával kapcsolatos készségek a legelemibb szinten a digitális tartalmak, információk keresését, értékelését,

tárolását, létrehozását, bemutatását és átadását, valamint az internetes kommunikációt és a közösségi hálózatokban való részvétel képességét foglalják magukban [39][160].

2.3.2 A digitális írástudás

A digitális írástudás több típusú műveltséget fog át, a funkcionális írástudás keretébe illesztve az írást, az olvasást és a számolást. Magába foglalja az értő olvasást, a megszerzett információk kritikus kezelését. Ennek a fajta írástudásnak a részét képezik a könyvtárak használatához, a keresési stratégiák alkalmazásához szükséges készségek, az információforrások és a talált információ értékelésével, kritikus kezelésével kapcsolatos készségek – ideértve a tömegkommunikációs eszközök közvetítette információk – kezelését, azaz a már említett média-írástudást [40][160].

A digitális írástudás tudatosság, beállítódások és képességek olyan együttese, amely lehetővé teszi, hogy megfelelően és biztonságosan használjuk a digitális eszközöket és intézményeket a digitális források azonosítására, elérésére, kezelésére, integrálására, értékelésére és szintetizálására, továbbá új tudás és média megnyilvánulások létrehozására, valamint arra, hogy másokkal kommunikáljunk és reflektáljunk erre a folyamatra [41][160].

2.3.3 A digitális kompetencia fontossága

Az alkalmazott digitális eszközöket kezelni tudó szakemberekre egyre nagyobb szükség van. A korszerű szakmai ismeretek megkövetelik a digitális eszközök ismeretét a meglévő „hagyományosnak” mondott szakmák tekintetében is. Akkor tud egy dolgozó hatékonyan dolgozni, hogyha nem jelent számára kihívást a „munkagépének” a kezelése. A digitalizációnak a fent említett megjelenése a mai 35 éves és annál idősebb korosztály esetében jelent igazi kihívást a munkavállalók körében. A korábban tanultak már elévültek. A cégek nem, vagy csak kis számban képeztetik át a saját munkavállalóikat [160]. A digitális alapkészségekkel nem rendelkezők magas aránya a nemzetgazdaság szintjén a növekedés és a foglalkoztatás korlátjaként jelenik meg, egyben komoly társadalmi feszültségek forrása és a szociális egyenlőtlenségek újratermelődésének egyik okozója. A modern technológia elutasítása főként kognitív eredetű és leginkább a vidéki, alacsony státuszú és végzettségű, 45-70 év közötti felnőttekre jellemző. Mind a hazai kezdeményezések, mind a nemzetközi tapasztalatok azt jelzik, hogy csak szisztematikus beavatkozással, helyi szintű, integrált programokkal és a lemaradás valamennyi dimenziójára kiterjedő komplex szemléletformáló programokkal lehet érdemi eredményeket elérni a felzárkóztatásban [42].

PK Agarwal, a Szilícium-völgyben található Northeastern University dékánja és igazgatója szerint néhány éve az informatikusok az adatmenedzsmentről beszéltek, ma pedig már az IoT[20]-ről és a devops[21]-ról [43]. A témák változnak, de a szükséges készségek nem, teszi hozzá a szakember. A mai IT-vezetőknek jobban kell támaszkodniuk a soft skill-ekre és az érzelmi intelligenciára, ha azt szeretnék, hogy mind a vállalaton belül, mind a külső partnerekkel jól megértsék egymást. Az automatizáció és az önkiszolgáló informatika terjedése miatt pedig végképp el kell kötelezniük magukat az élethosszig tartó tanulás mellett.

A digitális kompetencia hatása a GDP-re

A digitális kompetenciának a GDP-re gyakorolt hatása figyelemre méltó, mert a digitális írástudás 1%-os emelkedése a GDP-ben 0,123%-os növekedést, azaz 34,7 Mrd GDP többletet eredményez. Az infokommunikációs és az IT ipar alkotta IKT-szektor a magyar GDP mintegy 12%-át adja, és az ágazatban foglalkoztatottak száma az OECD országok többségével összevetve kiemelkedően magas hazánkban [38][160].

A NIS irányelvek a digitális kompetenciáról

A NIS irányelvekben a digitális kompetencia SWOT[22] analízisében a „Gyengeségek" között szerepel, hogy az uniós átlag alatti a digitális kompetencia szintje a magyar lakosság körében. Aminek okai, hogy negatív attitűddel rendelkeznek a felhasználók, valamint az 50 év felettiek közül a lakosság kevesebb, mint a fele írástudó, és a 8 általánossal rendelkezők körében vészesen alacsony az internet-használat. Továbbá nagyon az átlag alatt van a munkanélküliek és inaktívak digitális kompetenciája. Az állampolgárok nincsenek tisztában az infokommunikációs lehetőségekkel. A fejletlen régiók lakói esetében alacsony az internet-használat. Az átlag felhasználók között magas a kizárólag alapszintű szolgáltatások és alacsony a tranzakció-alapú szolgáltatások használata. Valamint az internet-használók körében **hiányzik a tudatosság és a társadalmi felelősségvállalás**. Ide sorolja még az analízis a köznevelést érintő problémákat, a pedagógusok motiválatlanságát és felkészületlenségét.

A NIS irányelvek SWOT analízisében a „Veszélyek" között található még, hogy az 50 év feletti korosztályoknál a nagyon alacsony digitális kompetenciaszint miatt a foglalkoztatási esélyek jelentősen romlanak. A lemaradó régiók versenyképessége romlik. A munkanélküliek digitális készségének hiánya akadályozza a (re)integrációt. A leszakadó rétegek esélyegyenlősége

[20] IoT – internet of thigs, dolgok internete
[21] DevOps - fejlesztés (**Dev**elopment) és az üzemeltetés (**Op**eration**s**)
[22] SWOT-analízis (Strengths – erősségek; Weaknesses – gyengeségek; Opportunities – lehetőségek; Threats - veszélyek)

tovább romlik. A digitális kompetencia hiányával küzdők nagy száma további gazdasági terheket jelent a társadalomnak [38]. Ezen megállapítások mindegyike alátámasztja az általam végzett kutatás eredményeit a különböző generációk és eltérő iskolai végzettséggel, valamint infrastruktúrával rendelkező felhasználók digitális kompetenciájának és biztonságtudatosságának nagyfokú eltérését.

2.3.4 A digitális kompetenciával és a biztonsággal kapcsolatos felmérések

Felismerve a digitális kompetencia biztonsági aspektusait és az abban betöltött szerepét, az UNICEF Magyar Bizottsága, valamint az Európai Bizottság és a Nemzeti Média és Hírközlési Hatóság (NMHH) egymástól függetlenül, de hasonló témában és hasonló korosztály körében végzett felmérést, amelyet az alábbiakban mutatok be (6. ábra) [160].

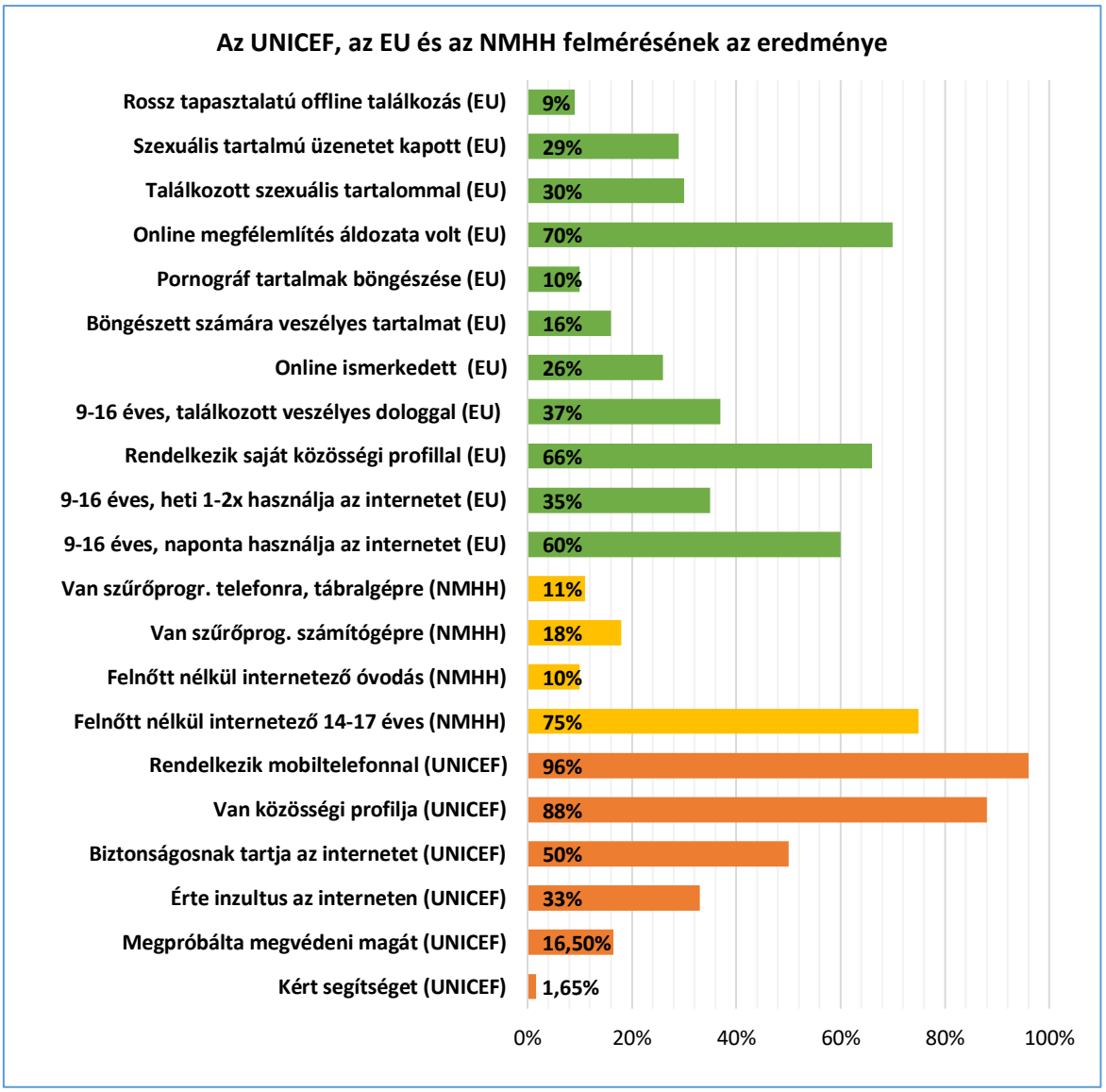
UNICEF Magyar Bizottságának felmérése

Egy 2014 őszén elvégzett nem reprezentatív kutatás az UNICEF Magyar Bizottsága által a gyermekjogokról és az internetes biztonságról elvégzett nem reprezentatív kutatás az alábbi eredményt adta, amelyet 1191 fő, 10-19 éves általános- és középiskolai diák bevonásával készítettek. A megkérdezettek 96%-a rendelkezik mobiltelefonnal, és 88%-nak van profilja valamilyen közösségi oldalon. A felmérés alapján a gyermekek 50%-a nem tartja biztonságosnak az internetet. A gyermekek 33%-át érte már kellemetlen “piszkálódás” az interneten. Az ilyen esetekben a sérelem áldozataivá vált gyermekek fele megpróbálta megvédeni magát, de segítséget csak 10% kért [18][160].

Az EU Kids Online nemzetközi felmérése

Az Európai Bizottság Biztonságos Internet Programjának támogatásával, 25 országban végzett felméréssel készült el az EU Kids Online nemzetközi tanulmánysorozat. A felmérés alapján, a magyar gyermekek átlagosan 9 éves korukban kezdik el önállóan használni az internetet. Az előrejelzések azt prognosztizálják, hogy ez az életkor csökkeni fog, valószínűleg 5-6 éves kor környékén fog stabilizálódni. A 9-16 éves korosztály 60%-a napi rendszerességgel internetezik, ezzel szemben 35% körül van azoknak a gyermekeknek az aránya, akik hetente egy-két alkalommal interneteznek. A korosztály kétharmada rendelkezik saját profillal a közösségi oldalakon. A magyar 9-16 éves korosztály 37%-a találkozott már kockázatos tevékenységek közül legalább eggyel az online térben. A gyermekek 26%-a már ismerkedett online módon. A gyermekek 16%-a böngészett már veszélyeket rejtő tartalmak között. A pornográf tartalmak böngészésében minden tizedik gyermeknek van tapasztalata. A megkérdezett gyermekek közel 70%-a volt már áldozata online megfélemlítésnek. Szexuális tartalmakkal a gyermekek 30%-a

találkozott, szexuális jellegű üzenetek és cselekvések a gyermekek 29%-át érintették. A gyermekek 9%-ának volt része olyan rossz tapasztalattal végződő „offline” találkozásban, amelyet online ismerkedés előzött meg [18][160].



6. ábra Az UNICEF, az EU és az NMHH felmérésének eredménye (forrás: UNICEF, EU, NMHH; Készítette a szerző) [18][160]

Az NMHH[23] felmérése

A 14 és 17 év közötti gyerekek 3/4-e szokott úgy internetezni számítógépen, hogy nincs jelen felnőtt. Az óvodásokkal egy háztartásban élő internethasználók 10%-a nyilatkozott úgy, hogy a velük együtt élő, 6 évnél fiatalabb gyerekek, felnőtt segítsége nélkül, táblagépen vagy telefonon szoktak egyedül internetezni, derül ki egy az NMHH által 2013-ban lefolytatott felmérésből. A megkérdezettek elenyésző része válaszolt úgy, hogy ő vagy szülője telepített

[23] Nemzeti Média és Hírközlő Hatóság

szűrőprogramot a gyermek által használt számítógépre (18%) vagy telefonra, táblagépre (11%) [18][160].

2.3.5 Összegzés

A felnőttek digitális kompetenciájának fontossága a fentiek alapján nem is kérdéses. A kormányzati stratégiák dícséretes módon a gyermekek digitális kompetenciájának és azon belül is a digitális írástudásnak a növelését tűzték ki célul. Sajnálatos azonban, hogy ezek nem terjednek ki a lakosság többi részének esetében a digitális kompetencia és a digitális írástudás fejlesztésére. Amennyiben a cégek, vállalkozások kapnának államilag támogatott oktatási lehetőséget az alkalmazottak általános digitális kompetenciájának növelésére, abban az esetben az általános digitális kultúra a magyar lakosság körében hatalmas növekedésnek indulna, amely a nemzetgazdaság növekedését is szolgálná.

A fentiekből kitűnik, hogy a szülők, az oktatók és a pedagógusok tudatossága is kulcsfontosságú a terület szempontjából. Amennyiben a gyermekek oktatásában, nevelésében szerepet vállaló személyek nem rendelkeznek megfelelő digitális tudással, valamint ezek átadásának szándékával és képességével, úgy az súlyos következményekkel járhat a gyerekekre nézve. Sajnálatos módon igen kicsi azon pedagógusok aránya, akik a szükséges digitális készségekkel rendelkeznek. Számos civil szervezet folytat képzéseket, amelyek nem kizárólag a gyermekek, de a pedagógusok ismereteinek bővítését is megcélozták. Tévhit azonban az idősebb, nyugdíjas generáció vonatkozásában, hogy egy bizonyos kor felett már nem sajátítható el a szükséges digitális kompetencia. Az élethosszig tartó tanulás („lifelong learning") a nyugat-európai társadalmakban sikeres, államilag támogatott kezdeményezés és folyamat, melynek pozitív hatása nem csak az érintetteken mérhető [18][160].

2.4 A biztonságtudatosság és a digitális kompetencia kapcsolata

A generációknak az előző részben lévő bemutatásából látszik, hogy mindegyik generációnak más és más az általános viselkedési kultúrája, ami nagyban kihat a biztonságtudatosságra is. A biztonságtudatosság fontossága a mai világunkban nem kérdőjelezhető meg [44]. Az informatika és az internet robbanásszerű fejlődése társadalmi változásokat hozott magával. Az iskoláskorúak számára az informatika oktatása és a digitális kompetencia fejlesztése már egész kora gyermekkortól kezdődően biztosított. Azonban nem csak az említett korosztálynak szükségesek a felsoroltak, hanem a társadalom teljes egészének [45]. A mai kor emberének az élethosszig tartó tanulás biztosítja azt a tudást, amivel piacképes lehetőséget tud teremteni magának [46]. Az ipar digitalizációja korunk kihívása, mely új lehetőségeket nyit meg, ezt a

modernizálódási folyamatot Ipar 4.0-nak vagy negyedik ipari forradalomnak nevezik [47]. Korunkban a legfontosabb digitális vívmányok, mint a felhő technológia (cloud technology), a dolgok internete (IoT), a mesterséges intelligencia (artificial intelligence) stb. egyre szélesebb körben ismertek és alkalmazottak. A hagyományos gyártórendszerek és gyártási eljárások optimális működtetése már az internetes alkalmazások támogatásával valósul meg [48]. Ahhoz, hogy az Ipar 4.0 által forradalmasított gazdaság jól működjön, elengedhetetlen a rendszerek „leggyengébb láncszemének", az ember tudásának és tudatosságának az elvárt szintre történő emelése [49]. Hiába alkalmaznak a gyárak modern technológiát, technikát, hogyha azt a felhasználó tudásának vagy a tudatosságának hiányában nem tudja optimálisan, biztonságosan üzemeltetni [164]. A biztonságtudatosság és a digitális kompetencia kapcsolatának kutatása céljából egy olyan kérdőívet állítottam össze, amelynek a kérdéseire kapott válaszok kiértékelésével, majd az eredményekből megállapított összefüggések alapján javaslatokat tudok kidolgozni a képességek és készségek fejlesztése érdekében a digitális-társadalom egyenlőtlenségeinek felszámolására [156][157].

2.5 A kutatás aktualitása

Az általam lefolytatott kérdőíves kutatás a biztonságtudatosság és a digitális kompetencia kapcsolatáról azt a célt szolgálja, hogy felmérjem a válaszadók körében hogyan érvényesülnek, és milyen arányban vannak jelen a válaszadók körében a korunk kihívásainak megfelelő informatikai ismeretek és a hozzá kapcsolódó biztonság. A kérdőív válaszai alapján levont következtetések felhasználásával elkészítettem egy olyan, a felhasználók digitális kompetenciájának felmérésére szolgáló keretrendszert, amely tartalmazza a biztonságtudatosságra és a tudásátadásra vonatkozó osztályt és szinteket is, valamint tartalmaz egy új szintet, amely a „teljesen kezdő" elnevezést kapta és ezzel kapcsolatban fogalmaz meg definíciókat. Kutatómunkám során az Európai Unió által összeállított digitális kompetencia keretrendszer esetében találtam meg azokat a számomra szükséges alapokat, amelyek a keretrendszer megalkotásához és a további kidolgozáshoz alapot tudnak szolgáltatni. Ennek oka az, hogy az Uniós keretrendszer esetében olyan követelményeket támasztottak és úgy értékeltek, ami az aktív munkavállalók és a munkáltatók sikeres egymásra találását segíti [50]. Ez azonban általában a nyugat-európai munkavállalók képességeit veszi alapul. Sajnos a régió munkavállalói a történelmi sajátosságokból adódóan a nyugatitól eltérően szocializálódtak. Ebből kifolyólag, különbözik az értékrendjük, mások a társadalmi szokásaik, az oktatási körülményeik, a lehetőségeik, a viselkedésük. Eltérő lehet a kulturális beállítottságuk, és különbözik az intelligencia szintjük is. Ami szembetűnően hatalmas szakadékot jelent, az a

társadalmak közötti jövedelemarány. Ebből adódóan más elvárásokat szükséges a saját régiónk polgáraival szemben felállítani, mint a nyugati társadalmakban élők esetében. Így szükség volt egy olyan keretrendszer megalkotására, amely az erre a társadalomra jellemző tulajdonságokat is tartalmazzák és lefedik a munkavállalókon felül azokat a társadalmi rétegeket is, amelyek már nem, vagy még nem férnek bele munkavállalói csoportba [51]. Például a gyerekek vagy fiatalkorúak, akik még nem dolgoznak, illetve azok a szépkorúak, akiknek a munkavállalásához még nem volt szükség a digitális kompetenciák meglétére.

Kutatásaim alapján, ha azok a szempontok is érvényesülnek, amelyekkel megalkottam a keretrendszert, abban az esetben teljes mértékben alkalmazható lesz mindannyiunk számára, akik ebben a régióban élünk. Ennek alapján a felhasználók fel tudják mérni a saját digitális képességeiket, a munkaadók, illetve az iskolák pedig képet kapnak arról, hogy a munkavállalóik és tanulóik milyen szintű digitális ismeretekkel rendelkeznek. Továbbá fény derülhet mindenki számára arra is, hol vannak hiányosságok a képességekben és mely területek azok, amelyeket már nem kell vagy nem szükséges fejleszteni. Ezáltal jelentős időt és pénzt lehet megtakarítani, valamint optimalizálni lehet a leendő, aktív és a már nem aktív munkavállalók, oktatását, képességeik fejlesztését is [158][159].

A kérdőív háttere

A kérdőívet először papír alapon készítettem el, amelynek kitöltésében azon rétegek válaszaira számítottam, akik valamilyen oknál fogva nem túl aktívak a digitális térben. Digitális megoldásként rátaláltam a GoogleForm alkalmazásra, amely praktikussága, hatékonysága miatt alkalmasnak bizonyult az online formájú válaszadásra, a válaszok gyűjtésére és kiértékelésére is. A kérdőívet először magyar nyelven készítettem el, alapvetően a magyar nyelvű felhasználók válaszainak felmérésére. Ezt követően készítettem el a nemzetközi válaszadók elérése érdekében az angol nyelvű változatot [52]. A kérdőív linkjének a potenciális kitöltőkhöz történő eljuttatására az e-mail formátumot választottam. Mivel úgy ítéltem meg, hogy a személyes hangvétellel hatékonyabb a felhasználók megszólítása egy ilyen jellegű megkeresés esetén, mintha egyéb közösségi médián keresztül kerestem volna meg őket. Természetesen nem én voltam az, aki minden egyes lehetséges válaszadónak elküldtem a linkeket tartalmazó e-mailt. Erre úgynevezett kulcsfelhasználókat kértem meg. Az általam a kulcsfelhasználók részére kiküldött e-mailek száma nem haladta meg a 100-as nagyságrendet. Ez természetesen nem jelenti azt, hogy minden kulcsfelhasználó továbbította volna a levelet, akinek én elküldtem. Az általam választott kulcsfelhasználók mindegyikével személyes ismeretségben állok. A tanulmányaim során megismert hallgatótársaimnak, tanáraimnak, más egyetemek tanárainak,

hallgatóinak küldtem el a kérdőívet. Segítségként használtam még az Óbudai Egyetem NEPTUN rendszerét is, melyen keresztül az egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, valamint az Óbudai Egyetem Biztonságtudományi Doktori Iskola hallgatói és tanárai részére a Kar dékánjának engedélyével került kiküldésre a kérdőív linkjét tartalmazó e-mail. Kifejezetten ügyeltem arra, hogy általánosságban ne tegyem közzé semmilyen közösségi médián a kérdőívet. Továbbá nem küldtem el olyan személy részére a kérdőívet tartalmazó levelet, aki nem válaszolt a segítségkérésemet tartalmazó üzenetre. A válaszadók többsége magyarországi magyar személy volt. A magyar nyelvű kérdőívet határon túl élő szerbiai és romániai magyarok is kitöltötték. Az angol nyelvű kérdőív kitöltésében elsősorban a közép-kelet-európai régió felhasználóinak aktivitására számítottam. A kérdőívet nagy számban orosz és román felhasználók töltötték ki, emellett szerb, szlovák, cseh, lengyel, albán, macedón felhasználók is megtiszteltek a válaszaikkal. A külföldiek számára szánt angol nyelvű kérdőívet a nemzetközi kapcsolatok segítségével, általában a korábbi határon túli konferenciák alkalmával kialakított kapcsolatrendszerek segítségével sikerült szétküldeni. Az angol nyelven megküldött segítségkérő e-mailek száma, amit én küldtem el, megközelíti a tizenötöt [53]. Azonban előfordult az is, hogy az egyetemi ismerőseim külföldi kapcsolatainak segítségével került kiküldésre a külföldieknek szánt kérdőív. Arról sajnos nincs tudomásom, hogy a megkeresett ismerőseim mennyi angol nyelvű emailt küldtek szét a külföldi ismerőseiknek. Ebben az esetben arra ügyeltem, hogy a kérdőív a régió országaiban maradjon elsősorban, és a kapott válaszokkal bizonyítani tudjam azt a hipotézisemet, hogy az általam megalkotott keretrendszer lefedi a régió és benne a magyarországi felhasználók digitális kompetenciáinak értékelendő részét. Sajnos arról sincs információm, hogy mennyi külföldihez jutott el a megkeresés pontosan és abból arányaiban hányan válaszoltak [54][156][157].

2.6 A kérdőívből nyert információk felhasználása

A keretrendszer megalkotásának érdekében további célom még az volt, hogy azon felhasználók számára is elérhető legyen egyfajta képességmérő rendszer, akik már nem az aktív munkavállalói rendszerhez tartoznak. A válaszadók kulturális és egyéb különbségekből fakadó válaszai alapján megállapítható, hogy a keretrendszer egy része a válaszok alapján megfogalmazott szempontok miatt szükséges. Azok az időskorú felhasználók, akik életük során nem találkoztak még a digitális eszközökkel és az azok által elérhető lehetőségekkel, vagy nem voltak rákényszerülve arra, hogy ezeket használják, az egyik említett felhasználói réteg. Jelen korunkban, ezzel szemben – habár már hosszú évtizedekre teltek el a digitális kor kezdete óta– ezek az emberek egyfajta robbanásszerű dologként élik meg azt, hogy most már bárki zsebében

ott lehet az internet [55]. Ennek a felhasználói rétegnek a biztonságtudatosságával igazából nincs probléma, mert bennük már kialakultak a védekező reflexek a fizikai világban. Viszont ha használják a digitális technológia által nyújtott lehetőségeket, nem tudják, hogyan védekezzenek a digitális veszélyekkel szemben. Amennyiben nem használják ezeket a lehetőségeket, akkor saját magukat rekesztik ki a társadalmi élet újszerű formájából. Mindezt teszik úgy, hogy sokszor nincsenek tisztában azzal, hogy miről is mondanak le azzal, hogy önként vagy külső kényszerből kirekesztik saját magukat. Fennáll azonban annak a veszélye ezen felhasználók esetében, hogy ezzel a választásukkal olyan mély társadalmi szakadékot generálnak, amely egyéb társadalmi problémákhoz is vezethet [56][158][159].

2.6.1 A gyermekkorú felhasználók

Az Egyesült Királyságban a gyermekkorúak (7-19 éves) internetes szokásainak felmérése során kiderült, hogy az egyes alkalmazások (közösségi hálózatok, kommunikációs csatornák és játékok) használatában igen jó kompetenciát mutatnak, azonban a felugró ablakokban megjelenő reklámok frusztrálják és félelmet keltenek bennük, pedig ezek kellő számítógépes ismerettel kikapcsolhatók. Tehát a gyermekkorú felhasználók esetében, függetlenül attól, hogy ők már a digitális világba születtek bele, nem beszélhetünk olyan szintű digitális kompetenciáról, ami elégséges lehetne a tanulás nélküli felhasználáshoz [57]. Tévhit ugyanis az, hogy ez a korosztály már úgy, olyan tudással született, hogy ők már rendelkeznek azon képességekkel, amelyekkel könnyedén elboldogulnak a digitális térben [58]. Tény, hogy sokkal gyorsabban tanulnak, mint a náluk idősebb generációk, de minden másfajta tudás elsajátítására is sokkal fogékonyabbak, legyen az egy idegen nyelv vagy akár a matematikai ismeretek. Így ennek a korosztálynak a digitális kompetenciáját gyorsan és hatékonyan lehet(ne) kellő szintűre fejleszteni. Azonban nem csak lehet, hanem szükséges is fejleszteni azt. A fiatalok esetében nem elegendő csupán az ösztönös, a kíváncsiságból adódó, valamint az egymás vagy a felnőttek utánzásán alapuló tudásra hagyatkozni, mert az beláthatatlan veszélyeket rejt magában. Vegyük figyelembe azt, hogy a gyerekek veszélyérzete jóval alacsonyabb, mint a felnőtteké, ezáltal a naivitásukból adódóan sokkal bátrabban használják a digitális eszközöket. Nem ismerik a veszélyt jelentő tényezőket, nem ismerik fel a gyanús jeleket, ezáltal könnyebben válhatnak áldozattá [59]. Szükséges ezért számukra is a mielőbbi és rendszeres, szervezett képzés-oktatás, mivel csak ilyen módon lehet felkészíteni őket a digitális világ biztonságos használatára [156][161].

2.6.2 A felnőtt korú felhasználók

A felnőtt korú felhasználók esetében, már általánosság az, hogy rendelkeznek valamilyen szintű digitális ismeretekkel. Ezt a tudást vagy az iskolai órákon, különböző tanfolyamokon vagy tapasztalati úton szerezték. A felnőtt korú felhasználó esetében is előfordulhat az, hogy mivel már tanult informatikát és alkalmazza ezen ismereteit, egy idő után rutinból, megszokásból cselekszik. Ezáltal a figyelme lankad és olyan hibákat vét, amelyek nála nem megszokottak. Ebből adódóan olyan károkat tud okozni, akaratlanul is, amelyek nagy erkölcsi és anyagi veszteséggel járhatnak. Az is előfordulhat, hogy olyan új támadási mechanizmus bukkan fel, amire a felhasználók egyáltalán nincsenek felkészülve. Ez korábbi években többször is előfordult, például a zsarolóvírusok megjelenésekor. Részükre is fontos a rendszeresen ismétlődő oktatás és a figyelemfelkeltő kampányok [60][162][163].

2.6.3 Az időskorú felhasználók

Az időskorú felhasználók digitális kompetenciaszintjének a növelése azért is fontos, hogy az egységes vagy a homogénhez közelítő digitális ismeretek révén növelhető legyen a társadalmi információbiztonság [59]. Amennyiben a társadalom ezen rétege nem rendelkezik megfelelő szintű biztonsági ismeretekkel, abban az esetben rajtuk keresztül a többi, egyébként biztonságtudatos felhasználó is veszélybe kerülhet saját tudtán kívül. Gondoljunk arra, amennyiben akár egy családot, akár egy céget veszünk alapul, akik egy hálózatot használnak, ott a védelem szintjét a leggyengébb felhasználó szintjéhez kell mérni. Ha például a nagymama kap egy zsaroló vírust tartalmazó kéretlen üzenetet a családi wifi hálózatán bejelentkezett okostelefonjára, és azt a nagymama gyanútlanul megnyitja, abban az esetben a családi hálózatra kötött összes, arra érzékeny eszköz megfertőződhet. Hiába alkalmazta a családfő vagy a digitális-bennszülött unoka a legjobb védelmi megoldásokat [61][156][157].

2.7 Összefoglalás

A kormányzat célja az EU-val összhangban, hogy a digitális javakhoz való hozzáférést mindenki számára lehetővé tegye. A digitális javak, a digitális jólét és maga a digitális kompetencia részét képező digitális írástudás is a digitális kompetencia fontosságát támasztja alá, mivel annak a GDP-re gyakorolt hatása jelentős, amelyet a NIS irányelvek is alátámasztanak. Az UNICEF Magyar Bizottságának, az EU Kids Online-nak és az NMHH-nak a magyar fiatalok körében lefolytatott felmérése és annak eredményei is az általam vizsgált digitális kompetencia és a biztonságtudatosság kapcsolatának relációját sugallják. A digitális kompetencia és a digitális írástudás alapfeltétele annak, hogy a felhasználó a kiberteret használni tudja.

A különböző korosztályokhoz tartozó felhasználók nem azonos digitális környezetben születtek és nőttek fel, ez a körülmény alapvetően meghatározza a kibertérben való tevékenykedésüket, befolyásolja digitális kompetenciájuk kialakulását, fejlődését, valamint biztonságtudatosságuk szintjét. Az eltérő korosztályokhoz tartozó felhasználók érdeklődése és tevékenységei a kibertérben eltérőek. Emellett korukból adódóan eltérő digitális eszközökkel találkoztak és igyekeztek ezeket alkalmazni. Az idősebb generáció tagjai közül csak kevesen találkoztak fiatal korukban informatikai eszközökkel, az internetes alkalmazásokat pedig talán még ennél is kevesebben érhették el. Az informatika rohamos fejlődése és elterjedése az utóbbi évtizedekben valósult meg, így már van olyan korosztály, akiket "digitális bennszülötteknek" neveznek. Ez a korosztály már beleszületett a digitális környezetbe, számára az alkalmazott eszközök megszokottak, digitális írástudásuk és kompetenciájuk gyorsan fejlődik, az újabb eszközök és alkalmazások használata nem jelent kihívást számukra. A biztonságtudatosság azonban, ahogyan a fizikai világban is, lassabban, inkább tapasztalatok útján, példamutatás alapján és oktatással fejleszthető. A megfelelő biztonságtudatosság a kibertérben is elengedhetetlen, hiszen a javaink nem csak a fizikai világban léteznek. A fizikai világban is tapasztalható a korosztályok közötti eltérő biztonságtudatosság, ami a digitális világban is jelentkezik. Kutatásom szempontjából a felhasználók elsődleges csoportosítása ezért életkoruk alapján történt.

A felhasználói digitális kompetencia és biztonságtudatosság fejlesztésének megvalósításához szükséges felmérni a felhasználók szintjét korosztályok szerint, majd felépíteni egy rendszert, melyben a felhasználói ismeretek, képességek és készségek, szintek és osztályok szerint besorolhatók.

A fentiek bemutatása és elemzése kellő alapossággal alátámasztja a következő fejezetekben bemutatásra kerülő kutatásaimat és azok eredményeit, valamint az eredmények alapján a bevezetésre és elfogadásra javasolt téziseimet.

3 A KÜLÖNBÖZŐ GENERÁCIÓK DIGITÁLIS KOMPETENCIÁJÁNAK ÉS BIZTONSÁGTUDATOSSÁGÁNAK FELMÉRÉSE

A felhasználók viselkedését a digitális környezetben ismernünk kell, hiszen a felhasználó kockázati tényező. A kockázati szint meghatározásához a felhasználó viselkedésének felmérésére kérdőíves módszer alkalmazható. A kérdőív kidolgozását viselkedés alapú szempontrendszer alapján lehet elvégezni, hiszen a felhasználó digitális cselekményei alapján mérhető fel a digitális kompetencia és a biztonságtudatosság.

A kérdőíves felmérésem a klasszikus statisztika definíciói szerint nem tekinthető reprezentatívnak, mivel a válaszadókat nem célzottan kerestem meg az általam felállított életkor és lakóhely szerinti szempontok alapján, hanem a válaszadók önkéntesen, saját akaratukból töltötték ki a kérdőívet jelentős számban. Annak ellenére, hogy nem tekinthető reprezentatívnak, számossága miatt az eredmények jellemzik a mai társadalom digitális kultúráját.

3.1 A beérkezett kitöltött kérdőívek

A kérdőívet összesen 1274-en töltötték ki, amiből az online kérdőívet 1195-en, a papíralapút 79-en [156][158].

3.2 A kérdéscsaládok csoportosítása

A kérdőívet alapvetően a digitális kompetencia és a biztonságtudatosság szintjének felmérésére állítottam össze, és több kérdéscsaládból tevődött össze. Ezek a kérdéscsaládok az alábbiak voltak.

- Általános kérdések:
    - A felsoroltak közül Ön hol él?
    - Ön Magyarországon él?
    - Hol lakik Ön?
    - Melyik korcsoporthoz tartozik?
    - Beszél Ön angolul?
- Felhasználói szokások és alkalmazott eszközök:
    - Használja az internetet?
    - Van önnek hordozható okos eszköze?
    - Szokott internetezni hordozható okos eszközön?

    - Milyen típusú internetkapcsolatot szokott használni?
    - Milyen gyakran használja az internetet?
    - Használ Ön a háztartásában okos (internetre csatlakoztatott) eszközt?
    - Az internetet milyen célra használja általában?
- A digitális kompetenciára és a biztonságtudatosságra vonatkozó kérdések:
    - Milyen szintűre értékeli a saját informatikai ismereteit és biztonságtudatosságát?
    - Milyen szintű informatikai ismerettel rendelkezik?
    - A hordozható okos eszközén használ védelmi megoldásokat?
    - Jelszavát, feloldó mintáját milyen gyakran változtatja?
    - Vett már részt valaha információbiztonsági oktatáson, képzésen?
    - Ha lehetősége lenne egy ingyenes tanfolyam, vagy oktatás keretében digitális ismereteket elsajátítani, részt venne rajta?
    - Amennyiben dolgozik, a munkájához szükséges az informatikai ismeret?
- Rosszindulatú kódok elleni védelem:
    - Használ vírusvédelmi- vagy tűzfal alkalmazást azon (azokon) az eszközön(eszközökön), amin internetezik?
    - Érte már vírus- és/vagy egyéb rosszindulatú támadás az Ön eszközét/eszközeit?
    - Esetleges vírustámadás és/vagy egyéb rosszindulatú támadás esetén tisztában van azzal, hogy mi a teendő?
- Internetes zaklatás (Cyberbullying):
    - Zaklatták már közösségi oldalon (pl. Facebook) vagy e-mail-ben Önt vagy hozzátartozóját (barátját)?
    - Mit tenne, ha zaklatnák Önt vagy hozzátartozóját, vagy mit tanácsolna ilyen esetben?
- Adatvagyon védelme:
    - Vesztett-e már el véglegesen pótolhatatlan digitális adatot/tartalmat?
    - Szokott-e készíteni az eszközén(eszközein) tárolt adatokról biztonsági másolatot?
    - Milyen gyakorisággal készít biztonsági másolatot?

A kérdéseket nem feltétlenül mindig egymást követően tettem fel azért, hogy az azonos kérdéscsaládhoz tartozó válaszok alapján kiszűrhessem azokat a válaszokat, amelyek ellentmondásosak.

A kérdéseket feleletválasztós formában tettem fel, hogy a kiértékelésnél korlátozott számú válasszal tudjak dolgozni. Igyekeztem a kérdéseket úgy kidolgozni, hogy mindenki megfelelően választhasson, illetve lehetőséget adtam egyes kérdések esetében, hogy az egyéb kategóriában saját, egyedi választ írhassanak.

A kérdőíves vizsgálatomat olyan koncepció szerint végeztem, hogy azokat a kérdéseket, amelyek logikai és/vagy bármilyen ellentmondást tartalmaztak, kizártam abból a „kérdéscsaládból", illetve az üresen hagyott válaszokat is figyelmen kívül hagytam. Ahol a kitöltő saját maga írhatta a választ és az nem volt egyértelműen besorolható, azt kiszűrtem és nem vettem figyelembe az értékelések során.

Az alábbiakban az általam kiválasztott szempontok szerinti kérdések és azokra adott válaszok egyesével történő összekapcsolása és kiértékelése alapján következtetéseket vontam le a biztonságtudatosság és a digitális kompetencia fejlesztésének érdekében.

3.3 Általános kérdések

Az általános kérdéscsaládot annak érdekében alkottam meg, hogy a felhasználókkal kapcsolatos általános, azonban a továbbiakban alapvetőnek számító információkat begyűjtsem. Ezek a kérdések a felhasználók korára, lakhelyére és idegennyelv ismeretére vonatkoztak.

3.3.1 Lakóhely szerinti eloszlás.

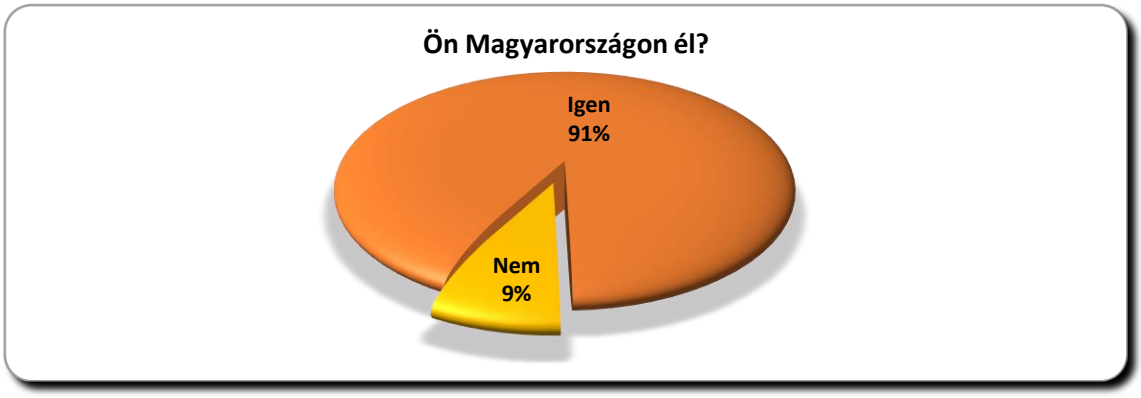
Az első kérdés „A felsoroltak közül Ön hol él?" volt. A kérdés feltevésével az volt a célom, hogy megtudjam azt, hogy a válaszadók milyen szerkezettípusú településen élnek. Abból a célból tettem fel ezt a kérdést, hogy láthassam, milyen fejlettségű informatikai infrastruktúrával rendelkezhet az adott településforma, amit a felhasználó elérhet.

7. ábra A kérdőív „A felsoroltak közül Ön hol él?" kérdésének kiértékelése (forrás: saját kérdőíves felmérés; készítette a szerző) [157][158]

Erre a kérdésre 1183 válasz érkezett. A válaszok alapján (7. ábra), a „Fővárosban” 38%-a, „Megyeszékhelyen” 17%-a, „Városban” 30%-a, míg „Községben” 15%-a él a válaszadóknak [157][158].

3.3.2 Hazai és külföldi válaszadók aránya

A második kérdés az „Ön Magyarországon él?” volt. Erre a kérdésre összesen 1196 válasz érkezett ebből az „igen” -re 91%, míg a „nem” -re 9% válasz érkezett (8. ábra).



8. ábra A kérdőív „Ön Magyarországon él?” kérdésének kiértékelése (forrás: saját kérdőíves felmérés; készítette a szerző)

Ez azért is fontos, mert a DJP2.0 is foglalkozik a kárpátmedencei magyarság digitális kompetencia növelésének kérdésével, mellyel ez a kérdés összhangban áll. A továbbiakban a külföldön élő felhasználók válaszait kizártam a felmérés kiértékelésének készítésekor.

3.3.3 Életkor szerinti eloszlás

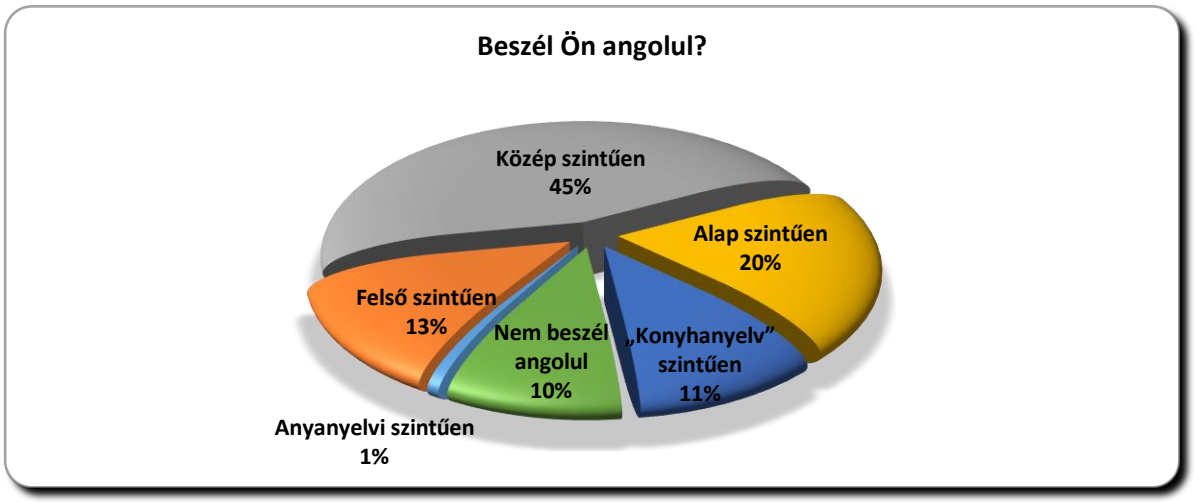
A „Melyik korcsoporthoz tartozik?” kérdésre, amit a 9. ábra mutat be, összesen 947-en adtak választ.

9. ábra A kérdőív „Melyik korcsoporthoz tartozik?” kérdésének kiértékelése (forrás: saját kérdőíves felmérés; készítette a szerző) [157][158]

A korcsoportokat az informatika fejlődésének és a felsőoktatásban résztvevők életkorának figyelembevételével határoztam meg. Az első válasz a „18-24” korcsoport volt, ami a nappali tagozatos felsőoktatásban résztvevők életkorára utal, akik a Z generáció tagjai. Ezt a választ összesen 40% jelölte be. A következő válaszlehetőség a „25-34” korcsoport volt, amiből látható, hogy ez az 1982 és 1993 között született felnőttek csoportja. Ennek a korosztálynak a tagjai már az Y generációhoz tartoznak és még a World Wide Web nyilvánossá tétele előtt születtek. Ezt a választ 24% jelölte meg. A „35-50” korcsoport volt a következő, amit 18% adott meg. Ennek a korcsoportnak a meghatározása a X generációhoz köthető. Ők azok, akiknek ahogyan korábban is említettem, felnőttként kellett megismerkedniük a számítógéppel, a mobiltelefonnal, az internettel, az e-maillel. Nekik is fel kellett venniük a tempót a digitális technológia rohamos fejlődésével. Az „51, vagy annál idősebb” választ 18% jelölte meg. Ez a korcsoport a „Baby-boom” generációhoz tartozó felnőtteket jelenti. Ehhez a generációhoz tartozók azok, akik a digitális szakadék másik, távolabbi felén vannak. Ennek a generációnak a legfiatalabbjai is már fiatal felnőttek voltak a PC korszak beköszönte idején. Az ő számukra a legnehezebb a digitális kor nyújtotta lehetőségeket beleilleszteni a mindennapjaikba [157][158].

3.3.4 Az angol nyelv ismerete

A kilencedik, „Beszél Ön angolul?” kérdést annak okán tettem bele a kérdőívbe, hogy más kapcsolódó kompetenciákról is képet kapjak, valamint a későbbiekben vizsgálom. Ennél a kérdésnél, amit a 10. ábra mutat be, összesen 928 választ értékeltem, amelyek logikailag ellentmondásosak voltak, azokat kizártam.



10. ábra A válaszadók angol nyelvi ismereti szintjei saját besorolásuk szerint (forrás: saját kérdőíves felmérés; készítette a szerző)

A válaszadók közül 1% „anyanyelvi szintűen”, 13% „felső szintűen”, 45% „közép szintűen”, 20% „alap szintűen” beszél angolul. 11% „konyhanyelv szintűen” tud angolul, míg a válaszadók 10%-a a „nem beszélnek angolul” választ adta. Az értékelésnél azokat a válaszokat is beleszámítottam, amelyek esetében két szomszédos szint került megjelölésre. Jól látható, hogy a válaszadók közül minden kilencedik az, aki egyáltalán nem beszél angolul, de azt, hogy az angolon és az anyanyelvén kívül beszél-e más nyelven, nem kérdeztem meg. Az idegen nyelvi kompetenciára vonatkozó kérdésemet a szoftver ergonómia fejlesztése miatt, annak indoklása okán tettem fel.

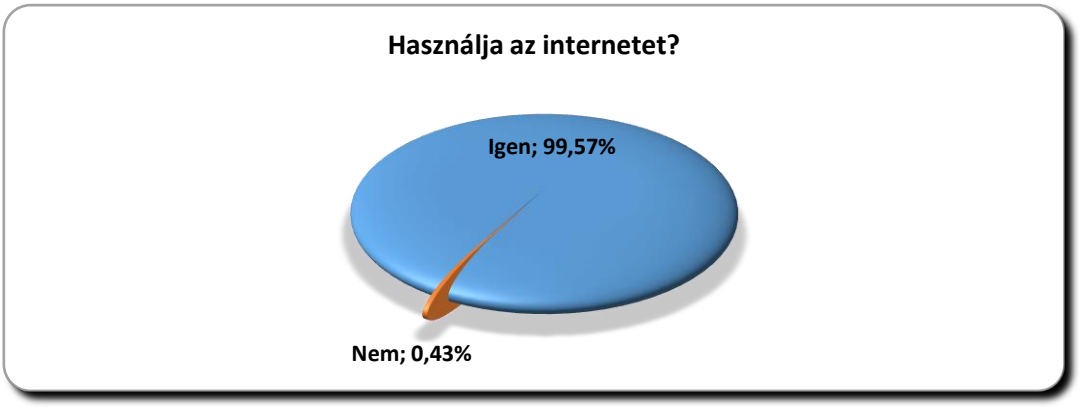
3.3.5 Összegzés

A felhasználók infrastrukturális, szociális, valamint iskolázottsági hátterének ismerete fontos része a kutatásomnak, mert ennek alapján tudom értékelni a későbbi kérdéscsaládokra adott válaszaikat. A kiértékelés alapján kimondható, hogy a lakóhely meghatározó tényező jelenleg, hiszen az internetelérési lehetőség, az elérhető internet sebessége, sávszélessége is befolyásolja (segíti vagy korlátozza) a felhasználó kibertérben történő tevékenységét. A következő kérdéscsalád a “Felhasználói szokások és alkalmazott eszközök” kérdéseire adott válaszokkal együtt tudok megalapozott következtetéseket levonni.

3.4 Felhasználói szokások és alkalmazott eszközök

A következő kérdéscsalád a “Felhasználói szokások és alkalmazott eszközök” címet viseli és ebben a kérdéscsaládban az internet használatát, az azzal kapcsolatos szokásokat, az arra használt és alkalmazott eszközöket mértem fel. Ennek, többek között a digitális kompetencia és biztonságtudatosság vizsgálatánál van nagy szerepe.

3.4.1 Internethasználat

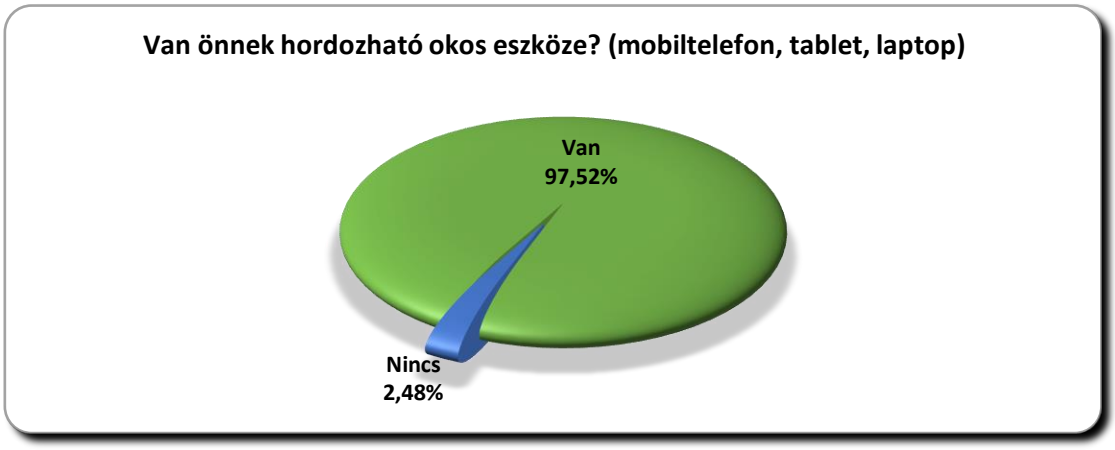


11. ábra A kérdőív „Használja az internetet?” kérdésének kiértékelése (forrás: saját kérdőíves felmérés; készítette a szerző)

A „Használja az internetet?” kérdésre, ami a negyedik, 928 válaszadó válaszolt. 99,57% „igen” és 0,43% „nem” válasz érkezett, ami azt jelenti, hogy a válaszadók majdnem teljes egészében internethasználók, ezt a 11. ábra mutatja be.

3.4.2 Internetezésre használt eszköz

Az ötödik kérdésre, ami a „Van önnek hordozható okos eszköze? (mobiltelefon, tablet, laptop)” volt, 926 válasz érkezett. Ezek között 97,52% „van” és 2,48% „nincs” válasz volt, ezt a 12. ábra mutatja be. Ez alapján kiderült, hogy szinte minden válaszadónak van olyan hordozható okos eszköze, amelyen internetezni lehet.



12. ábra A kérdőív „Van önnek hordozható okos eszköze?” kérdésének kiértékelése (forrás: saját kérdőíves felmérés; készítette a szerző)

3.4.3 Internethasználat okos eszközön

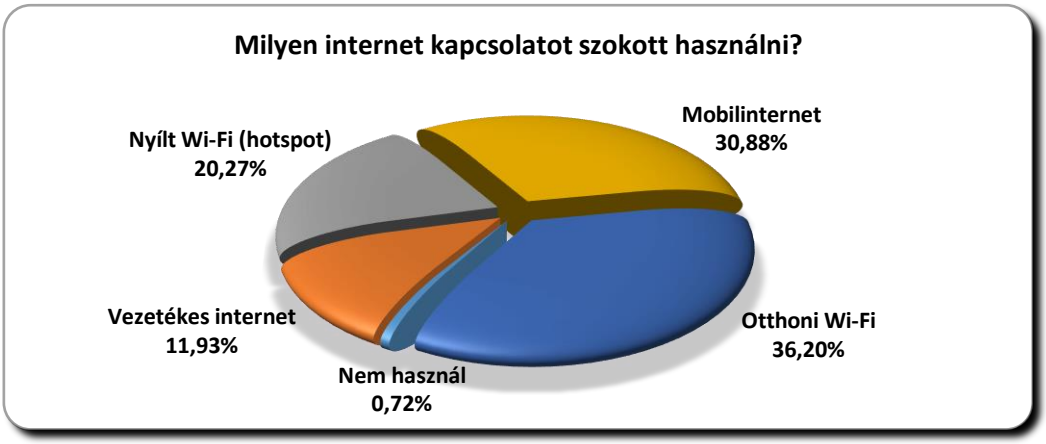
A hatodik kérdéssel azt szerettem volna megtudni, hogy a megkérdezett „Szokott internetezni hordozható okos eszközön? (mobiltelefon, tablet, laptop)”.

13. ábra Az okos eszközök megjelenése az internethasználatban (forrás: saját kérdőíves felmérés; készítette a szerző)

Ezt a kérdést 926-an válaszolták meg, azonban azokat a válaszokat kizártam, ahol a „Használja az internetet?” kérdésre nemmel válaszoltak. Így a figyelembe vett válaszadók száma erre a kérdésre 922, amelyből az „igen” 95% és a „nem” 5% volt, ezt a 13. ábra mutatja be.

3.4.4 Az internet infrastruktúra használatának bemutatása

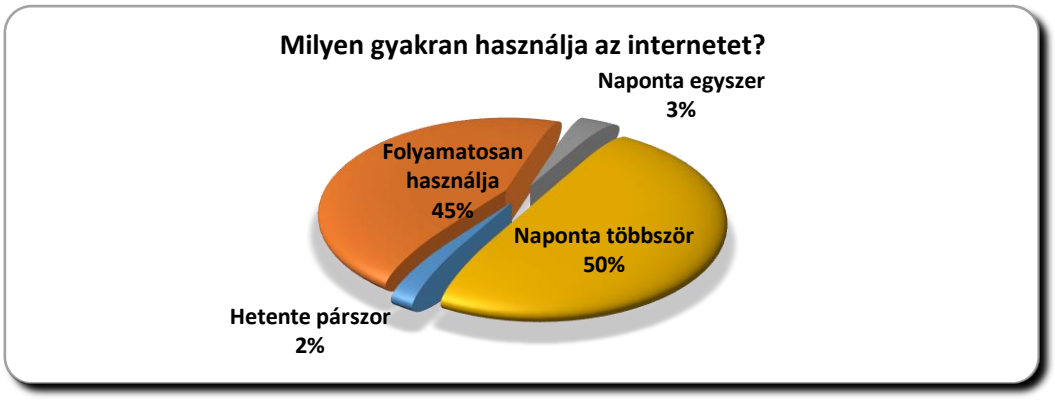
Arra a kérdésre, hogy „Milyen típusú internetkapcsolatot szokott használni?”, összesen 943 választ értékeltem, mivel azokat a válaszokat, amelyek logikailag ellentmondásosak voltak, kizártam. A válaszok a következőképpen alakultak: „Előfizetéshez kapott mobilinternetet” 30,88%, „Otthoni Wifi hálózatot” 35,2%, „Nyílt Wifi (hotspot) hálózatot” 20,27%, „Vezetékes internetet” 11,93% használnak, és 0,72% „nem használ” mobil eszközön internetet. A 14. ábra alapján a válaszokból jól látszik, hogy a válaszadók többsége az otthoni internetet használja [156][157][158].



14. ábra A kérdőív „ Milyen internetkapcsolatot szokott használni?” kérdésének kirétékelése (forrás: saját kérdőíves felmérés; készítette a szerző)[156][157]

3.4.5 Az internet használatának gyakorisága

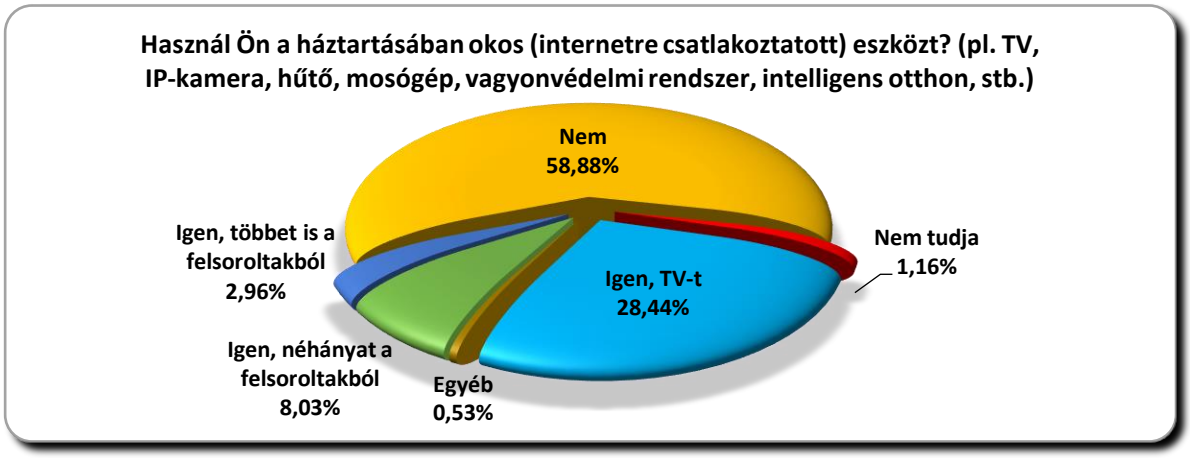
A nyolcadik, „Milyen gyakran használja az internetet?” kérdésre 947 választ értékeltem, amelyek logikailag ellentmondásosak voltak, kizártam. A „Folyamatosan használja” lehetőséget 45%, a „Naponta többször” választ 50%, a „Naponta egyszer” lehetőséget 3%, a „Hetente párszor” választ 2% jelölték be. A válaszokból jól látszik, hogy a válaszadók hatalmas többsége vagy folyamatosan internetkapcsolatot használ, vagy naponta többször, de legalább egyszer. A 15. ábra alapján elenyésző kisebbség az, aki csak heti pár alkalommal használja az internetet. A „Nem használta még” lehetőségre nem érkezett jelölés.



15. ábra A kérdőív „Milyen gyakran használja az internetet?” kérdésének kiértékelése (forrás: saját kérdőíves felmérés; készítette a szerző)

3.4.6 Okos eszközök használata

A „Használ Ön a háztartásában okos (internetre csatlakoztatott) eszközt? (pl. TV, IP-kamera, hűtő, mosógép, vagyonvédelmi rendszer, intelligens otthon stb.)” kérdésre összesen 947 válasz érkezett.



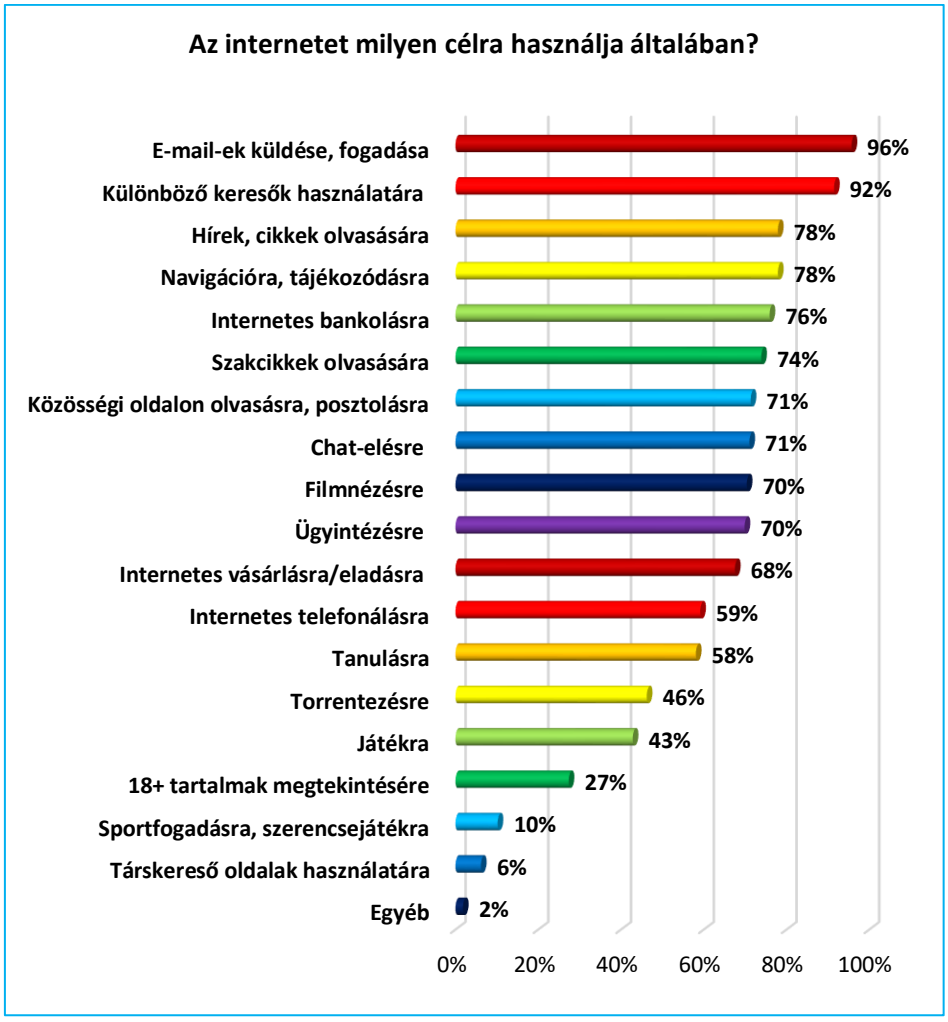
16. ábra A kérdőív „Használ Ön a háztartásában okos (internetre csatlakoztatott) eszközt?” kérdésének a kiértékelése (forrás: saját kérdőíves felmérés; készítette a szerző)

A kérdést annak érdekében tettem fel, hogy képet kapjak arról a tendenciáról, hogy az IoT (Internet of Things – a dolgok internete) eszközök milyen penetrációban vannak már jelen a mindennapokban (16. ábra). A „Nem” közel 56%, „Nem tudja” 1% felett, „Igen, TV-t” közel 28,5%, „Igen, néhányat a felsoroltakból” 8%, „Igen, többet is a felsoroltakból” majdnem 3%, „Egyéb” fél százalék érkezett a válaszokat tekintve.

3.4.7 Mire használja az internetet?

„Az internetet milyen célra használja általában?” kérdésre 943 válasz érkezett összesen. Az alábbi lehetőségeket volt mód megjelölni: „Hírek, cikkek olvasására (Origo, Index, 444, stb.)”

78%, „Szakcikkek olvasására” 74%, „Különböző keresők használatára (Google, Yahoo stb.)”92%, „Navigációra, tájékozódásra (pl. Google maps, Waze, iGo)” 78%, „E-mail-ek küldése, fogadása” 96%, „Internetes telefonálásra (Skype, Viber, Messenger stb.)” 59%, „Chat-elésre (Skype, Viber, Messenger stb.)” 71%, „Közösségi oldalon olvasásra, posztolásra (Facebook, Twitter, LinkedIn, Instagram)” 71%, „Társkereső oldalak használatára” 6%, „18+ tartalmak megtekintésére” 27%, „Torrentezésre” 46%, „Filmnézésre (pl. YouTube)” 70%, „Játékra” 43%, „Sportfogadásra, szerencsejátékra” 10%, „Internetes vásárlásra/eladásra (pl. eBay, Vatera, Jófogás, Tinydeal)” 68%, „Tanulásra (pl. DuoLingo)” 58%, „Ügyintézésre (pl. Ügyfélkapu)” 70%, „Internetes bankolásra” 76%, „Egyéb munka, oktatás-tanítás, szabadidős program szervezés, könyv- és szépirodalom olvasása, tudományos kutatásra.” 2% válasz érkezett. Az eredményt a 17. ábra tartalmazza.



17. ábra A kérdőív „ Az internetet milyen célra használja általában?” kérdésének kiértékelése (forrás: saját kérdőíves felmérés; készítette a szerző)

3.4.8 Összegzés

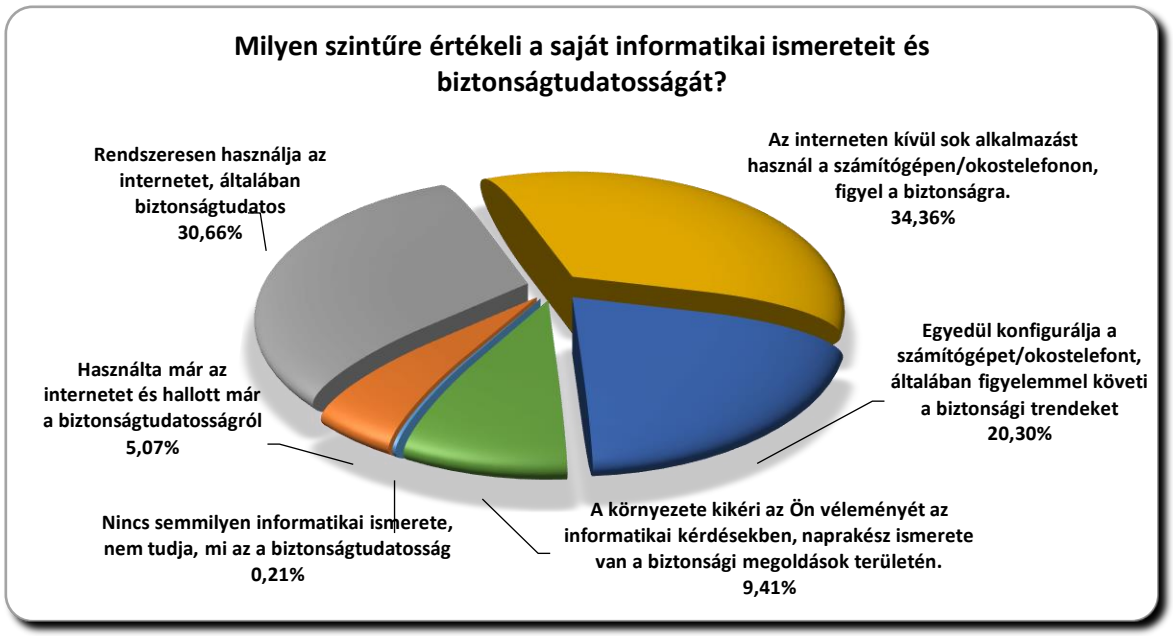
Megállapítom a kérdéscsoport válaszainak kiértékelése alapján, hogy kortól és lakóhelytől függetlenül, mindenki használja az internetet. Ezért mindenképpen indokolt a felhasználók digitális kompetenciájának és biztonságtudatosságának megismerése, hiszen amint azt disszertációm bevezető részében kifejtettem, a felhasználó biztonsági kockázatot jelent.

3.5 A digitális kompetenciára és a biztonságtudatosságra vonatkozó kérdések

A digitális kompetencia és a biztonságtudatosság kérdéscsoport kérdései a vizsgálatom azon alapját képezik, amelynek segítségével meg tudtam alkotni és definiálni tudtam azokat a felhasználói profilokat, amelyeknek az alkalmazásával különböző összefüggéseket tudtam kimutatni. A szempontok kialakításánál a felhasználók kockázati szint szerinti besorolását is elvégeztem.

3.5.1 Informatikai ismeretek saját értékelése

A tizedik kérdésre, hogy „Milyen szintűre értékeli a saját informatikai ismereteit és biztonságtudatosságát?”, 946 válasz érkezett.



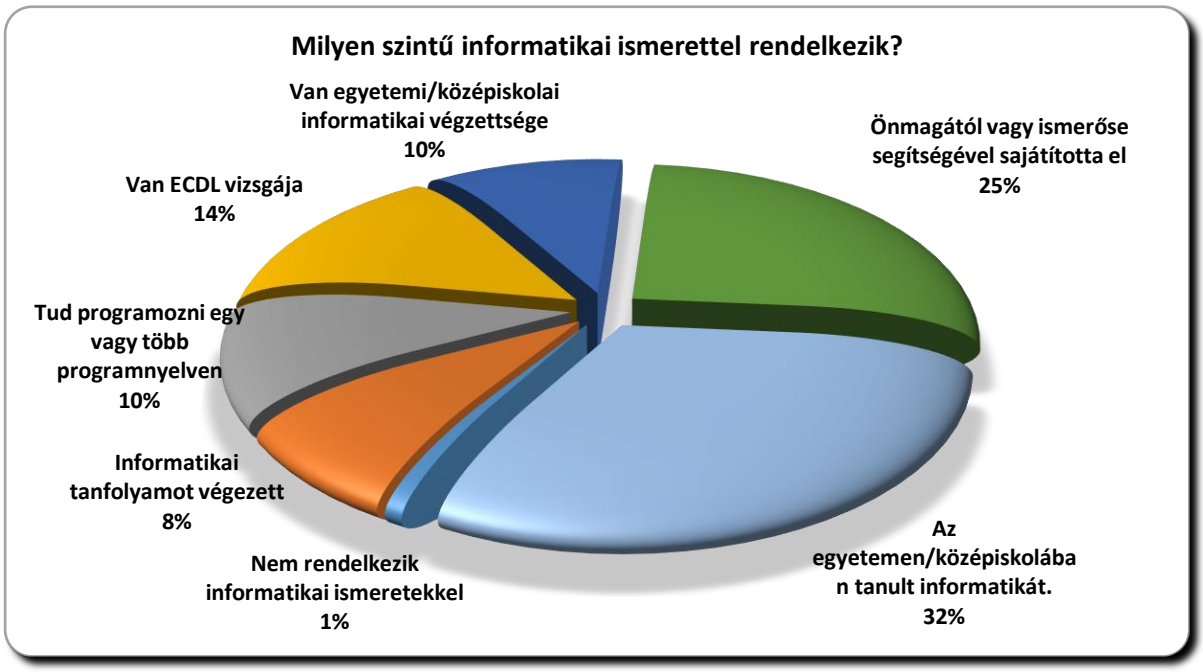
18. ábra Az informatikai ismeretek és a biztonságtudatosság a válaszadók önértékelése alapján (forrás: saját kérdőíves felmérés; készítette a szerző)

A 18. ábra alapján arra, hogy „Használta már az internetet és hallott már a biztonságtudatosságról” 5%, a „Rendszeresen használja az internetet, általában biztonságtudatos” közel 31%, „Az interneten kívül sok alkalmazást használ a

számítógépen/okostelefonon, figyel a biztonságra” több, mint 34%, az „Egyedül konfigurálja a számítógépet/okostelefont, általában figyelemmel követi a biztonsági trendeket” több, mint 20%, „A környezete kikéri az Ön véleményét az informatikai kérdésekben, naprakész ismerete van a biztonsági megoldások területén” kevesebb, mint 10% válasz érkezett. Arra, hogy „Nincs semmilyen informatikai ismerete, nem tudja, mi az a biztonságtudatosság” 0,2% válasz érkezett, ami úgy gondolom viszonylag jó arány.

3.5.2 Informatikai ismeretek végzettség alapján

A tizenegyedik kérdésre, ami a „Milyen szintű informatikai ismerettel rendelkezik?” 949 válasz érkezett.



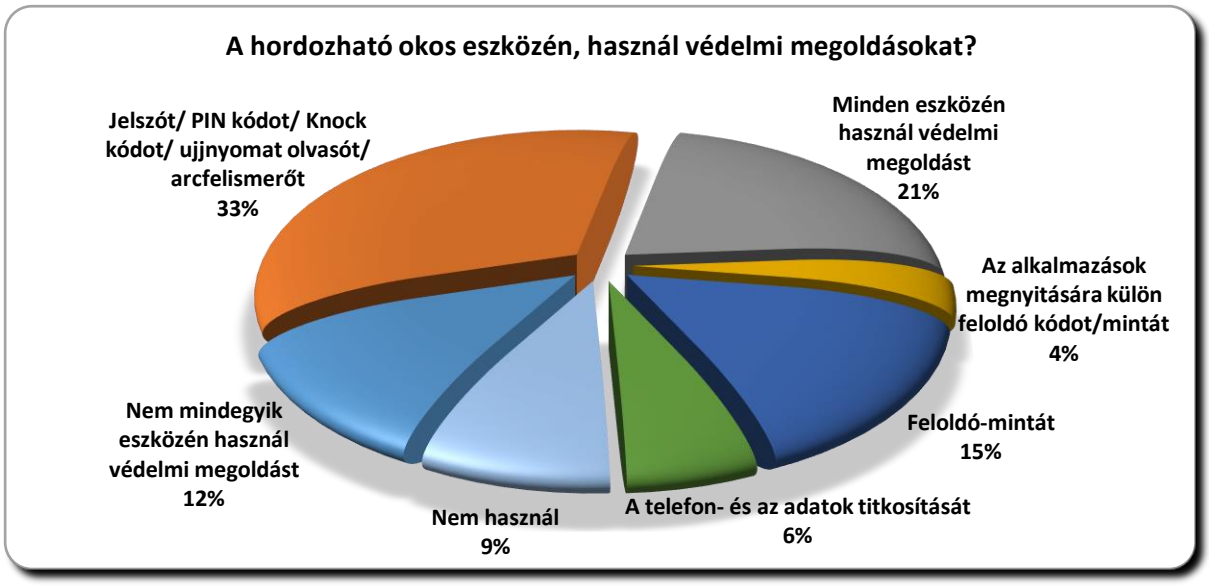
19. ábra Az informatikai ismeretek szintjének kérdése (forrás: saját kérdőíves felmérés; készítette a szerző)

A válaszadók a 19. ábra alapján, az alábbiak szerint sorolták be saját magukat. A „Van egyetemi/középiskolai informatikai végzettsége” 10%, „Az egyetemen/középiskolában tanult informatikát” 32%, a „Tud programozni egy vagy több programnyelven” 10%, a „Van ECDL vizsgája” 14%, az „Informatikai tanfolyamot végezett” 8%, az „Önmagától vagy ismerőse segítségével sajátította el” 25%, a „Nem rendelkezik informatikai ismeretekkel” 1% választ kapott.

3.5.3 Mobileszközök védelme

A tizenharmadik kérdésre, ami „A hordozható okos eszközén, használ védelmi megoldásokat?”, 938 választ értékeltem, amelyek logikailag ellentmondásosak voltak,

kizártam. A feltett kérdésre több válasz is megjelölhető volt. A 20. ábra szerinti válaszok alapján arra, hogy „Nem mindegyik eszközén használ védelmi megoldást” 12%, a „Minden eszközén használ védelmi megoldást” 21%, a „Feloldó-mintát” 15%, a „Jelszót/ PIN kódot/ Knock kódot/ ujjnyomat olvasót/ arcfelismerőt” 33%, „A telefon- és az adatok titkosítását” 6%, „Az alkalmazások megnyitására külön feloldó kódot/mintát” 4%, a „Nem használ” 9% válasz érkezett. Látható, hogy a felhasználók mindössze 9 %-a nem használ semmilyen védelmi megoldást, valamint a gyenge védelmet biztosító feloldó-mintát a válaszadók 15%-a használja. Az alkalmazások megnyitására mindössze 4% használ külön feloldási védelmet.

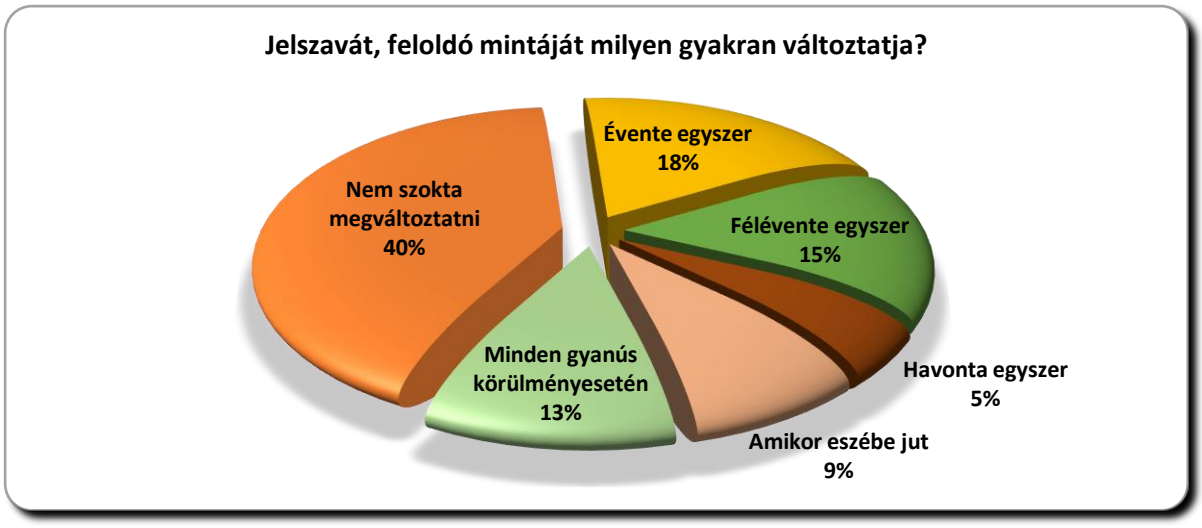


20. ábra A hordozható okos eszközökön használt védelmi megoldások (forrás: saját kérdőíves felmérés; készítette a szerző)

3.5.4 Jelszóházirend alkalmazása

A tizennegyedik kérdés a „Jelszavát, feloldó mintáját milyen gyakran változtatja?” volt. Erre a kérdésre 936 választ értékeltem, amelyek logikailag ellentmondásosak voltak, kizártam.

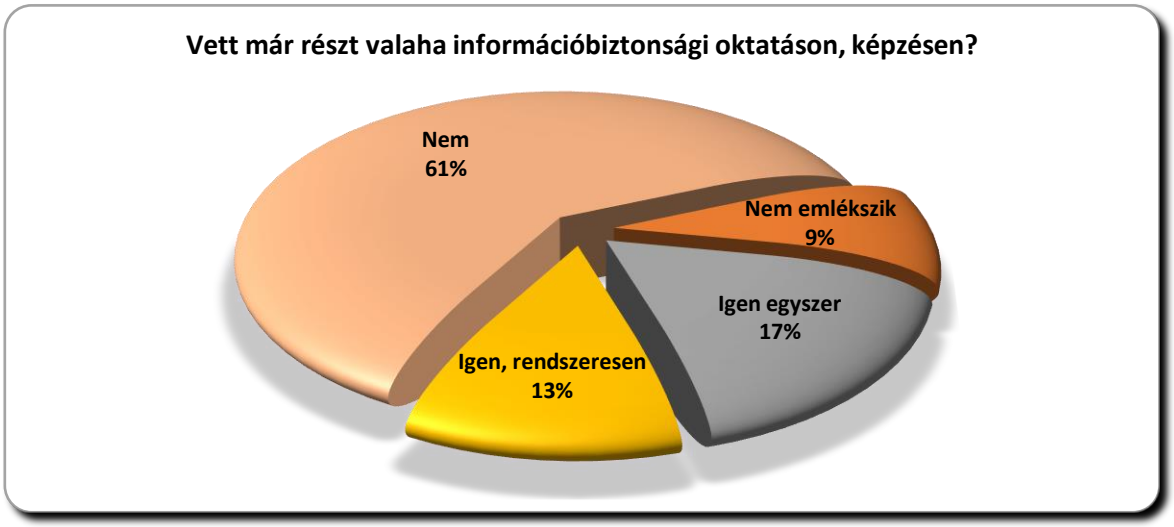
A „Nem szokta megváltoztatni” 40%, az „Évente legalább egyszer” 18%, a „Félévente legalább egyszer” 15%, a „Havonta legalább egyszer” 5%, az „Amikor eszébe jut” 9% és a „Minden gyanús körülmény esetén” 13% jelölést kapott, amit a 21. ábra mutat be. A felhasználók egyharmada egyáltalán nem változtatja meg a jelszavait. A felhasználók több, mint egyharmada évente egyszer-kétszer változtatja csak meg a jelszavait. Kimondható, hogy a válaszadók majdnem 80%-a alacsony biztonságtudatossággal bír a jelszóházirend alkalmazása területén.



21. ábra A kérdőív „Jelszavát, feloldó mintáját milyen gyakran változtatja?" kérdésének kiértékelése (készítette a szerző) (forrás: saját kérdőíves felmérés; készítette a szerző)

3.5.5 Információbiztonsági oktatás

Az alábbi kérdés azért került a kérdéssorba, mert az információbiztonsági oktatás meglétét is felmértem.



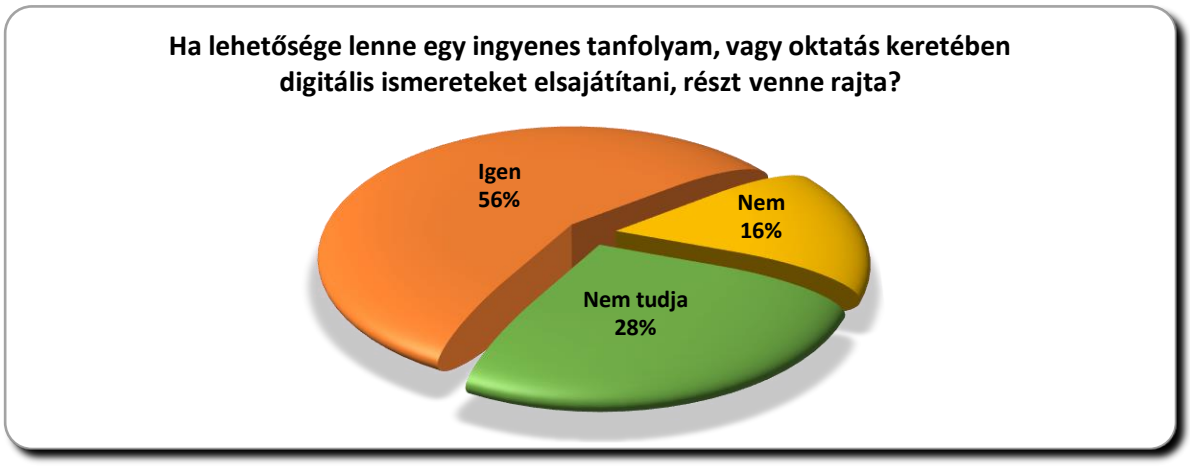
22. ábra A kérdőív „Vett már részt valaha információbiztonsági oktatáson, képzésen?" kérdésének a kiértékelése (forrás: saját kérdőíves felmérés; készítette a szerző)

A „Vett már részt valaha információbiztonsági oktatáson, képzésen?" kérdésre 946 válasz érkezett. Ebből a „Nem" 61%, a „Nem emlékszik" 9% és az „Igen, egyszer" 17%, valamint az „Igen rendszeresen" 13% választ kapott (22. ábra). Döbbenetesen magas azok száma, akik még egyáltalán nem vettek részt semmilyen információbiztonsági oktatáson. A rendszeresen résztvevő felhasználók aránya nagyon alacsony (13%). Ez az eredmény is azt bizonyítja, hogy

az információbiztonsági képzésre, valamint annak rendszeresen történő ismétlésére szükség van.

3.5.6 Digitális ismeretek oktatása

Az alábbi kérdést annak vizsgálata érdekében tettem fel a válaszadóknak, hogy meggyőződjek arról, hogy „Ha lehetősége lenne egy ingyenes tanfolyam, vagy oktatás keretében digitális ismereteket elsajátítani, részt venne rajta?”. Erre 944 válasz érkezett (23. ábra). Örömteli, hogy a válaszadók az „Igen” lehetőségre 56%, míg a „Nem” 16% és a „Nem tudja” 28% választ adtak. Ez azt bizonyítja, hogy a felhasználókban megvan az az egészséges, ösztönös igény, hogy az új ismereteket szervezett körülmények között elsajátítsák. Az „ingyenes” megjelölést a DJP2.0 és az Európai Digitális Menetrend célkitűzéseinek megfelelően használtam, mivel a kormányzat és az unió is azt az álláspontot képviseli, hogy a felhasználók számára ugyanúgy, mint más kompetenciát, ezt is közoktatási formában kell biztosítani.

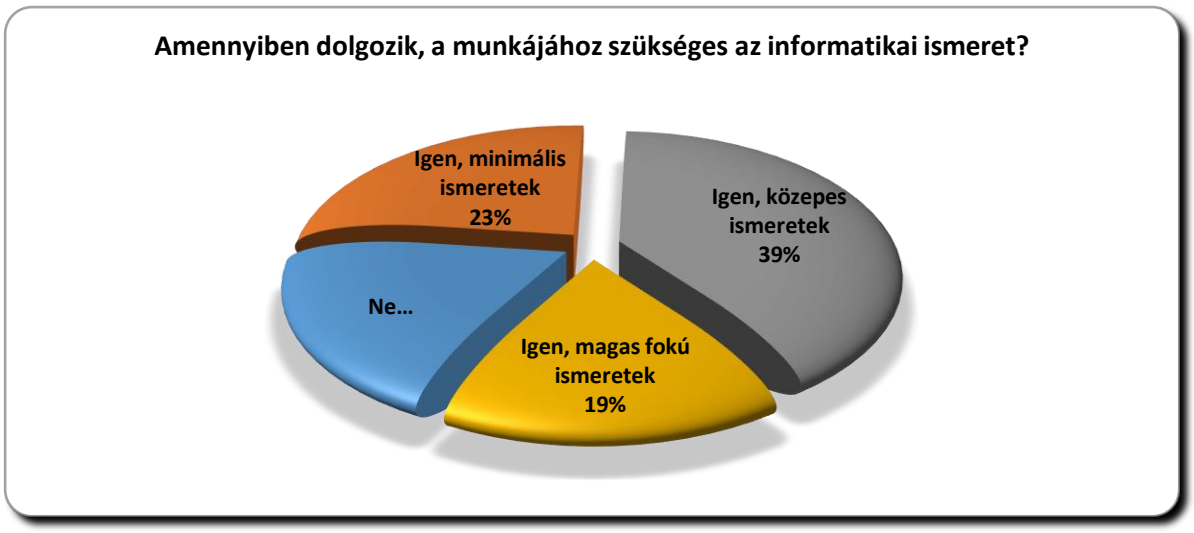


23. ábra A kérdőív „Ha lehetősége lenne egy ingyenes tanfolyam, vagy oktatás keretében digitális ismereteket elsajátítani, részt venne rajta?” kérdésének a kiértékelése (forrás: saját kérdőíves felmérés; készítette a szerző)

3.5.7 Az informatikai ismeretek szükségessége a munkavégzéshez.

Az már korábban is köztudott volt, hogy egyre több szakmához válik elengedhetetlenné az informatikai ismeretek megléte. A digitalizálódó világban prognosztizálható az, hogy a közeljövőben a szakmák szinte mindegyikéhez szükséges lesz legalább alapszintű informatikai ismeretekre. Valamint az is látható, hogy a jelenleg meglévő és elégséges informatikai ismereteknél is magasabb szintű ismeretre lesz szükség az adott szakmában a technológia egyre gyorsabb fejlődésének köszönhetően. A kérdőívem egyik kérdése arra irányult, hogy jelenleg a válaszadóknak milyen szintű informatikai ismeretekre van szüksége a munkájához. Az „Amennyiben dolgozik, a munkájához szükséges az informatikai ismeret?” kérdésre a válaszok összességében megdöbbentőek, amit a 24. ábra mutat be, és egyben alátámasztják azt a

feltételezést, amelyet az előzőekben leírtam. Az összes válaszadó közül 867 válaszolt. Ebből a "Nem" 19%, az "Igen, minimális ismeretek" 23%, az "Igen, közepes ismeretek" 39%, az "Igen, magas fokú ismeretek" 21% válasz volt [156][157][158].



24. ábra A kérdőív „Amennyiben dolgozik, a munkájához szükséges az informatikai ismeret?" kérdésének kiértékelése (forrás: saját kérdőíves felmérés; készítette a szerző) [156][157]

3.5.8 Összegzés

Az önértékelés és a valós ismeretek szintje a felhasználók tekintetében nem minden esetben egyezik meg. Az alacsony szintű digitális kompetenciából adódó hibás reakció egy adott veszélyhelyzet esetén jelentős károkat okozhat. A vírustámadások vagy rendszerhiba miatti adatvesztések jelentős anyagi kárt is okozhatnak. A felhasználók biztonságtudatosságát viszont a valós tevékenységük alapján is vizsgálni kell, vagyis alkalmaznak-e megfelelő védelmet. Az összefüggések felismerésével olyan módszer- és viselkedésspecifikus szempontrendszert állítottam fel, amely alkalmas a felhasználók digitális kompetencia és biztonságtudatossági kockázati célú értékelésére.

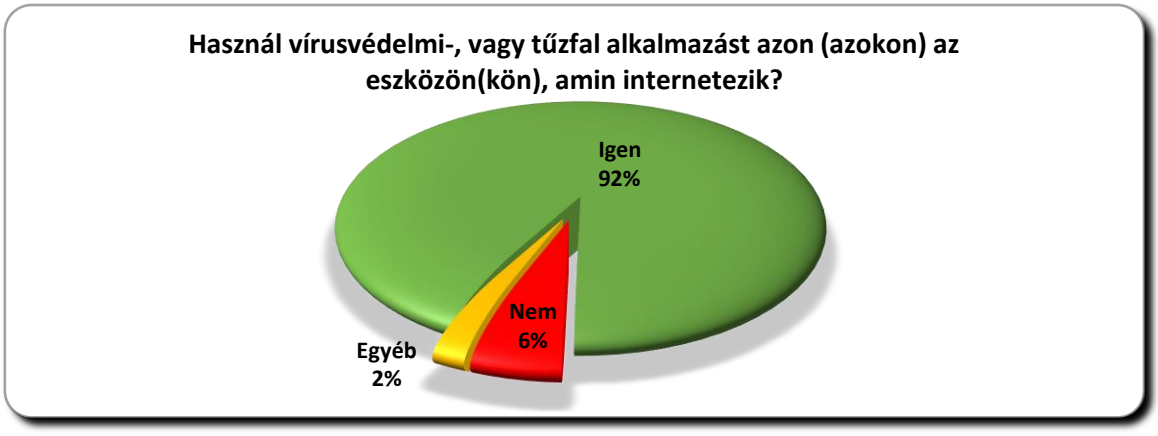
3.6 Rosszindulatú kódok elleni védelem

A "Rosszindulatú kódok elleni védelem" kérdéscsalád kimondottan a biztonságtudatosság felmérése céljából került összeállításra. Ennek a kérdéscsaládnak a kérdései azok, amelyek segítségével sikerült a megalkotott felhasználói profilok összefüggéseit vizsgálnom.

3.6.1 Biztonsági alkalmazás használata

A tizenkettedik kérdésre, ami a „Használ vírusvédelmi vagy tűzfal alkalmazást azon (azokon) az eszközön (eszközökön), amin internetezik?" 872 választ értékeltem, amelyek logikailag ellentmondásosak voltak, kizártam. A válaszadóknak a 25. ábra szerint, nagyon nagy száma,

92%-a „igen”-nel válaszoltak, míg „nem”-mel csak 6%-a. Az „egyéb” választ 2% jelölte be, és a válaszaik alapján az a jellemző, hogy laptopra, számítógépre használnak, de hordozható okos eszközre nem. Jól látható, hogy a túlnyomó többség használ valamilyen vírusvédelmet, de 8% vagy nem használ minden eszközön, vagy nem tudja, hogy használ-e, vagy „egyedi” elképzelései vannak a védelmi szoftverek alkalmazásáról. Ez a szám nagyon magas, mert ezeken a felhasználókon keresztül a többi rendszer, amihez hozzákapcsolódnak, sérülékennyé válhat.



25. ábra A kérdőív „Használ vírusvédelmi-, vagy tűzfal alkalmazást azon (azokon) az eszközön(kön), amin internetezik?” kérdésének kiértékelése (forrás: saját kérdőíves felmérés; készítette a szerző)

3.6.2 Rosszindulatú támadások

A tizenötödik kérdés az „Érte már vírus- és/vagy egyéb rosszindulatú támadás az Ön eszközét/eszközeit?” volt, amire 869 választ értékeltem, amelyek logikailag ellentmondásosak voltak, kizártam.

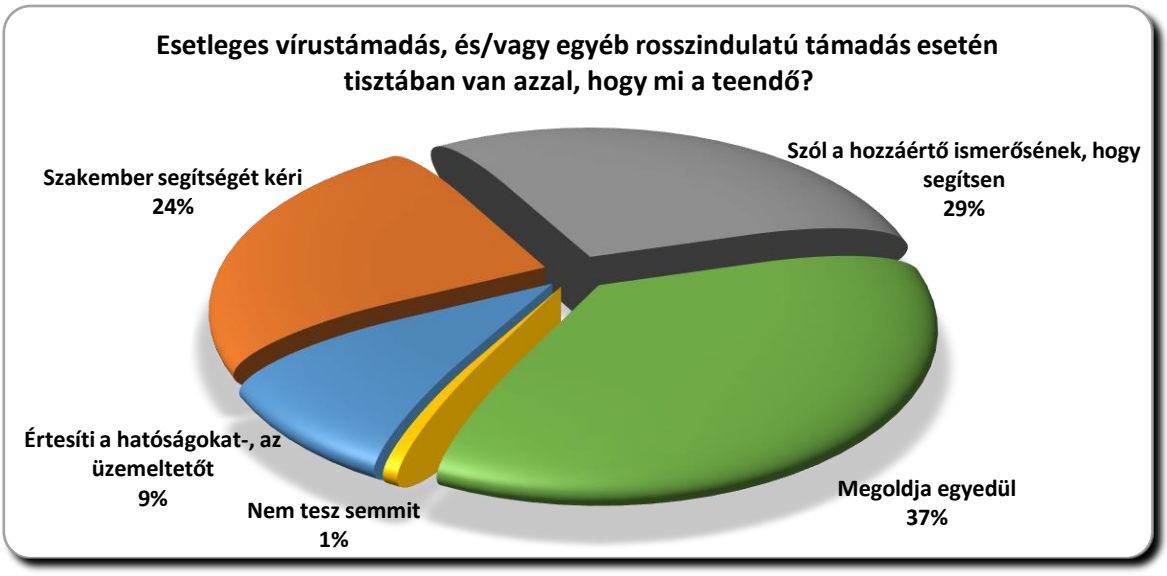
26. ábra A kérdőív „Érte már vírus- és/vagy egyéb rosszindulatú támadás az Ön eszközét/eszközeit?” kérdésének kiértékelése (forrás: saját kérdőíves felmérés; készítette a szerző)

Az „Igen” -t 59%, a „Nem” -et 20%, a „Nem tud róla” választ 21% válaszadó jelölte meg. Jól látható a 26. ábra szerint, hogy a válaszadók több, mint felét érte már rosszindulatú támadás.

Kijelenthető, hogy a válaszadók több mint felét biztosan érte rosszindulatú támadás és több, mint húsz százaléka nem tudja, tehát akár érhette is. A válaszadók mindössze egy ötödét (20%) nem érte rosszindulatú támadás a saját bevallása szerint.

3.6.3 Rosszindulatú támadás kezelése

A tizenhatodik kérdés az „Esetleges vírustámadás, és/vagy egyéb rosszindulatú támadás esetén tisztában van azzal, hogy mi a teendő?" kérdés volt, amire 946 választ értékeltem, amelyek logikailag ellentmondásosak voltak, kizártam. Az „Igen, felméri a károkat, próbálja minimalizálni a kárt, értesíti a hatóságokat-, az üzemeltetőt" 9%, az „Igen, szakember segítségét kéri" 24%, az „Igen, szól a hozzáértő ismerősének, hogy segítsen" 29%, a „Megoldja egyedül" 37%, a „Nem tesz semmit" választ a válaszadók 1%-a adta meg.



27. ábra A kérdőív „Esetleges vírustámadás, és/vagy egyéb rosszindulatú támadás esetén tisztában van azzal, hogy mi a teendő?" kérdésének kiértékelése (forrás: saját kérdőíves felmérés; készítette a szerző)

A 27. ábra alapján látható, hogy a válaszadók egy százaléka nem tesz semmit, viszont az összes többi valamilyen módon vagy segítség révén, vagy a saját tudása alapján megoldja a rosszindulatú támadásból származó problémákat.

3.6.4 Összegzés

A rosszindulatú támadások elleni védekezés és azokra a megfelelő válaszintézkedések megtétele jellemzi a magas biztonságtudatossággal rendelkező felhasználót. Ezt megoldhatja a felhasználó úgy, hogy egy magas kompetenciájú szakértő segítségét kéri, aki telepíti és beállítja a megfelelő alkalmazásokat vagy saját maga oldja meg. A kérdéscsalád válaszai tehát sok információt szolgáltatnak az átlag felhasználó biztonságtudatosságáról és kompetenciájáról is. A válaszadók kétharmadának a digitális kompetenciája nem elegendő egy esetleges

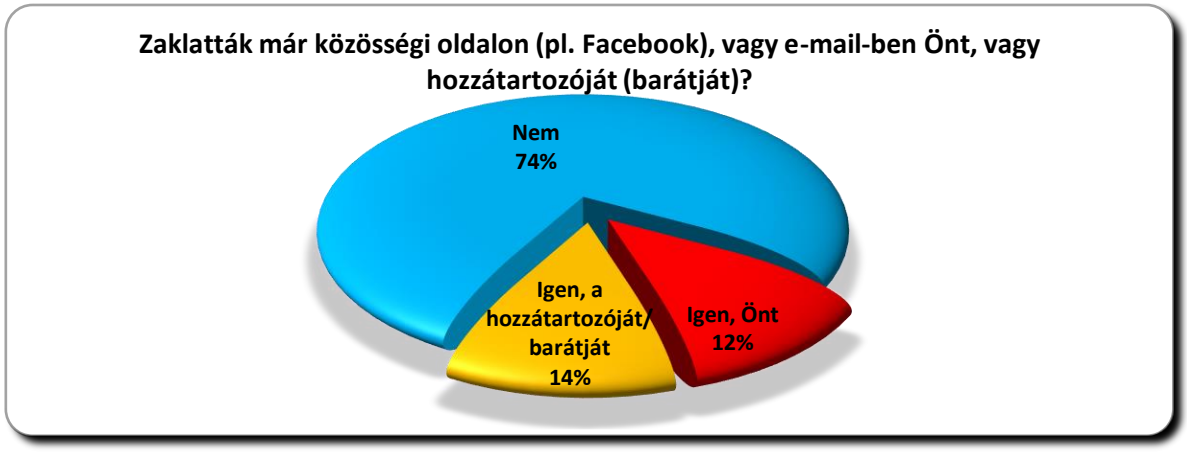
vírustámadás önállóan történő elhárítására. Az értékelések alapján kimondható, a digitális kompetencia fejlesztése a válaszadók körében szükséges.

3.7 Internetes zaklatás (cyberbullying)

Az Internetes zaklatás kérdéscsalád megalkotására annak aktualitása indított. Szakirodalmi kutatásaim alapján, ez egy olyan már korábban a fizikális világban is meglévő pszichológiai hadviselés új formája, amely a kibertérben elvesztve a tér és az idő korlátait, anonimitása és kiszámíthatatlansága miatt sokkal veszélyesebb fegyverré vált, válhat. Ennek a korai felismerése és megakadályozása, korunk egyik nagy kihívása.

3.7.1 Zaklatás

A „Zaklatták már közösségi oldalon (pl. Facebook), vagy e-mail-ben Önt, vagy hozzátartozóját (barátját)?” kérdés volt a tizenhetedik, erre 941 válasz érkezett. Az „Igen, Önt” 12%, az „Igen, a hozzátartozóját/barátját” 14%, a „Nem” lehetőségre 74% válasz érkezett.



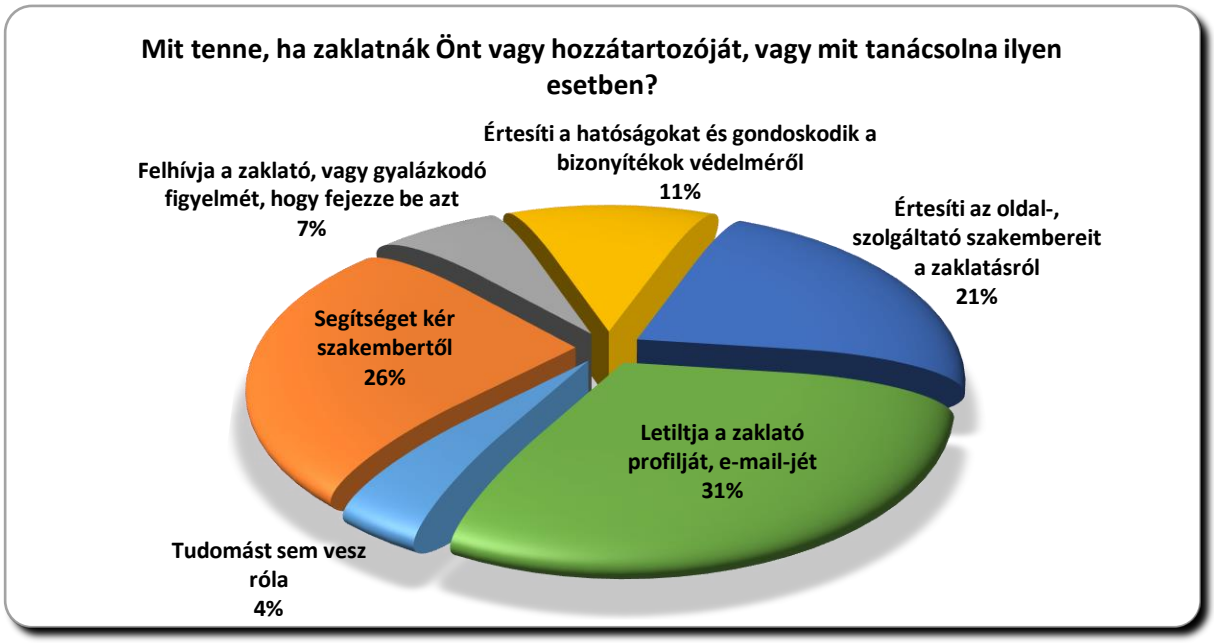
28. ábra A kérdőív „Zaklatták már közösségi oldalon (pl. Facebook), vagy e-mail-ben Önt, vagy hozzátartozóját (barátját)?” kérdésének kiértékelése (forrás: saját kérdőíves felmérés; készítette a szerző)

A 28. ábra értelmében jól látható, hogy a válaszadók 3/4-ét (74%) személyesen vagy ismerősi körét még nem érte internetes zaklatás.

3.7.2 Zaklatás kezelése

A „Mit tenne, ha zaklatnák Önt vagy hozzátartozóját, vagy mit tanácsolna ilyen esetben?” kérdésre a válaszadók közül 947 adott választ. Arra, hogy „Tudomást se vesz róla” 4%; a „Felhívja a zaklató, vagy gyalázkodó figyelmét, hogy fejezze be azt” 7%, a „Letiltja a zaklató profilját, e-mail-jét” 31%, a „Segítséget kér szakembertől” 26%, az „Értesíti az oldal-, szolgáltató szakembereit a zaklatásról” 11%, az „Értesíti a hatóságokat, és gondoskodik a bizonyítékok védelméről” 21% válasz érkezett. A 29. ábra alapján látható, hogy 100

válaszadóból 4 sajnálatosan tudomást sem vesz egy esetleges zaklatásról. Szerencsére a válaszadók többsége valamilyen formában fellép egy esetleges zaklatással szemben.



29. ábra A felhasználó zaklatással szemben mit tesz, tanácsol (forrás: saját kérdőíves felmérés; készítette a szerző)

3.7.3 Összegzés

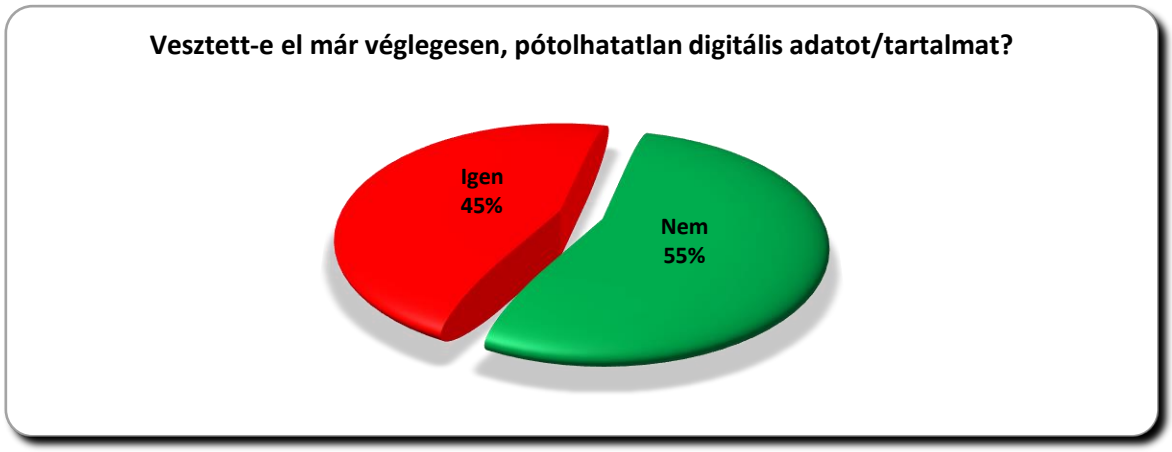
Az internetes zaklatás sajnos a kibervilág egy olyan negatív velejárója, mellyel bárki találkozhat. A felhasználók különböző módon reagálnak ezekre a támadásokra. Sok esetben a határozott fellépés a felhasználó megfelelő kompetenciaszintje esetén a megfelelő lépések megtétele gátat szabhat a zaklatásnak. A kutatásomban részt vevő felhasználók válaszai alapján megállapítom, hogy ezen a területen az önvédelmi reflexek fejlesztésével a felhasználó biztonságtudatosságát növelni kell.

3.8 Adatvagyon védelme

Az „Adatvagyon védelme” című kérdéscsalád esetében a digitális „vagyonunk” védelmét és annak kezelését mértem fel. Vannak olyan digitális adatok, melyek modern kori vagyonelemek, ezek elvesztésével, illetve kompromittálódásával komoly valós anyagi veszteség keletkezhet. Tehát a vagyonvédelem a kibertérben is elsőbbséget kell, hogy élvezzen.

3.8.1 Digitális adat elvesztése

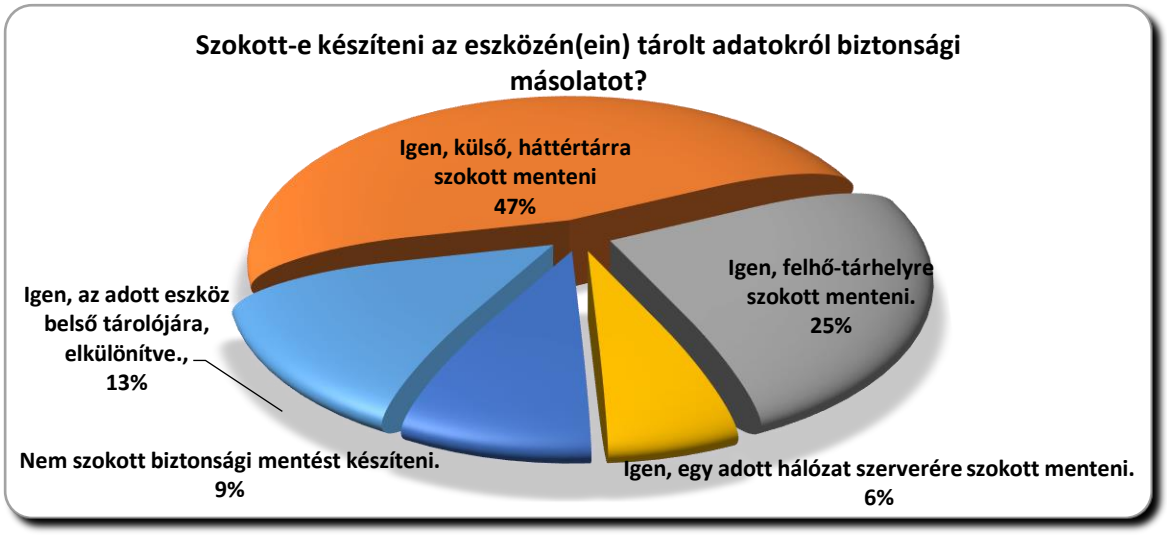
A tizenkilencedik kérdésre, ami a „Vesztett-e el már véglegesen, pótolhatatlan digitális adatot/tartalmat? (családi fotó-videó, saját készítésű fájl, címlista)” volt, 944 válasz érkezett. Ebből „Igen” 45% és a „Nem” 55% válasz volt. A 30. ábra jól ábrázolja, hogy a válaszadók több mint fele vesztett már el úgy adatot, hogy nem tudta azt pótolni.



30. ábra A kérdőív „Vesztett-e el már véglegesen, pótolhatatlan digitális adatot/tartalmat? (családi fotó-videó, saját készítésű fájl, címlista)" kérdésének kiértékelése (forrás: saját kérdőíves felmérés; készítette a szerző)

3.8.2 Biztonsági másolatok

A huszadik kérdésre, ami a „Szokott-e készíteni az eszközén (eszközein) tárolt adatokról biztonsági másolatot?" volt, 946 válasz érkezett. A „Külső, háttértárra szokott menteni (pendrive, memória kártya, külső merevlemez, CD/DVD)" 47%, „Az adott eszköz belső tárolójára, elkülönítve" 13%, „Egy adott hálózat szerverére szokott menteni" 6%, a „Felhő-tárhelyre szokott menteni" 25%, a „Nem szokott biztonsági mentést készíteni" 9% voksot kapott.



31. ábra Biztonsági másolat készítési szokások (forrás: saját kérdőíves felmérés; készítette a szerző)

A 31. ábra alapján jól látható, hogy a válaszadók közül majdnem minden tizedik nem készít egyáltalán biztonsági másolatot az érzékeny adatairól, ezzel szemben a válaszadók jelentős többsége gondoskodik az adatai védelméről. Az egyéb válaszok között jellemzően a külső- vagy felhő tárhely igénybevétele volt megjelölve, csak konkretizálva.

3.8.3 Biztonsági másolat készítésének gyakorisága

A felhasználók az előző kérdéshez kapcsolódóan kapták a „Milyen gyakorisággal készít biztonsági másolatot?” kérdést, amire 945 válasz érkezett. „Naponta” 5%, „Hetente” 8%, „Havonta” 15%, „Ritkában” 27%, „Csak bizonyos adatokról készít rendszertelenül. (pl. családi eseményen készült fotók esetében)” 34%, „Nem készít biztonsági másolatot” 11% válasz érkezett. A 32. ábra alapján jól látható, hogy a felhasználók közül minden tizenegyedik nem készít biztonsági másolatot az adatairól. A rendszeres biztonsági mentést végzők nagyon alacsony számban vannak mindössze a válaszadók kevesebb, mint egyharmada (28%). A rendszertelen időközönként mentést végzők aránya az összes válaszadónak majdnem kétharmada (61%). Ebből is látszik, hogy a megkérdezettek biztonságtudatossága nagyon alacsony. Tisztában vannak a biztonsági mentés fontosságával, de annál kényelmesebbek, mint hogy azt rendszeresen elvégezzék, a saját érdeküket figyelembe véve.

32. ábra A kérdőív „Milyen gyakorisággal készít biztonsági másolatot?” kérdésének a kiértékelése (forrás: saját kérdőíves felmérés; készítette a szerző)

3.8.4 Összegzés

Az adatvagyon védelme a mai digitális korunkban nagyon fontos. A felhasználó biztonságtudatosságát jól mutatja, hogy milyen módon védi adatait. Az adatvesztés mindig kárt jelent, ennek mértéke eltérő. Kutatási eredményeim alapján megállapítom, hogy a biztonsági másolat készítésének lehetőségével a kutatásban részt vevő felhasználók kis számban élnek [172][173].

3.9 Összefoglalás

Az általam lefolytatott kérdőíves felmérést és annak eredményeit, amely a generációk digitális kompetencia és biztonságtudatosság felmérésére irányult, alátámasztja azt a hipotézisemet, amely kimondja, hogy a különböző generációknak és az eltérő infrastruktúrával rendelkező embereknek nem azonos szintű a biztonságtudatossága. Látható továbbá, hogy az elmúlt harminc évben élt és a ma élő generációk között a digitális kompetencia és a biztonságtudatosság területén is éles különbségek vannak. A biztonságtudatosság és a digitális kompetencia kapcsolatának vizsgálatát szolgálta a kérdőívem, és az abból kinyert információk felhasználásával megfigyelhetők a fiatal felnőtt korú, a középkorú és az időskorú felhasználók problémái a digitális kompetencia és a biztonságtudatosság területén. Az informatika, az internet, az információs rendszerek és informatikai eszközök fejlődése és elérhetősége jelentős hatást gyakorol a felhasználók mindennapi életére, szokásaikra. A felhasználók adataik védelmét különböző módon igyekeznek megoldani, ami egyrészt az eltérő biztonságtudatosságra, másrészt az eltérő digitális kompetenciára vezethető vissza. A fiatalok esetében még a fizikai világban sem alakultak ki teljesen a védekezési reflexek, pedig azt a szüleiktől idősebb felnőtt ismerőseiktől naponta látják, látens tanulással lassan beléjük rögzül. A digitális világban a biztonságtudatosság kialakulása még nehezebb, hiszen a digitális eszközökön való kommunikáció, játék és különböző alkalmazások használata általában individuális tevékenység, melyet a felhasználók egyedül végeznek. Ezen a területen tehát nem jellemző a példa utáni látens tanulás, inkább saját kárukon keresztül jutnak ismeretekhez a felhasználók. A bemutatott diagramokon ez jól látható, tehát a vizsgált felhasználók nagy része veszített már adatot és érte vírustámadás, vagyis a saját kárán már tapasztalta a digitális világ veszélyeit. A kibertérben tehát veszélyekkel találkozik a felhasználó, melyekkel szemben védenie kell magát. A magasabb digitális kompetenciával és biztonságtudatossággal rendelkezők a kibertérben kevesebb támadással és káreseménnyel találkoznak. Eredményeimből arra következtetek, hogy a digitális kompetencia és a biztonságtudatosság között kapcsolat van. A kérdőívemre adott válaszok részletes eredményei, mind a 26 kérdésre egyesével, és azok grafikonos ábrázolása megalapozza a következő részekben leírt eredményeimet, megállapításaimat melyek a téziseim alapjául szolgálnak. A kérdőíves felmérésemből származó eredményekkel igazolom a hipotéziseimet, és ennek segítségével bizonyítom a téziseimet.

4 A DIGITÁLIS KOMPETENCIA ÉRTÉKELÉSI SZEMPONTRENDSZERE

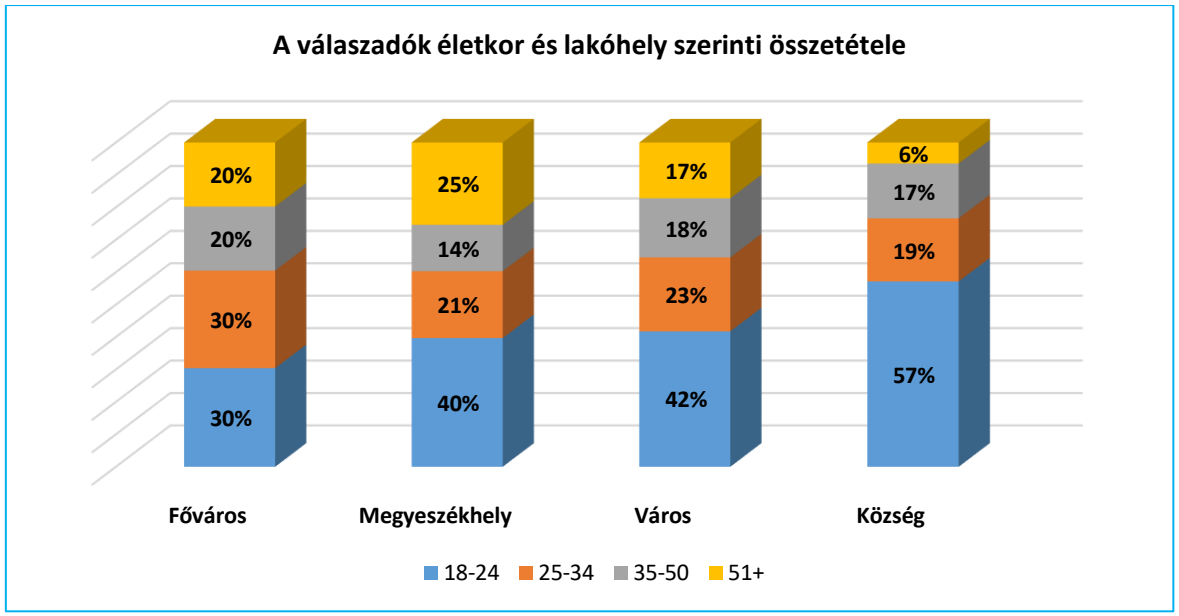
Az alábbi részben a biztonságtudatosság és a digitális kompetencia közötti kapcsolatokat vizsgálom különböző értékelési szempontok alapján. A kutatásom során a különböző mérési eredmények értékelésére korrelációs vizsgálatot alkalmaztam, ahol a korrelációs együttható abszolút értéke a mértékadó, amely alapján vizsgálati szempontok szerinti korrelációkat találtam [62].

4.1 A felhasználók életkor és lakóhely szerinti biztonságtudatosságának vizsgálata

A vizsgálatom arra irányult, hogy képet kapjak arról, hogy a lakóhely és az életkor alapján mennyi felhasználót ért már vírustámadás. Ezt olyan felhasználók esetében elemzem, akik gyakran interneteznek, használják a hotspot-ot, alkalmaznak vírusvédelmet, gyakran változtatják a jelszavaikat [63][156][157][158].

4.1.1 A válaszadók lakóhely és életkor szerinti eloszlása

A válaszadók lakóhely és életkor szerinti eloszlásának elemzése során látható (33. ábra), hogy a főváros(ok)ban közel azonos az életkor szerinti eloszlás, míg a többi helységek esetében az életkori eloszlás jelentősen elmozdul.

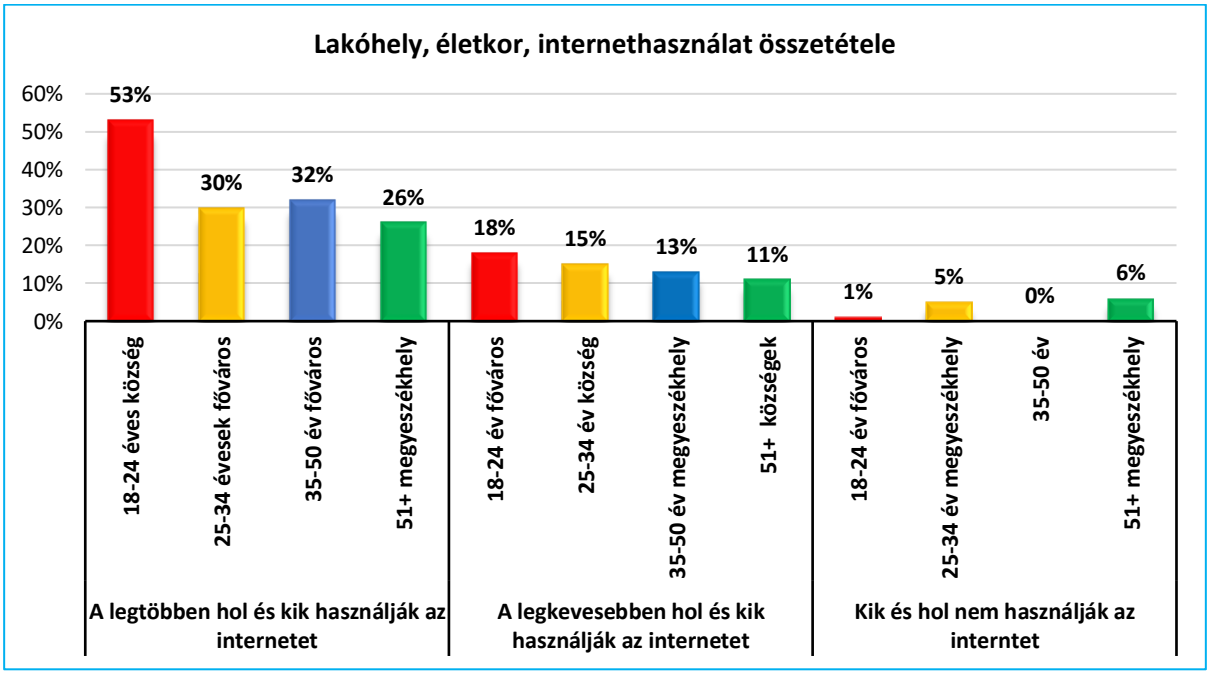


33. ábra A kérdőív "A válaszadók lakóhely szerinti eloszása" szempontjának a kiértékelése (forrás: saját kérdőíves felmérés; készítette a szerző)

A főváros esetében a 18-24 és a 25-34 korosztályok 30-30%-ban, a 35-50 és az 50+ korosztályok 20-20%-ban arányban képviselik magukat. Míg a többi vizsgált lakóhelyen a válaszadók az 18-24 korosztályhoz tartoznak inkább nagyobb számban.

4.1.2 A lakóhely, az életkor és az internethasználat kapcsolata

Az alábbi szempontokat tekintve megállapítható, hogy a megkérdezettek az életkort figyelembe véve a legtöbben a 18-24 év közötti válaszadók 53 %-a községekben, a 25-34 évesek 30 %-a és a 35-50 évesek 32%-a fővárosban, míg az 51 feletti életkorú válaszadók 26%-a megyeszékhelyeken él. A legkevesebben a 18-24 évesek közül (18%) a fővárosban, a 25-34 évesek (15%) és az 51 évnél idősebbek (11%) községekben, a 35-50 évesek (13%) megyeszékhelyeken élnek. A válaszadók szinte mindegyike használja az internetet, azonban a fővárosi 18-24 éveseknek 1%-a, a 35-50 évesek 5%-a és az 51 évnél idősebb válaszadók 6%-a megyeszékhelyeken élőknek nem használja az internetet, amelyet a 34. ábra mutat be [64][156][157][158].

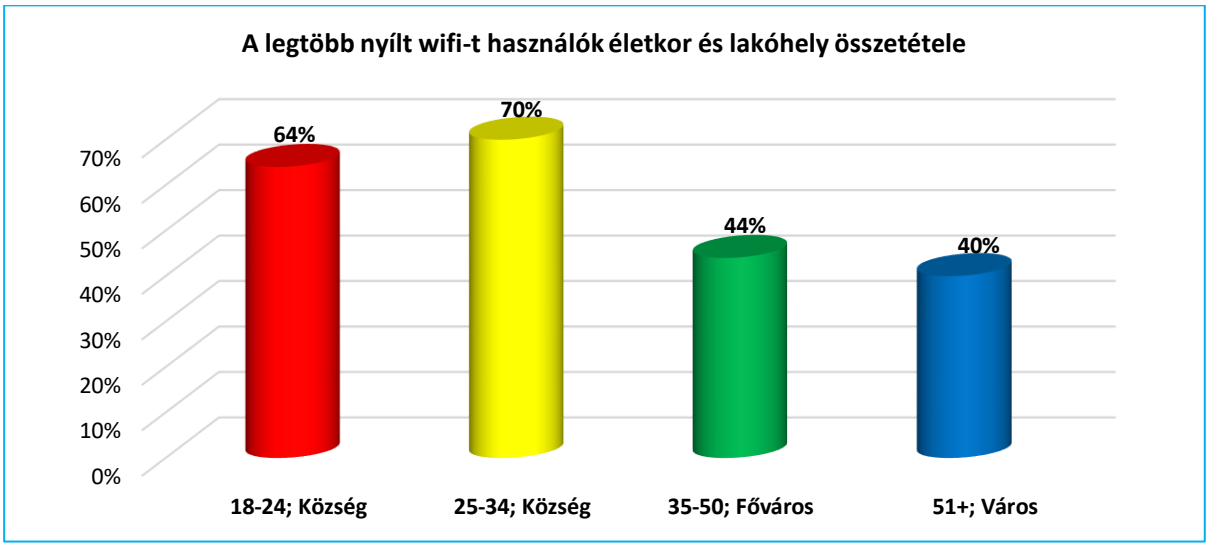


34. ábra A kérdőív válaszaiból levezetett korrelációk a lakóhely, az életkor és az internethasználat vonatkozásában (forrás: saját kérdőíves felmérés; készítette a szerző)[180][184]

4.1.3 A nyílt wifi-t használók életkor és lakóhely szerinti összetétele

Hordozható mobil eszköze, amin internetezni szokott, a 18-24 év közötti válaszadók közül csak a városban élők mindegyikének van. A 25-34 évesek közül a fővárosban élők kivételével mindegyiknek van ilyen eszköze. Csak a 35-50 év közötti és az 50 évnél idősebb városban és községben lakó válaszadók mindegyikének van ilyen mobil eszköze. Ezek közül a nyilvános wifi hálózatokat, a hotspot-okat a legtöbben a 18-24 éves (64%) és a 25-34 éves (70%)

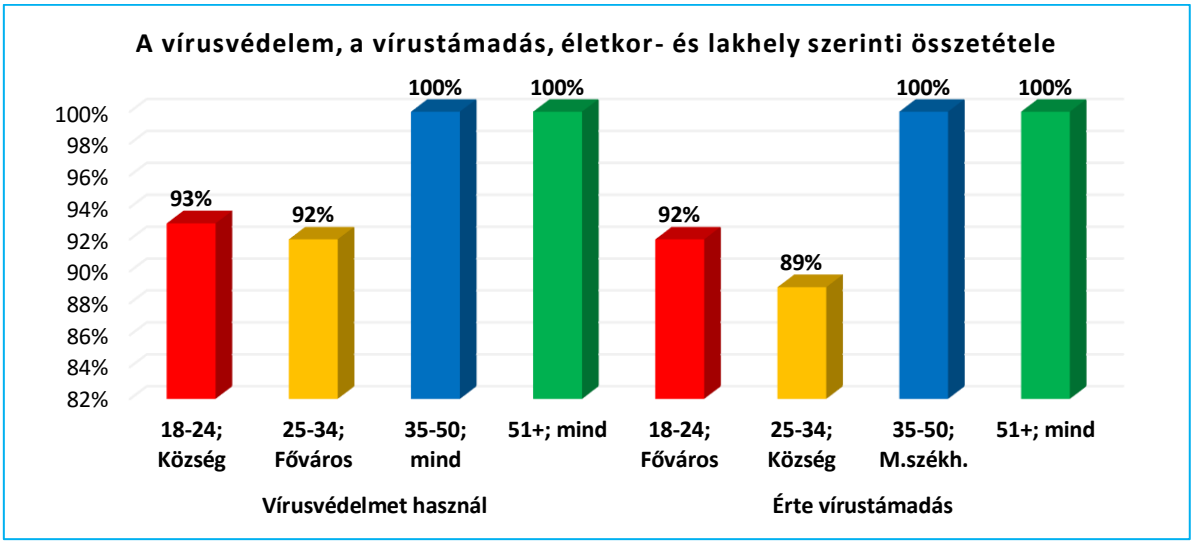
válaszadók közül a községben élők, a 35-50 éves fővárosiak (44%) és az 51 évnél idősebb városban élők (40%) szokták használni, amit a 35. ábra mutat be. Megállapítom, hogy a 25-34 év közötti községben élő válaszadók, folyamatosan használják az internetet és a legnagyobb arányban használják a hotspot-ot [65][66][156][157][158].



35. ábra A kérdőív válaszai alapján, a legtöbb, nyílt wifi-t használó életkor és lakóhely szerinti összetétele (forrás: saját kérdőíves felmérés; készítette a szerző) [157][158]

4.1.4 A vírusvédelmet használók és a vírustámadás-károsultak életkor és lakhely közötti kapcsolata

Vírusvédelmet, a fenti szempontokat is figyelembe véve, a 35-50 évesek és az 51 évnél idősebbek mindegyike használ.



36. ábra A kérdőív válaszai alapján, a legmagasabb számú vírusvédelmet használók és a vírustámadás-károsultak életkor és lakhely szerinti összetétele (forrás: saját kérdőíves felmérés; készítette a szerző) [157][158]

Ezzel szemben a 18-24 évesek közül a községben élők (93%), a 25-34 évesek közül a fővárosban élők (92%) használnak vírusvédelmet. Ezen válaszadók közül a legtöbb vírustámadás a 18-24 éves fővárosi felhasználókat (92%) és a 25-34 évesek közül a községben élő válaszadókat (89%) érte. Míg a 35-50 évesek közül a megyeszékhelyeken élők és az 51 évnél idősebb fővárosban és megyeszékhelyen élők mindegyikét érte már vírustámadás, amit a 36. ábra mutat be [67][156][157][158].

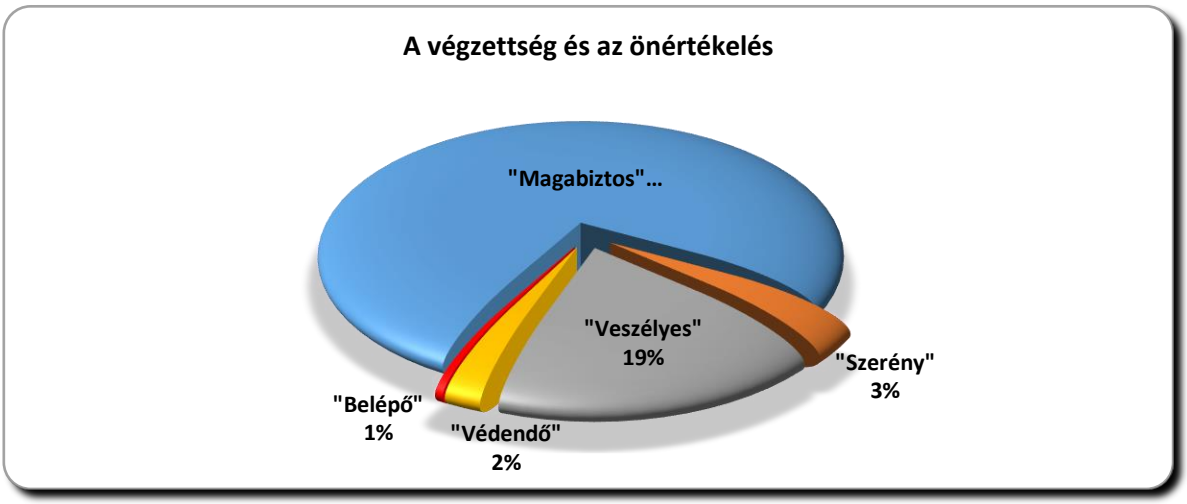
4.1.5 Összegzés

A felmérésem eredményeként megállapítom, hogy a vizsgált felhasználók digitális kompetenciáját és biztonságtudatosságát tekintve jelentős eltérés mutatható ki a lakóhely és az életkor szerint. A lakóhely meghatározza az elérhető infrastruktúrát, ami hatással van az internetezési szokásokra. Vidéken a nyílt wifi kevésbé széleskörű, mint a fővárosban. A lakóhely tehát igen fontos tényező. Emellett életkor szerint is találtam különbségeket, hiszen a digitális bennszülöttek már születésüktől a digitális rendszerben élnek. A fiatalabb korosztály digitális kompetenciája magasabb fokú, mint az idősebb korosztályoké. Ezzel szemben az idősebb korosztály rendelkezik magasabb biztonságtudatossággal, ami a fizikai valós térben az évek során kialakult „reflexeknek" köszönhető, mert azt könnyebben át tudták ültetni a kibertérre. A probléma csak az, hogy a biztonságtudatosságukat az alacsonyabb digitális kompetenciájuk miatt nem tudják olyan szinten alkalmazni, mint a fiatalabb generációk, akiknek a digitális kompetenciája magasabb fokú, de még nem alakult ki megfelelően a biztonságtudatosságuk. A lakosság eltérő digitális kompetenciája és biztonságtudatossága biztonsági kockázatot jelent. A felhasználókat ezért vizsgálni, biztonsági kockázat szerint csoportosítani kell, ennek alapján pedig erősíteni a gyengeségeket képzéssel. A lakosság digitális jóléte, biztonságos internethasználatának szintje képzéssel növelhető [156][157][158].

4.2 A felhasználók besorolási szempontjai

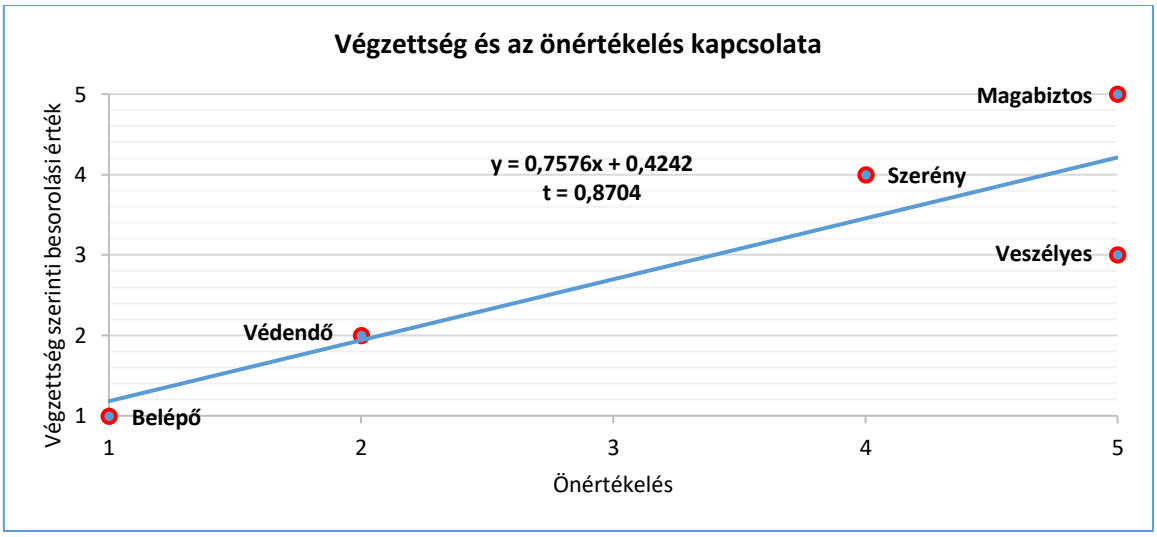
A felhasználók nem minden esetben tudják saját kompetenciaszintjüket reálisan felmérni, ezért az iskolai végzettséget, ezen belül is az informatikai ismereteket tekintettem mérvadónak, és a hozzá válaszul adott önértékelési szintet kritikával kezeltem, főként akkor, ha a két besorolási kategória között jelentős különbség volt [68]. Az általam definiált öt csoporthoz (37. ábra) az oktatási rendszerben alkalmazott értékeléseket hozzárendelve a következő osztályzatokat adtam a felhasználóknak: magabiztos (5), védendő (2), szerény (4), veszélyes (3), belépő (1). A kérdőívek kiértékelése során alkalmaztam a Pearson korrelációs együttható értékének meghatározását (r), valamint ebből az értékből a determinációs együtthatót ($d=r^2 \cdot 100$ (%)) is meghatároztam, mely a lineáris típusú korrelációs kapcsolat mérőszáma. A korrelációs

együttható abszolút értéke, ha |r|=0 nincs kapcsolat, 0<|r|<0,3 gyenge kapcsolat 0,3<|r|<0,7 közepes kapcsolat 0,7<|r|<1 erős kapcsolat |r|=1 determinisztikus kapcsolat. Lineáris regresszió esetén, ami a változók közötti lineáris kapcsolat erősségére utal, a kapcsolat erősségét a determinációs együttható %-ban határozza meg [69][70].



37. ábra Az informatikai végzettség és az önértékelés kapcsolata (forrás: saját kérdőíves felmérés; készítette a szerző)

A 38. ábra a valós tudás és az önértékelés értékei közötti erős korrelációt mutatja (korrelációs együttható |r|=0,8704). Ebből egyszerű számítással ($d=r^2*100$ (%)) meghatároztam a determinációs együtthatót, mely a végzettség és önérékelés kapcsolatát tekintve 75,76%, tehát a lineárisra jól illeszkedik. A kiszámított értékekkel, valamint az előzőekben (3.4; 3.5; 3.6; 3.8 alfejezet) bemutatott kapcsolatok által bizonyítást nyer, hogy a besorolást helyesen végeztem, a felhasználók besorolása a kibertérben mutatott viselkedésük értékét jelenti [161][165].



38. ábra Az informatikai végzettség és az önértékelés korrelációja (forrás: saját kérdőíves felmérés; készítette a szerző)

Az elvégzett felmérés szerint kimutatható az, hogy maga a felhasználó a legveszélyesebb a rendszert tekintve. Az értékelés eredménye szerint azok a válaszadók, akik azokra a kérdésekre, hogy „Milyen szintűnek értékeli a saját informatikai ismereteit és biztonságtudatosságát?" valamint „Milyen szintű informatikai ismerettel rendelkezik?" az általam definiált csoportokat az alábbiakban mutatom be [71]. A "Belépő" csoportra vonatkozóan kisszámú adatot sikerült regisztrálni, mivel ők még nem használják az internetet, ezért a további eredmények szempontjából ennek a csoportnak az értékelésével nem számolok.

4.2.1 A „Veszélyes" felhasználó

Ebbe a kategóriába azokat az amatőröket soroltam, akik a potenciális veszélyforrást jelenthetik. Általában ebből a kategóriából kerülnek ki a cégek „shadow IT" azaz a „árnyék informatikus" „szakemberei". Azokat a válaszadókat gyűjtöttem ide, akik a kérdésekre a következő válaszokat adták: „A környezete kikéri az Ön véleményét az informatikai kérdésekben, naprakész ismerete van a biztonsági megoldások területén."; „Egyedül konfigurálja a számítógépet/okostelefont, általában figyelemmel követi a biztonsági trendeket."; „Az interneten kívül sok alkalmazást használ a számítógépen/okostelefonon, figyel a biztonságra." valamint „Nem rendelkezik informatikai ismeretekkel."; „Önmagától vagy ismerőse segítségével sajátította el. Tehát nincs semmilyen informatikai végzettsége, de jónak mondja magát (az önértékelését nem támasztja alá). A vizsgálat alapján a válaszadók 18%-ára mondható ki a „veszélyes" jelző [161][163].

4.2.2 A „Védendő" felhasználó

Ebbe a kategóriába azokat a kezdő felhasználókat soroltam, akik szintén veszélyforrást jelentenek, viszont mivel feltehetően tisztában vannak a saját képességeikkel (a végzettség és a saját kompetenciaszint megítélése közel azonos), ezért óvatosabban használják az internetet. Azokat a válaszadókat gyűjtöttem ide, akik a fenti kérdésekre „Nincs semmilyen informatikai ismerete, nem tudja, mi az a biztonságtudatosság."; „Rendszeresen használja az internetet, általában biztonságtudatos", valamint a „Nem rendelkezik informatikai ismeretekkel."; „Önmagától vagy ismerőse segítségével sajátította el." válaszokat adták. Tehát nincs semmilyen informatikai végzettsége, és nem is vallja magát csak átlagosnak vagy az alattinak. A fenti vizsgálatban a felhasználók mindössze 4%-a sorolható be, a „védendő" kategóriába [161][163].

4.2.3 A „Szerény" felhasználó

Ebbe a kategóriába azokat a félprofi felhasználókat soroltam, akik rendelkeznek valamilyen informatikai végzettséggel/tanfolyammal, viszont a képességeiket alacsony szintűnek ítélik

meg (az iskolai végzettség és a saját önértékelés azonos szintet mutat). Azokat a válaszadókat gyűjtöttem ide, akik a kérdésekre a „Rendszeresen használja az internetet, általában biztonságtudatos”; „Nincs semmilyen informatikai ismerete, nem tudja, mi az a biztonságtudatosság.” valamint a „Az egyetemen/középiskolában tanult informatikát.”; „Tud programozni egy vagy több programnyelven.”; „Van ECDL vizsgája.”; „Van egyetemi/középiskolai informatikai végzettsége.”; „Informatikai tanfolyamot végezett.” válaszokat adták. Tehát rendelkezik informatikai végzettséggel, de átlagosnak vagy az alattinak vallja magát. A fenti vizsgálatban a felhasználók mindössze 8%-a sorolható be ebbe a „szerény” kategóriába [161][163].

4.2.4 A „Magabiztos” felhasználó

Ebbe a kategóriába azokat a profi felhasználókat soroltam, akik rendelkeznek informatikai végzettséggel/tanfolyammal és digitálisan kompetensnek, valamint biztonságtudatosnak vallják magukat. Ez a felhasználói csoport az, aki már nem csak, mint egyszerű felhasználó, hanem akár rendszeradminisztrátorként vagy egyéb üzemeltetőként lehet jelen a kibervilágban. Azokat a válaszadókat gyűjtöttem ide, akik a kérdésekre a „A környezete kikéri az Ön véleményét az informatikai kérdésekben, naprakész ismerete van a biztonsági megoldások területén.”; „Egyedül konfigurálja a számítógépet/okostelefont, általában figyelemmel követi a biztonsági trendeket.”; „Az interneten kívül sok alkalmazást használ a számítógépen/okostelefonon, figyel a biztonságra.” valamint „Az egyetemen/középiskolában tanult informatikát.”; „Tud programozni egy vagy több programnyelven.”; „Van ECDL vizsgája.”; „Van egyetemi/középiskolai informatikai végzettsége.”; „Informatikai tanfolyamot végezett.” válaszokat adták. Tehát rendelkezik informatikai végzettséggel, és jónak mondja magát a biztonság és a kompetencia területén. A fenti vizsgálatban a válaszadók 70%-a sorolható be, a „magabiztos” kategóriába [161][163].

4.2.5 A “Belépő” szintű felhasználó

A “Belépő” szintű felhasználók azok a természetes személyek, akik egyáltalán nem használják a digitális eszközöket. Azok a felnőtt korúak értendők ebbe a csoportba, akiknek nincs lehetősége használni a modern korunk által biztosított digitális lehetőségeket, esetleg valamilyen okból nem is akarják. Továbbá azok a csecsemőkorú gyerekek, akik még nincsenek abban a korban, hogy már használják valamilyen formában a digitális eszközöket. A kutatásaim bizonyítják azt, hogy ilyen csoportok valóban léteznek, mivel a 3.4.1 bekezdésben látható, hogy az összes válaszadó mindössze 0,6%-a nem használja az internetet (11. ábra). Mivel ez a szám

nagyon alacsony, ezért a válaszok eredményei nem alkalmazhatók a csoport jellemzésére, viszont a csoport létét igazolják [160].

4.2.6 Összegzés

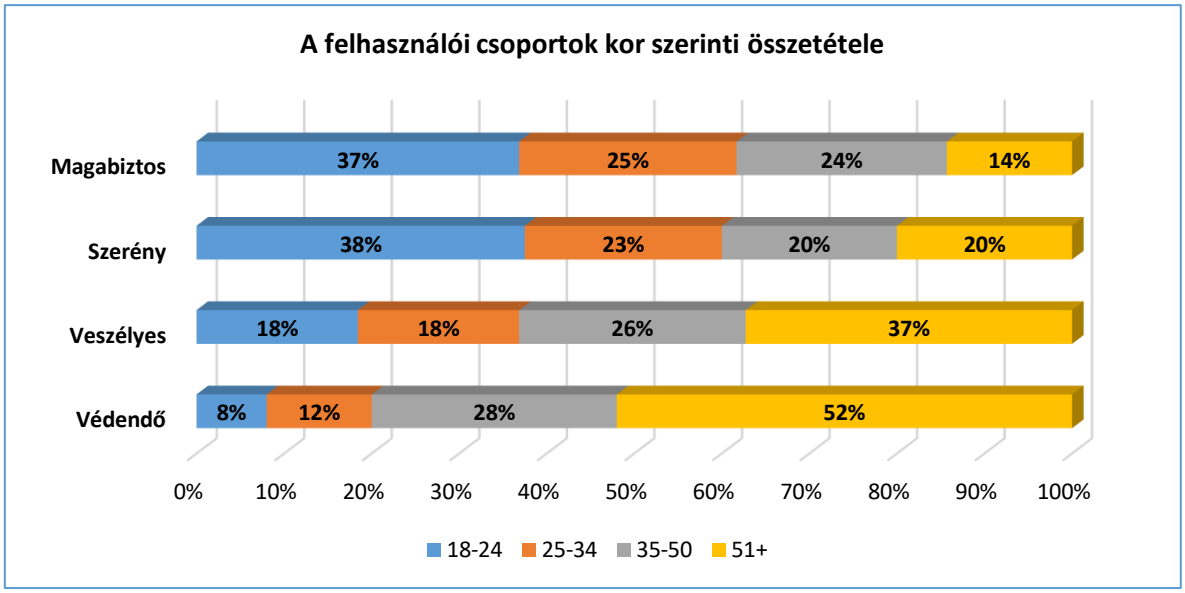
A továbbiakban az általam definiált öt felhasználói csoporthoz egyenként a 37. ábra és a 38. ábra esetében is alkalmazott besorolási értéket rendeltem, azaz osztályzatokat alkalmazva értékelem az egyes csoportok és a kibertérben történő viselkedésük, tevékenységük kapcsolatát, valamint az önértékelés és a valós kompetencia közötti korrelációt. Megállapítom, hogy az általam kidolgozott kérdőív kérdései, mint módszer és viselkedésspecifikus szempontrendszer, és az abból kinyert válaszok alapján a felhasználók digitális kompetencia és biztonságtudatosság szempontjából besorolhatók azokba a felhasználói csoportokba, amelyeket megalkottam. Olyan módszer- és viselkedésspecifikus szempontrendszert állítottam fel, amely alkalmas a felhasználók kockázati célú értékelésére most és a jövőben.

4.3 A felhasználói csoportok életkor és lakóhely szerinti összetételének a vizsgálata

Az előző részben definiált és általam vizsgált felhasználócsoportok lakóhely és életkor szerinti összetételének vizsgálata nagyon fontos, hogy a felhasználói csoportok oktatásának a megszervezése hatékony legyen.

4.3.1 A felhasználói csoportok életkor szerinti összetételének vizsgálata

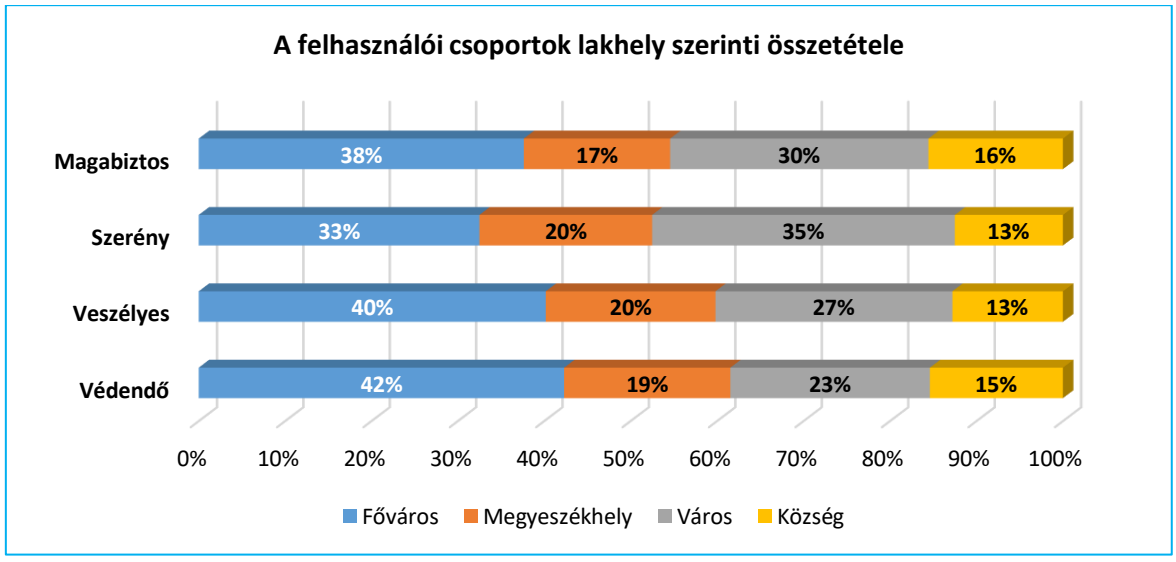
Az általam definiált és a kérdőíves felmérésben vizsgált felhasználói csoportok esetében (39. ábra) a 1167 válaszadónak a „Milyen korcsoporthoz tartozik?” kérdésre adott válaszát tudtam figyelembe venni. Az összetételt tekintve megállapítható, hogy minden korosztály esetén a „Magabiztos” felhasználói csoport lélekszáma a legnagyobb, ebben a felhasználói csoportban a 18-24 éves korosztály kategóriába a felhasználók 37%-a tartozik. A korosztályok közötti arányt tekintve a 18-24 éves korosztály „Magabiztos” felhasználói vannak a legtöbben, összesen 85%. A felhasználói csoportokat figyelembe véve az 51+ „Védendő” felhasználók aránya a legmagasabb, 52%. Továbbá megállapítható az is, hogy a legkisebb számú felhasználói csoport a 18-24 éves korosztály „Védendő” felhasználói csoportja, ide tartozik a válaszadók 8%-a. Továbbá megállapítható az is, hogy a legkisebb számú felhasználói csoport a 18-24 éves korosztály „Védendő” felhasználói csoportja. Az összes válaszadó 0,17%-a, ez a „Védendő” csoport 8%-a, és a korosztályokat tekintve mindössze 1%.



39. ábra A felhasználói csoportok kor szerinti összetétele (forrás: saját kérdőíves felmérés; készítette a szerző)

4.3.2 A felhasználói csoportok lakóhely szerinti összetételének vizsgálata

Az előző ponthoz hasonlóan elemeztem az általam definiált és a kérdőíves felmérésben vizsgált felhasználói csoportokat. „A felsoroltak közül Ön hol él?” kérdésre 1159 válaszadó válaszát vettem figyelembe. (40. ábra) Az összetételt tekintve megállapítható ebben az esetben is, hogy minden lakóhelyre vonatkozóan a „Magabiztos” felhasználói csoport lélekszáma a legnagyobb, ebbe a felhasználói csoportba a fővárosban élő felhasználók tartoznak, mintegy 38%. A lakóhelyek közötti arányt figyelembe véve a fővárosban lakó „Magabiztos” felhasználók vannak a legtöbben, összesen 75%.

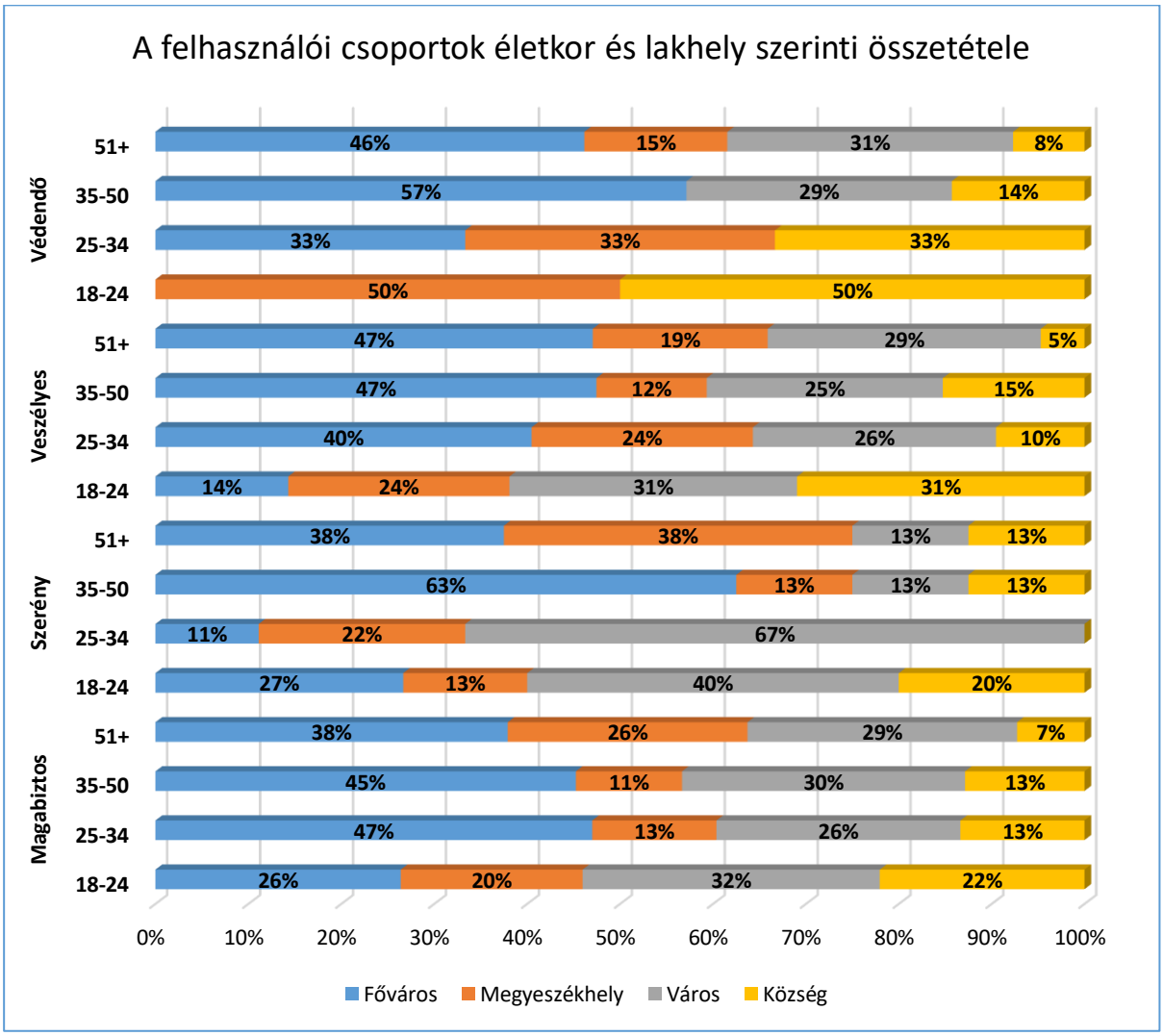


40. ábra A felhasználói csoportok lakhely szerinti összetétele (forrás: saját kérdőíves felmérés; készítette a szerző)

A felhasználói csoportok szempontjából nézve a fővárosban élő „Védendő” felhasználók aránya a legmagasabb, ez 42%. Továbbá megállapítható az is, hogy a legkisebb számú felhasználói csoport a községben élő „Védendő” felhasználók csoportja. Az összes válaszadó 0,35%-a, ez a „Védendő” csoport 15%-a, és a korosztályokat tekintve mindössze 2%.

4.3.3 A felhasználói csoportok életkor és lakóhely szerinti összetételének vizsgálata

A felhasználói csoportok életkor és lakóhely szerinti összetételének vizsgálata során 1166 felhasználó válaszát vizsgáltam és értékeltem ki. (41. ábra)



41. ábra A felhasználói csoportok életkor és lakhely szerinti összetétele (forrás: saját kérdőíves felmérés; készítette a szerző)

A „Magabiztos” felhasználói csoport számát nézve a városban élő 18-24 korosztály tagjai vannak legtöbben, az életkor arányát alapul véve 32%. A lakóhely aránya alapján a legtöbben a községben élő 18-24 éves felhasználók vannak, ez 52%. A legkevesebben számosságot tekintve a községben élő 51+ korosztály van, életkort és lakóhelyet alapul véve 7-7%.

A „Szerény” felhasználói csoport számát nézve a városban élő 18-24 és a 25-34 éves korosztály tagjai vannak legtöbben, az életkor arányát alapul véve 40 és 67%, a lakóhely aránya alapján 43-43%.

A „Veszélyes” felhasználói csoport számát nézve a fővárosban élő 51+ korosztály tagjai vannak legtöbben, az életkor arányát alapul véve ez 44%. A lakóhely aránya alapján a legtöbben a községben élő 18-24 éves felhasználók vannak, ez 48,72%. A legkevesebben számosságot tekintve a községben élő 25-34 évesek vannak, életkort alapul véve 9,3%, a lakóhelyet tekintve 8,25% a 18-24 éves fővárosban élők aránya.

A „Védendő” felhasználói csoportot vizsgálva a fővárosban élő 35-50 éves felhasználók vannak a legtöbben, az arányokat tekintve a korosztály alapján 57%, míg a lakóhely szerint 55%.

4.3.4 Összegzés

A felhasználókat a besorolási értékükhöz kapcsolva, a lakóhely és az életkor szerinti megoszlás szerint vizsgálva megállapítom, hogy a fiatal korosztályok aránya domináns minden területen. Azonban a vizsgálat alapján jól feltérképezhető, hogy mely felhasználói csoportok életkor szerint hol élnek. Ez a kormányzat számára, valamint a biztonságtudatosság és a digitális kompetencia fejlesztésére szakosodott szervezetek számára szolgálhat olyan információval, hogy a társadalom mely rétegének képzésére, oktatására milyen módszert alkalmazva tudja fejleszteni a képességeket és készségeket.

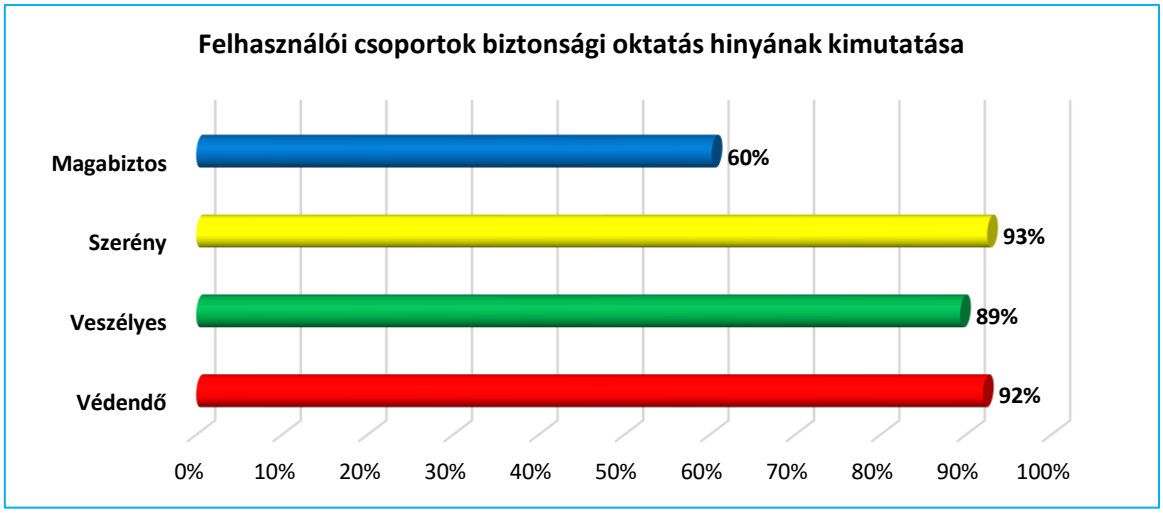
4.4 A felhasználók biztonsági oktatásának vizsgálata

Az általam lefolytatott kérdőíves felmérés eredményei alapján definiált négy felhasználói csoport tekintetében vizsgálom, hogy milyen a felhasználók motiváltsága a biztonsági oktatások, képzések, valamint egy ingyenes informatikai képzésen való részvétel lehetőségének az esetleges kihasználása terén. Másik fontos szempont, melyre kutatásomban figyelmet fordítottam, hogy a felhasználók a munkájukhoz szükséges informatikai ismeretek szintjeit hogyan határozzák meg, mivel ez a velük szemben támasztott elvárást mutatja meg. Fontos tehát, hogy a felhasználó az általa megadott és a munkaadó vagy iskola által meghatározott informatikai ismeretszint különbségének megszüntetésére mennyire motivált, ezt az általam feltett kérdések közötti kapcsolatokkal mutatom be [72][165].

4.4.1 A felhasználói csoportok és a biztonsági oktatás összefüggése

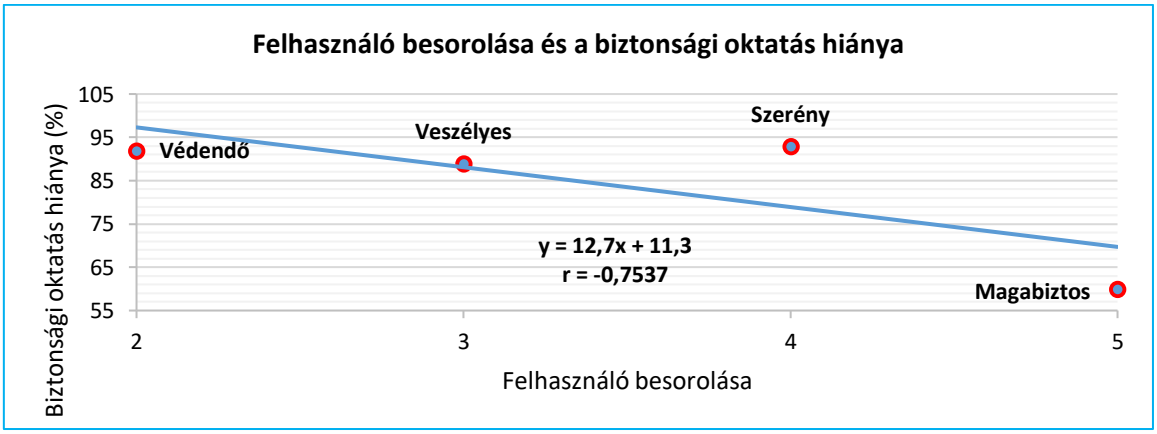
Az ebben a pontban szereplő vizsgálat célja az általam korábban definiált felhasználói csoportok és a biztonsági oktatáson való részvételük arányának kimutatása volt. A vizsgálat

során a négy felhasználói csoport esetében a „Vett már részt valaha információbiztonsági oktatáson, képzésen?” kérdésre a „Nem” vagy „Nem emlékszik” válaszokat vettem alapul.



42. ábra Felhasználói csoportok esetén a biztonsági oktatás hiányának kimutatása (forrás: saját kérdőíves felmérés; készítette a szerző)

A vizsgálat eredményéből látható (42. ábra), hogy a „Védendő” csoport tagjai esetében fordul elő a legkisebb arányban (92%) az, hogy nem vettek részt biztonsági oktatáson, vagy nem emlékeznek rá. A „Szerény” csoportba tartozó felhasználók esetében látható, hogy (93%) a legnagyobb számban nem vettek részt ilyen képzésen. Ennek a két csoportnak a tagjai az önértékelés során azt vallották, hogy a biztonságtudatossági szintjük alacsony. Ebben az esetben ezen felhasználók oktatása vagy nem volt elég hatékony, vagy nem kellő gyakorisággal vettek részt ilyen képzésen. A „Magabiztos” felhasználók esetében nagy százalékban fordul elő (60%), hogy ezek a felhasználók nem vettek részt ilyen képzésen, ezért vélelmezni lehet, hogy ennek a csoportnak a tagjai foglalkozásszerűen informatikai felhasználással foglalkoznak.

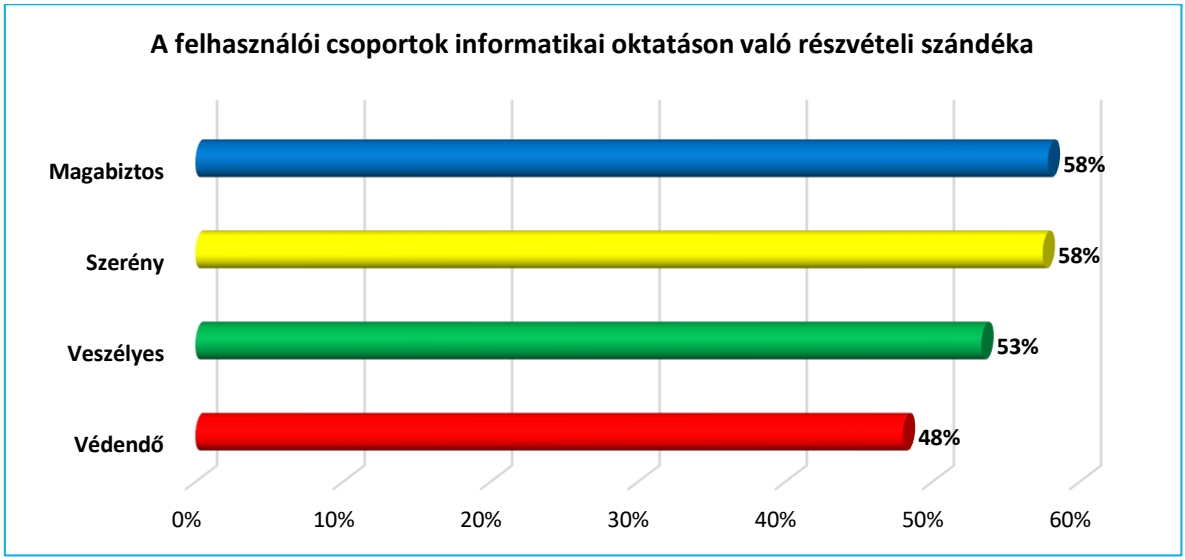


43. ábra Korreláció a felhasználói csoportok és a biztonsági oktatás hiánya között (forrás: saját kérdőíves felmérés; készítette a szerző)

A „Veszélyes” csoport esetében látható (89%), hogy ezen felhasználók közül tízből kilenc fő egyáltalán nem vett még részt ilyen oktatáson, bár saját magukat jó biztonságtudatosságúnak jellemezték, ezzel szemben nem rendelkeznek semmilyen informatikai végzettséggel. (43. ábra) A biztonsági oktatás hiánya az egyes csoportok esetén erős korrelációt mutat a felhasználói besorolásuk értékével, mivel a korrelációs együttható abszolút értéke 0,7537. A negatív előjel pedig azt mutatja, hogy minél magasabb besorolású a felhasználó, annál kevésbé jelenik meg a biztonsági oktatás hiánya. Tehát a “Magabiztos” felhasználók nagyobb arányban vettek részt biztonsági oktatáson, mint a többi felhasználói csoport tagjai. A fenti vizsgálat alapján megállapítom, hogy a felhasználók hatékony biztonsági oktatása nagymértékben szükséges, és annak rendszeres megismétlése növeli a biztonságtudatosság szintjét, illetve magas szinten tartaná azt, tekintettel az informatika rohamos fejlődésére és a biztonsági kihívások robbanásszerű növekedésére [73][165].

4.4.2 A felhasználói csoportok informatikai oktatáson való részvételének szándéka

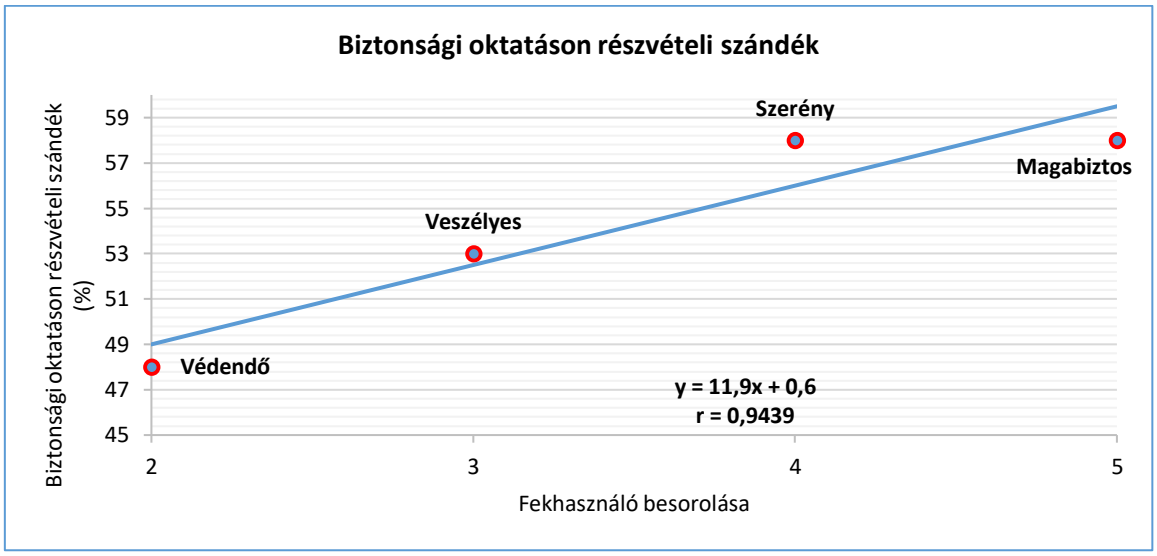
Az alábbi pontban a felhasználók informatikai oktatáson való részvételének szándékát vizsgáltam. A „Ha lehetősége lenne egy ingyenes tanfolyam, vagy oktatás keretében digitális ismereteket elsajátítani, részt venne rajta?” kérdésre az „Igen” válaszokat vettem figyelembe.



44. ábra A felhasználói csoportok informatikai oktatáson való részvételi szándéka (forrás: saját kérdőíves felmérés; készítette a szerző)

A vizsgálat eredménye azt mutatja (44. ábra), hogy a „Magabiztos” csoportba tartozó válaszadók részvételi szándéka a legmagasabb (58%), annak ellenére, hogy ennek a csoportnak a tagjai rendelkeznek valamilyen informatikai végzettséggel, és a biztonságtudatosságukat is magasfokúként jelölték meg. A „Szerény” csoport válaszaiból kiderül, hogy a kérdésben szereplő oktatást a válaszadóknak szintén 58%-a vállalná. Ez a csoport rendelkezik ugyan

informatikai képzettséggel, viszont, a biztonságtudatosságukat alacsonynak értékelték. A „Veszélyes” csoport tagjai által adott válaszok alapján kiderül, hogy a válaszadók több mint fele (53%) venne részt egy ilyen informatikai képzésen. A korábbi definíció alapján látható, hogy ez a csoport nem rendelkezik semmilyen informatikai végzettséggel. A legkevesebb számú válaszadó (48%) a „Védendő” csoportból adta azt a választ, hogy részt venne informatikai oktatáson (45. ábra).

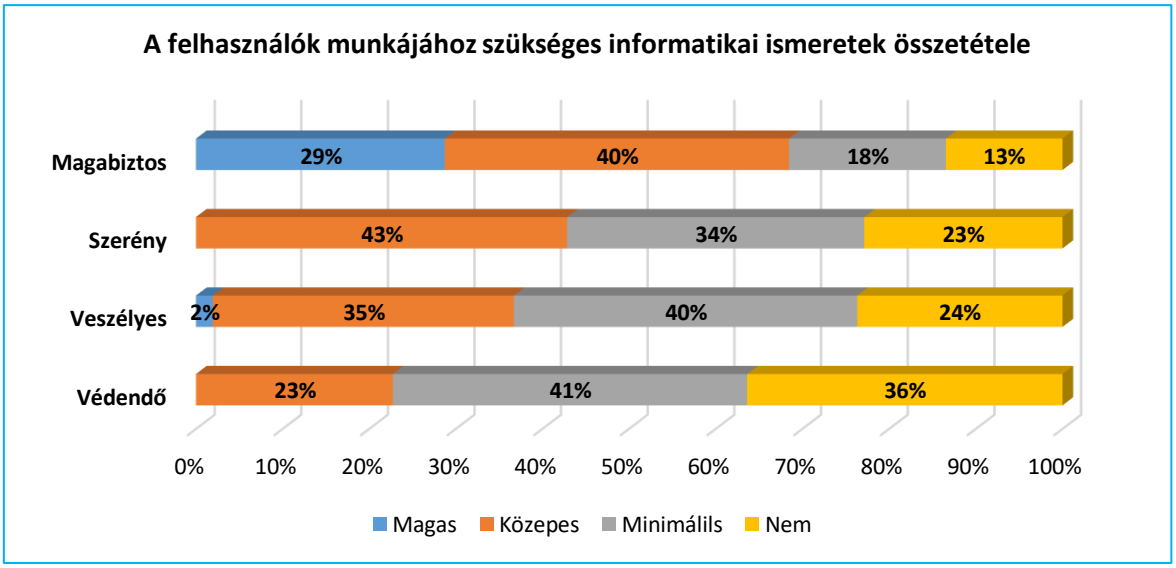


45. ábra A felhasználói csoportok informatikai oktatáson való részvételi szándéka (forrás: saját kérdőíves felmérés; készítette a szerző)

A biztonsági oktatáson való részvételi szándék és a felhasználói besorolás között erős a korreláció (|r|=0,9439). A már képzettséggel rendelkező, magas besorolási értékű felhasználók további ismereteket szeretnének szerezni, nagy számban vennének részt oktatáson, hiszen tudják, hogy ez szükséges. Az alacsony képzettségűeknek pedig csak kis része érdeklődik. Ez az eredmény, megegyezik a DJP-ben közölt megállapított felmérés eredményével. Azaz, azon felhasználók, akik alacsony digitális képzettséggel rendelkeznek, elutasítóak a további tanulással szemben [74][165]. Megállapítom az eredmények és a DJP felmérései alapján, hogy a képzéssel a felhasználói biztonságtudatosság növekszik, mert így a felhasználó belátja a folyamatos élethosszig tartó tanulás szükségességét, mivel az informatika és a digitális eszközök folyamatosan fejlődnek.

4.4.3 Az informatikai ismeretek munkához való szükségessége és a felhasználói csoportok vizsgálata

Az alábbi vizsgálati szempontok alapján lefolytatott elemzés azt mutatja be, hogy milyen összetételben van szüksége a felhasználóknak az informatikai ismeretekre a munkavégzésben (46. ábra).



46. ábra A felhasználók munkájához szükséges informatikai ismeretek összefüggésének vizsgálata (forrás: saját kérdőíves felmérés; készítette a szerző)

Az „Amennyiben dolgozik, a munkájához szükséges az informatikai ismeret?” kérdésre az „Igen, magas fokú ismeretek (speciális végzettség, céltanfolyam)”, az „Igen, közepes ismeretek (tanfolyam)”, az „Igen, minimális ismeretek (betanított)” és a „Nem” válaszokat vizsgáltam. A vizsgálatom eredményeképpen az alábbi eloszlást tapasztaltam. A „Védendő” kategória esetében látható, hogy a legnagyobb arányban (36%) nincs szüksége informatikai ismeretekre a munkájában, míg minimális ismeretre 41%, közepesre 23%, magasra nincs senkinek szüksége. A „Veszélyes” felhasználók esetében nincs szükség informatikai ismeretre a munkájához 24%, minimálisra 40%, közepesre 35%, míg magasra 2% felhasználónak van csak szüksége. A „Szerény” csoport felhasználói számára nincs szükség informatikai ismeretre 23%-nak, minimálisra 34%-nak, közepesre 43% felhasználónak van szüksége, míg magas szintű senkinek sem kell. A „Magabiztos” felhasználók esetében nincs szükség informatikai ismeretre a munkájához 13%-nak, minimálisra 18%-nak, közepesre 40%-nak, magasra 29% felhasználónak van szüksége. A vizsgálat eredménye kimutatta, hogy a legnagyobb számban a „Magabiztos” felhasználóknak van szükségük informatikai ismeretre, ami a korábbi feltételezésemet is alátámasztja, miszerint ezek a felhasználók foglalkozás-szerűen használják az informatikai ismereteiket. Látható, hogy minimális ismeretre a legnagyobb arányban a „Veszélyes” és a „Szerény” felhasználóknak van szükségük [75][161].

4.4.4 Összegzés

A fenti eredmények alapján látható, hogy a négy felhasználói csoport közül a „Védendő” az amelyiknek a munkavégzéshez a legalacsonyabb szintű informatikai ismeretek is elégségesek, valamint az informatikai tanfolyamon való részvételi motiváltságuk is a legalacsonyabb,

viszont ennek a csoportnak a tagjai vettek részt a legnagyobb számban már biztonsági oktatáson.

A „Szerény” felhasználók esetében látható, hogy a munkájukhoz már az előző csoportnál magasabb számban szükséges az informatikai ismeret, és motiváltságban is ezt a csoportot előzi meg az informatikai oktatáson való részvétel esetében, szintén a második legtöbb számban vettek részt biztonsági oktatáson.

A „Veszélyes” csoport tagjai esetében megfigyelhető, hogy a munkájukhoz a második legnagyobb arányban szükséges az informatikai ismeret motiváltságuk is ehhez mérhetően a második legmagasabb arányú, valamint ez a csoport vett részt a legkevesebb számban biztonsági oktatáson.

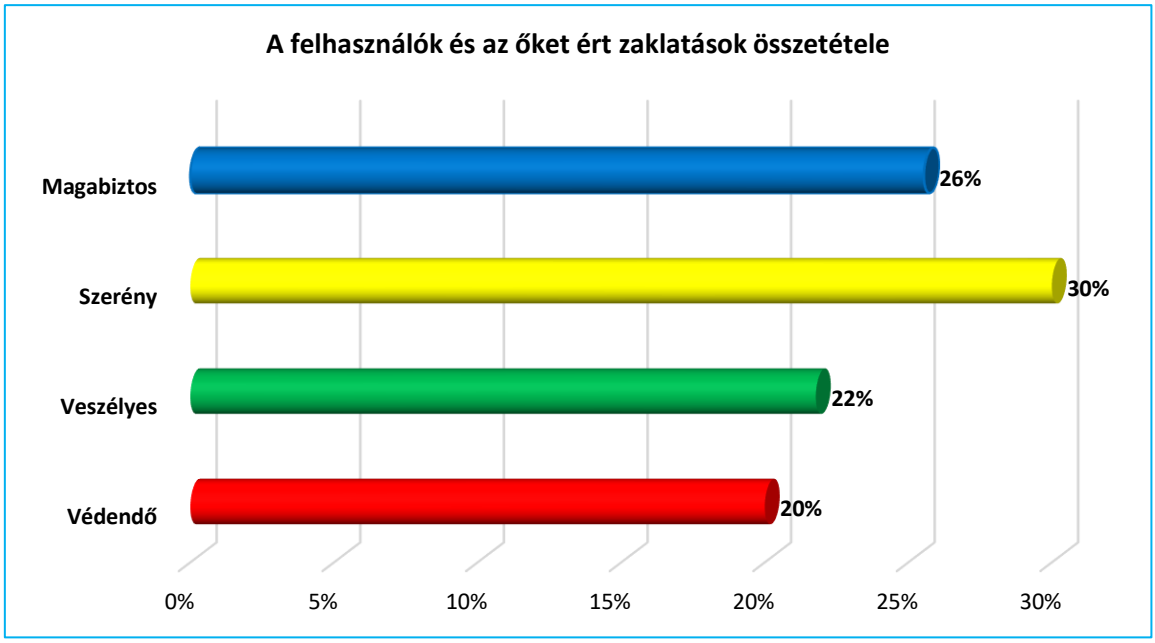
A „Magabiztos” csoport az, akiknek van valamilyen szintű informatikai ismerete, és a válaszok alapján a munkavégzéshez nélkülözhetetlen az ilyen irányú ismeret. Ők a legnagyobb számban motiváltak egy esetleges informatikai oktatáson való részvétel vonatkozásában, viszont ez a csoport vett rész a második legkisebb számban biztonsági képzésen.

4.5 A felhasználók zaklatásának és az erre adott reakcióiknak a vizsgálata

Az alábbiakban a felmérésem kérdései alapján azt vizsgáltam, hogy a felhasználó az általam definiált csoportok szerinti felosztásban esett-e már áldozatául zaklatásnak, egy esetleges zaklatás milyen válaszreakciót váltana ki belőle, valamint amennyiben zaklatták már, abban az esetben mit tett [76][170].

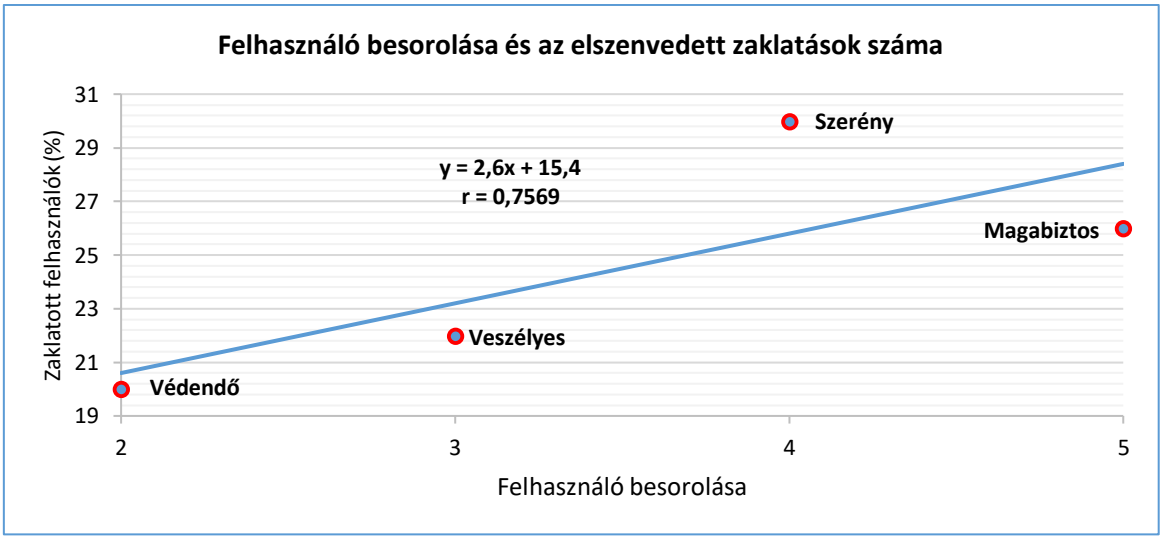
4.5.1 A felhasználói csoportok és az őket ért zaklatások eloszlása

Az alábbi vizsgálat a felhasználói csoportokban az internetes zaklatás – Cyberbulling előfordulásának felmérésére irányul. Akik kérdőíves felmérésem azon kérdésére, hogy „Zaklatták már közösségi oldalon (pl. Facebook), vagy e-mail-ben Önt, vagy hozzátartozóját (barátját)?” azt a választ adták, hogy „Igen, Önt.” és „Igen, a hozzátartozóját/barátját.”, azok a négy felhasználói csoportban az alábbiak szerint válaszoltak (47. ábra). Látható a kiértékelésből, hogy a „Veszélyes” csoport tagjainak vagy hozzátartozójának/barátjának 22%-át zaklatták már. A „Magabiztos” csoport tagjai esetében már kissé rosszabb eredményt (26%) mutat a vizsgálat. A „Védendő” csoport tagjait már 20%-ban érte internetes zaklatás. A legnagyobb arányban a „Szerény” csoport válaszai esetében mutatkozott az internetes zaklatás (30%).



47. ábra A felhasználók és az őket ért zaklatások összetétele (forrás: saját kérdőíves felmérés; készítette a szerző)

Látható, hogy azokat a felhasználói csoportokat érte magasabb számban internetes zaklatás, akik magasabb informatikai ismerettel, informatikai végzettséggel rendelkeznek (48. ábra). A felhasználói besorolás és a zaklatás közötti korreláció erősnek tekinthető (|r|= 0,7569). A magasabb kompetencia szintű felhasználót nagyobb számban éri zaklatás, mint az alacsony szintűt. A 48. ábrán látszik, hogy a lineárisra a „Szerény" besorolású felhasználó kevésbé illeszkedik, mint a másik három csoport. Azt gondolom, hogy a magasabb szintű felhasználók több és nagyobb számban látogatnak olyan közösségi oldalakat, ahol a zaklatás előfordulhat.



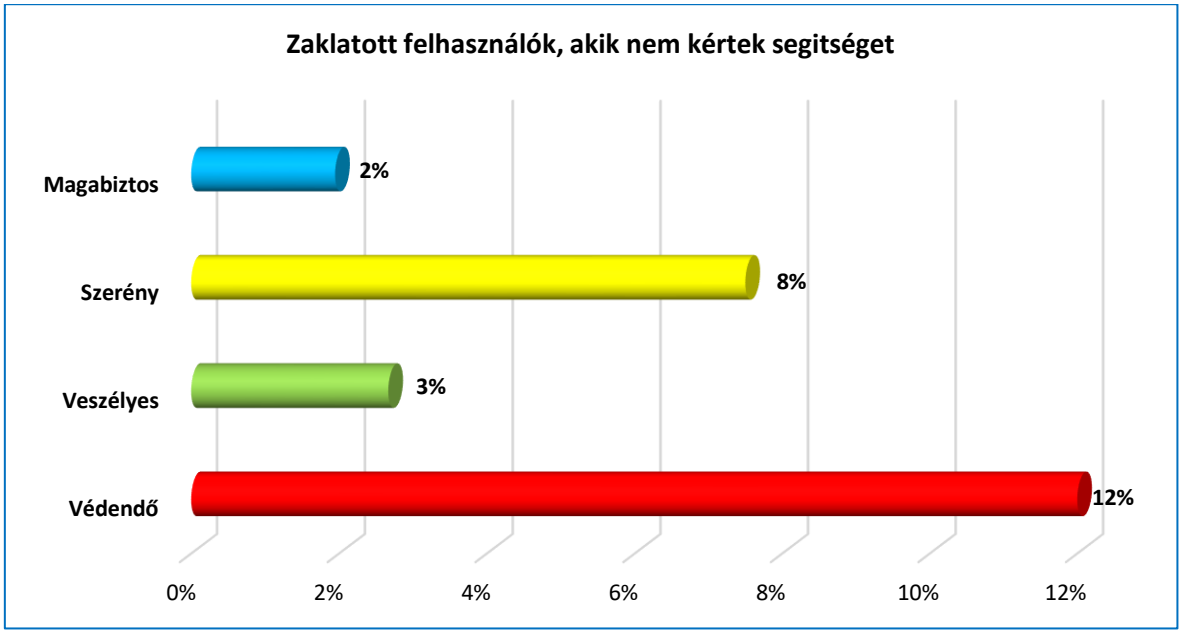
48. ábra A felhasználók és az őket ért zaklatások közötti korreláció (forrás: saját kérdőíves felmérés; készítette a szerző)

Akik alacsonyabb informatikai ismeretekkel rendelkeznek, azoknál alacsonyabb ez az arány. Azt gondolom, hogy ezek a felhasználók kisebb számban használják az előbb említett oldalakat.

A vizsgálat eredményeképpen látható, hogy az egyre nagyobb számban előforduló internetes zaklatás, a cyberbulling, azokat a felhasználókat éri nagyobb arányban, akik magasabb szintű informatikai ismeretekkel rendelkeznek [170]. Azonban az is előfordulhat, hogy a zaklatások száma azonos a különböző felhasználói csoportok esetében, de a magasabb kompetencia szintű felhasználók felismerték a zaklatást, míg az alacsonyabb kompetencia szintűek nem. Ez is azt bizonyítja, hogy amennyiben magasabb a digitális kompetencia szintje a felhasználóknak, abban az esetben könnyebben felismerik az ilyen jellegű tevékenységet.

4.5.2 A segítséget nem kérő internetes zaklatást elszenvedők vizsgálata

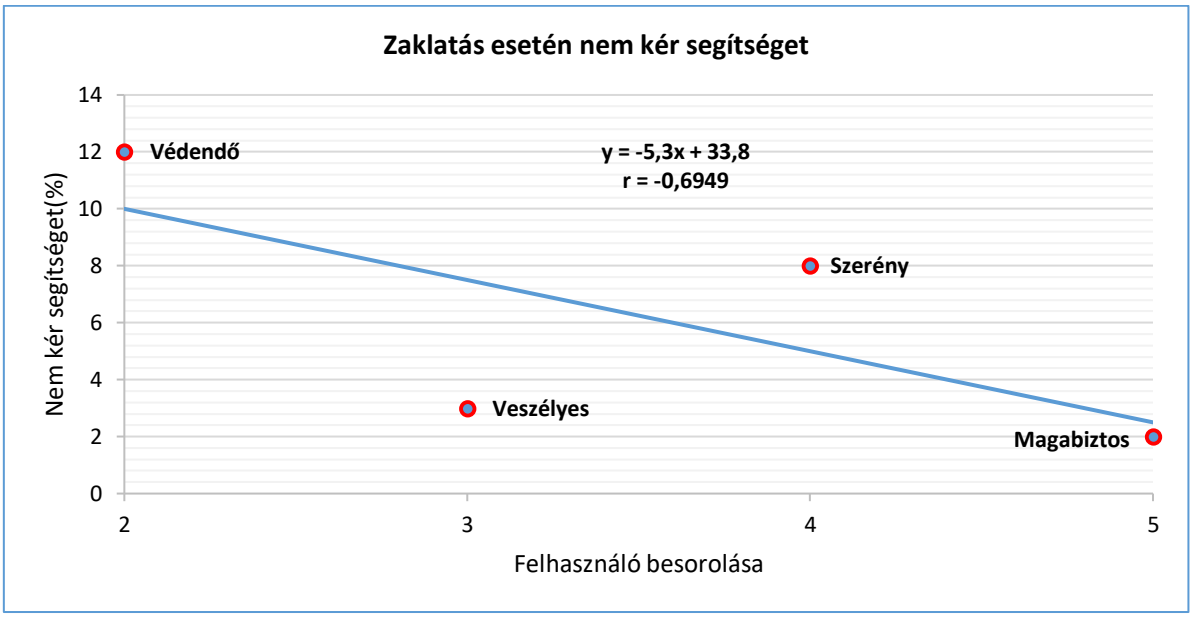
Az alábbiakban a kérdőíves felmérésem alapján azt vizsgálom, hogyan alakult azon felhasználók aránya, akiket ért internetes zaklatás – cyberbulling és nem tettek semmit ez ellen (49. ábra).



49. ábra A segítséget nem kérő, internetes zaklatást elszenvedők eloszlásának vizsgálata (forrás: saját kérdőíves felmérés; készítette a szerző)

Azokat a felhasználókat vizsgáltam, akik a kérdőívemben a „Zaklatták már közösségi oldalon (pl. Facebook), vagy e-mail-ben Önt, vagy hozzátartozóját (barátját)?” kérdésre az „Igen, Önt.” és az „Igen, a hozzátartozóját/barátját.” válaszokat adták, valamint a „Mit tenne, ha zaklatnák Önt vagy hozzátartozóját, vagy mit tanácsolna ilyen esetben?” kérdésre a „Tudomást se vesz róla” választ adták. Az általam előre definiált felhasználói csoportok esetében a „Magabiztos” csoportnál a fenti 2%-os értéket mértem. A „Veszélyes” csoport tagjai esetében adódott a második legkisebb érték, ami 3% volt. A „Szerény” felhasználók esetében látható, hogy a második legnagyobb a mért érték, ami 8% volt. A „Védendő” csoport felhasználóinak válaszai

esetében 12% ilyen felhasználó volt (50. ábra). A felhasználó besorolása és az internetes zaklatásra történő reagálása, vagyis “nem kér segítséget” között közepes erősségű korreláció mutatható ki (|r|= 0.6949). Tehát van kapcsolat a besorolási szint és zaklatásra adott felhasználói viselkedés között, de ez nem egyértelműen lineáris kapcsolat. Az jól látszik, hogy a „Védendő” és a „Szerény” magasabb számban nem kér segítséget, mint a „Veszélyes” és a „Magabiztos”, az 50. ábrán a lineáristól való negatív, illetve pozitív eltérés is ezt mutatja.



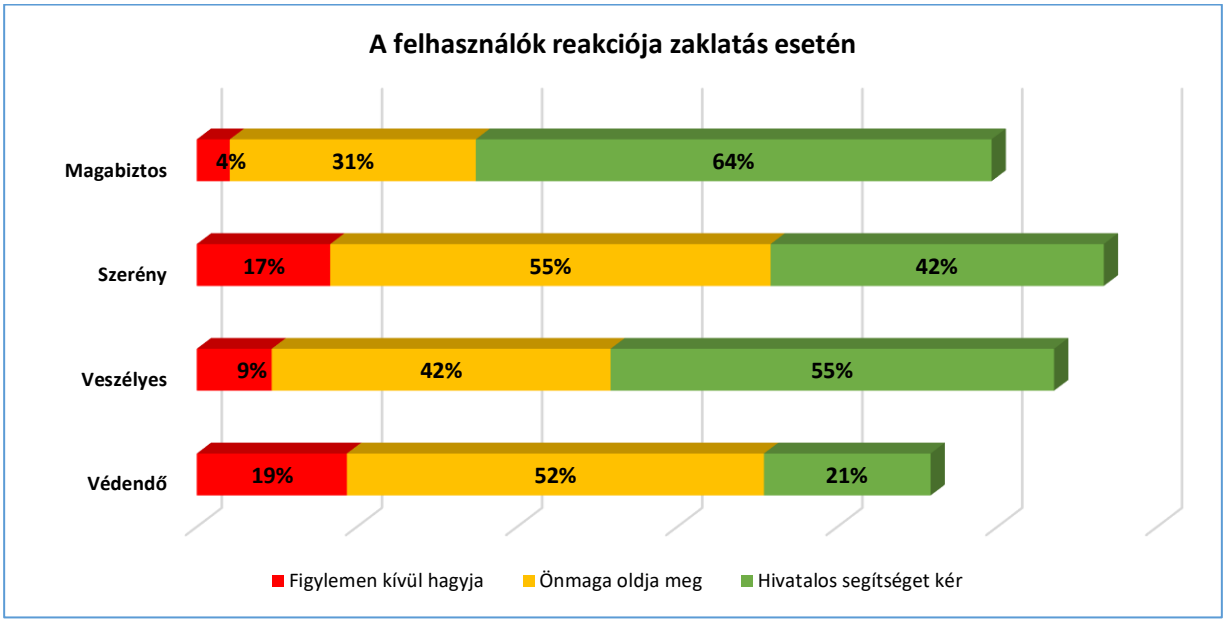
50. ábra A segítséget nem kérő internetes zaklatást elszenvedők eloszlásának vizsgálata (forrás: saját kérdőíves felmérés; készítette a szerző)

A korrelációs együttható negatív értéke arra utal, hogy minél magasabb a felhasználó besorolása annál kevésbé kér segítséget. A felmérés eredménye szintén alátámasztja azt a feltételezésemet, hogy olyan csoportok esetében fordult elő a legmagasabb számban, hogy internetes zaklatás esetében nem tettek semmit, úgynevezett „struccpolitikát” folytattak, ahol alacsony a biztonságtudatosság. Továbbá jelentős emelkedés mutatható ki a vizsgálat eredményeiben az önmagát jónak értékelő és az önmagát alacsony biztonságtudatosságúnak értékelő csoportok között, ami szintén azt támasztja alá, hogy a digitális kompetenciát és a biztonságtudatosságot a felhasználók körében folyamatos oktatásokkal és képzésekkel növelni kell, vagy magas szinten kell tartani [170].

4.5.3 A felhasználók és az internetes zaklatás - cyberbulling esetén adott reakcióiknak a vizsgálata

Az alábbiakban a kérdőíves felmérésem eredménye alapján a felhasználói csoportok reakcióját vizsgálom (51. ábra). A felhasználói csoportok a kérdőívem azon kérdésére, hogy „Mit tenne, ha zaklatnák Önt vagy hozzátartozóját, vagy mit tanácsolna ilyen esetben?”, a „Letiltja a zaklató

profilját, e-mail-jét", az „Értesíti az oldal-, szolgáltató szakembereit a zaklatásról", az „Értesíti a hatóságokat, és gondoskodik a bizonyítékok védelméről", a „Felhívja a zaklató, vagy gyalázkodó figyelmét, hogy fejezze be azt", a „Segítséget kér szakembertől" és a „Tudomást se vesz róla" válaszokat jelölhették be. A válaszokat a jobb átláthatóság kedvéért, valamint a későbbiekben történő felhasználhatóság érdekében az alábbiak szerint csoportosítottam. Létrehoztam egy válaszcsoportot, aminek azt a nevet adtam, hogy „Hivatalos segítséget kér", ebbe a csoportba a „Értesíti az oldal-, szolgáltató szakembereit a zaklatásról", az „Értesíti a hatóságokat, és gondoskodik a bizonyítékok védelméről" válaszokat vettem figyelembe minden előfordulásukban. A következő válaszcsoportnak az „Önmaga oldja meg" elnevezést adtam és ebbe a csoportba a „Letiltja a zaklató profilját, e-mail-jét", a „Felhívja a zaklató, vagy gyalázkodó figyelmét, hogy fejezze be azt", a „Segítséget kér szakembertől" válaszokat vettem figyelembe, annak önálló vagy az ebbe a válaszcsoportba tartozó válaszokkal együtt történő előfordulása esetén. A harmadik válaszcsoport, ami csak egy válasz, a „Tudomást se vesz róla" kizárólagos előfordulásából állt, annak a „Figyelmen kívül hagyja" elnevezést adtam.



51. ábra A felhasználói csoportok reakciója a z internetes zaklatás esetén (forrás: saját kérdőíves felmérés; készítette a szerző)

Az alábbiakban látható, hogy a „Hivatalos segítséget kér" válaszcsoportba tartozó válaszokat a „Magabiztos" csoport válaszadói a legnagyobb számban (64%), míg a legkevesebb számban (21%) a „Védendő" csoport tagjai adták. Itt is megfigyelhető, hogy a két csoport a végzettség és önértékelési eredmények alapján, egymás pontos ellentétei. Az „Önmaga oldja meg" válaszcsoportba tartozó válaszokat a „Szerény" csoport tagjai a legnagyobb számban (55%), míg a legkevesebb számban (31%) a „Magabiztos" csoport tagjai adták, ami jól jellemzi a két

csoport biztonságtudatosságát. A „Figyelmen kívül hagyja” válaszcsaládba tartozó válasz a legnagyobb számban (19%) a „Védendő” csoport tagjai esetében fordult elő, míg a legkevesebb számban (4%) a „Magabiztos” csoport tagjai esetében érkezett. Ebben a vonatkozásban is látható a két felhasználói csoport fentebb említett ellentéte. Ennek a vizsgálatnak az eredményeképpen megállapítható, hogy a saját biztonságtudatossági szintjüket és a digitális kompetenciájukat alacsonynak ítélő felhasználók esetében fordul elő a legnagyobb számban, hogy maguk akarják megoldani a jelentkező problémát, avagy figyelmen kívül hagyják a zaklatást, ami szintén nem vezet a probléma felszámolásához és a zaklató esetleges felelősségre vonásához. A zaklatásnak a saját maguk által történő felszámolása természetesen egy előzetes, tűzoltó jellegű tevékenységnek elfogadható, de mindenképpen ki kell egészülnie a hivatalos szervek vagy szolgáltató felé irányuló segítségkéréssel is. Továbbá megállapítható, hogy azon felhasználók esetében fordul elő a legmagasabb számban a szakemberek által is javasolt hivatalos segítségkérés, akik magasnak vallották a biztonságtudatossági szintjüket és a digitális kompetenciájukat. Ennek a vizsgálatnak az eredménye is alátámasztja azt, hogy a felhasználók biztonságtudatossági szintjét oktatásokkal/képzésekkel folyamatosan emelni szükséges [170].

4.5.4 Összegzés

Az internetes zaklatás, azaz a cyberbulling napjaink egyik fontos problémája, amivel foglalkozni kell a szakmának és a társadalomnak egyaránt. A bemutatott felmérések eredményei alapján kijelenthető, hogy abban az esetben, ha alacsony a felhasználó biztonságtudatossága, akkor magas az előforduló internetes zaklatások száma. Továbbá az is kijelenthető, hogy azoknak a felhasználóknak az esetében fordul elő a legnagyobb számban, hogy maguk akarják megoldani a jelentkező problémát, avagy figyelmen kívül hagyják a zaklatást, akiknek alacsony a biztonságtudatossági szintjük és a digitális kompetenciájuk. Javaslom egy digitális segélyhívó rendszer kialakítását, hogy azok a felhasználók, akiket zaklatás ér a kibertérben, késedelem nélkül, akár egy gombnyomásra olyan szakember segítségét tudja kérni, aki erre a feladatra specializálódott [170].

4.6 Összefoglalás

Az általam összeállított és végrehajtott kérdőíves felmérés eredményeinek kiértékelése során igazolom a hipotéziseimet. Kutatásom eredményeként megállapítom, hogy a válaszadók döntő többsége folyamatosan használja az internetet. Ez a felismerés alátámasztja azt a hipotézisemet, hogy a teljes társadalomra érvényes besorolást kell alkalmazni.

Megállapítom, hogy a felhasználók digitális kompetencia és biztonságtudatossági szintje jelentős eltérést mutat a lakóhely és az életkor függvényében. Kijelentem, hogy a lakosság digitális jóléte, biztonságos internethasználatának szintje képzéssel növelhető. Továbbá megállapítom, hogy a vizsgált fiatalabb korosztályok (18-24, 25-34) digitális kompetenciaszintje magasabb, mint a vizsgált idősebb korosztályoké (35-50, 51+). Ezzel szemben az idősebb korosztály rendelkezik magasabb biztonságtudatossággal.

Bizonyítást nyert, hogy a felhasználók besorolását helyesen végeztem el, a kibertérben mutatott viselkedésük alapján és megállapítom, hogy kérdőívem kérdései, mint módszer- és viselkedésspecifikus szempontrendszer, és az abból kinyert válaszok szerint a felhasználók digitális kompetencia és biztonságtudatosság szempontjából besorolhatók azokba a felhasználói csoportokba, amelyeket definiáltam. Olyan módszer- és viselkedésspecifikus szempontrendszert állítottam fel, amely alkalmas a felhasználók kockázati célú értékelésére.

Megállapítom, hogy a felhasználói csoportokban a lakóhely és az életkor alapján a fiatal korosztályok aránya a domináns minden területen. A vizsgálat alapján jól feltérképezhető, hogy mely felhasználói csoportok életkor szerint hol élnek. Ez a biztonságtudatosság és a digitális kompetencia fejlesztéséhez szolgálhat olyan információval, hogy a társadalom mely rétegének képzésére, oktatására milyen módszert alkalmazva lehet fejleszteni a képességeket és készségeket. A „Védendő” csoport 22%-a adta azt a választ, hogy részt venne informatikai oktatáson, ami megegyezik a DJP-ben megállapítottakkal, azaz azon felhasználók, akik alacsony digitális képzettséggel rendelkeznek, elutasítóak a további tanulással szemben.

Megállapítom, hogy a „Védendő” felhasználói csoport munkavégzéséhez a legalacsonyabb szintű informatikai ismeretek is elégségesek. Az informatikai tanfolyamon való részvételi motiváltságuk is a legalacsonyabb, viszont ennek a csoportnak a tagjai vettek már részt a legnagyobb számban biztonsági oktatáson. Megállapítom, hogy a „Szerény” felhasználók munkájához magasabb számban szükséges az informatikai ismeret, motiváltságuk nagyobb az informatikai oktatáson való részvétel esetében, mint az előző csoporté, és a második legtöbb számban vettek részt biztonsági oktatáson. A „Veszélyes” csoport tagjai esetében megállapítom, hogy a munkájukhoz a második legnagyobb arányban szükséges az informatikai ismeret, motiváltságuk is ehhez mérhetően a második legmagasabb arányú, valamint ez a csoport vett rész a legkisebb arányban biztonsági oktatáson. Megállapítom, hogy a „Magabiztos” csoportnak van informatikai ismerete, és a válaszok alapján a munkavégzéséhez nélkülözhetetlen az ilyen irányú ismerete. Ők a legnagyobb számban motiváltak egy esetleges

informatikai oktatáson való részvétel esetében, viszont ez a csoport vett rész a második legkisebb számban biztonsági képzésen.

A zaklatás vizsgálata során megállapítom, hogy a legnagyobb arányban a „Szerény” csoportot érte internetes zaklatás. Ennél a csoportnál közel 15%-kal több az internetes zaklatás előfordulása a “Magabiztos” csoporttal szemben. A vizsgálat bebizonyította, hogy az egyre nagyobb számban előforduló internetes zaklatás, a cyberbulling azokat a felhasználókat éri nagyobb arányban, akik kevésbé biztonságtudatosak. Azok a felhasználók, akik alacsonynak vallották biztonságtudatossági szintjüket és digitális kompetenciájukat, azok esetében fordul elő a legnagyobb számban, hogy maguk akarják megoldani a jelentkező problémát, avagy figyelmen kívül hagyják a zaklatást. Továbbá megállapítom, hogy azon felhasználók esetében, akik magasnak vallották a biztonságtudatossági szintjüket és a digitális kompetenciájukat, azok a legnagyobb számban kértek hivatalos segítséget. A fejezetben bemutatott vizsgálataim eredménye is alátámasztja azt, hogy a felhasználók biztonságtudatossági szintjét oktatásokkal/képzésekkel folyamatosan emelni szükséges.

5 A FELHASZNÁLÓK MÓDSZER- ÉS VISELKEDÉSSPECIFIKUS VIZSGÁLATA

A felhasználók módszer- és viselkedésspecifikus vizsgálatát egy szempontrendszer szerint végeztem el, mely alkalmas a felhasználó kockázati szintje szerinti csoportosításra.

5.1 A felhasználók vírusvédelemi szokásainak vizsgálata

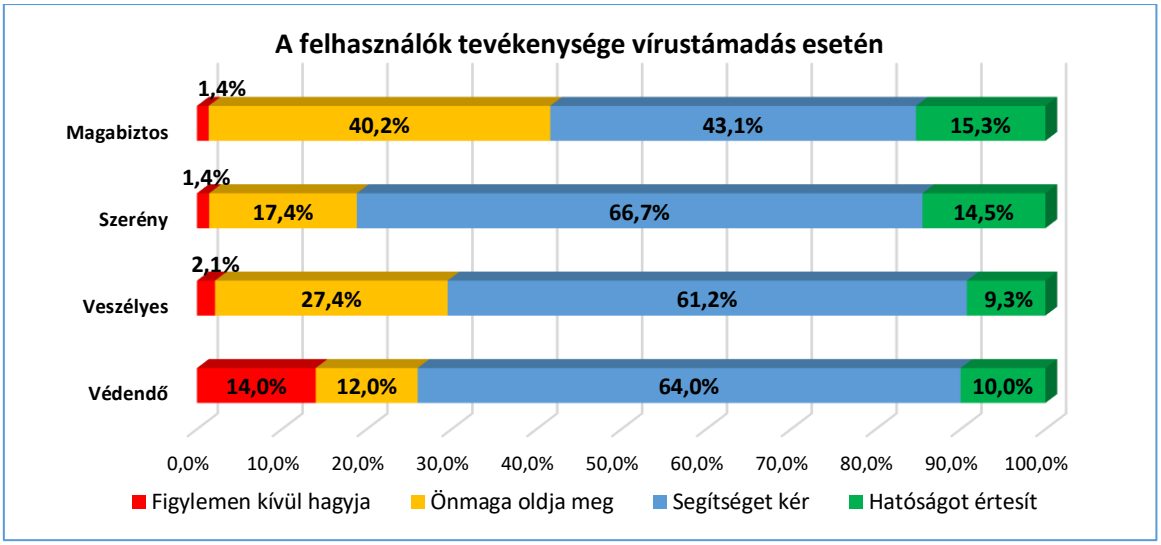
Az alábbi részben az általam korábban definiált négy felhasználói csoport vírusvédelemmel kapcsolatos szokásait vizsgálom különböző aspektusokból, mint például a vírusvédelmi alkalmazások használatának, valamint az esetlegesen elszenvedett vírustámadásoknak a négy felhasználói csoport közötti kapcsolatok vonatkozásában [77].

Az informatikai eszközeink egyik legfontosabb védelmi megoldása a vírusvédelem. A vírusvédelem alkalmazása minden informatikai eszközön kiemelten szükséges. Tévhit, hogy bizonyos operációs rendszerekhez nincs szükség vírusvédelemre, mondván, arra az operációs rendszerre nem készítenek rosszindulatú szoftvert. A hálózatok világában előfordulhat, hogy egy kártékony kódot tartalmazó levelet egy rezisztens gép továbbít egy olyan eszköznek, ami arra érzékeny, úgy, hogy a rezisztens nem is tudja, hogy vírusos tartalmat küldött. Speciális és szeparált célrendszerek esetében előfordulhat, hogy a vírusvédelmi alkalmazás nem közvetlenül a rendszerre van telepítve, hanem egy úgy nevezett „dirty pc”-n található [170].

5.1.1 A felhasználók tevékenységének vizsgálata vírustámadás esetén

Az alábbiakban kérdőíves felmérésem alapján a felhasználói csoportok tevékenységét vizsgálom egy esetleges vírustámadás esetén (52. ábra). Az általam előre definiált felhasználói csoportoknak a felmérésem „Esetleges vírustámadás, és/vagy egyéb rosszindulatú támadás esetén tisztában van azzal, hogy mi a teendő?” kérdésre adott válaszait elemeztem. Annak érdekében, hogy az elemzésem átlátható legyen és a későbbi munkámat segítse, négy válaszcsoportot alkottam. Az első válaszcsoportnak a „Figyelmen kívül hagyja”, a másodiknak az „Önmaga oldja meg”, a harmadiknak a „Segítséget kér”, a negyediknek a „Hatóságot értesíti” elnevezéseket adtam. Az első csoportba a „Nem tesz semmit” válasz került, a másodikba a „Megoldja egyedül”, a harmadikba az „Igen, szakember segítségét kéri.” és az „Igen, szól a hozzáértő ismerősének, hogy segítsen.”, a negyedikbe az „Igen, felméri a károkat, próbálja minimalizálni a kárt, értesíti a hatóságokat-, az üzemeltetőt.” válaszokat soroltam be. Látható, hogy a „Magabiztos” felhasználók (1,4%), a „Veszélyes” felhasználók (2,1%) és a „Szerény” felhasználók (1,4%) esetében nagyon alacsony számban fordul elő, hogy nem tennének semmit egy esetleges vírustámadás bekövetkeztekor. Magasabb számot

eredményezett a „Védendő” felhasználók (14%) tevékenységének elemzése az előbbi kérdéssel kapcsolatban. A „Magabiztos” felhasználók nagy számban (40,2%) oldanák meg egyedül az esetleges vírustámadással járó kárenyhítést. A „Veszélyes” felhasználók már az előző csoportnál kevesebb (27,4%), de még mindig jelentős számban enyhítenék önállóan a károkat. A „Szerény” csoport (17,4%) és a „Védendő” csoport (12%) kis hányada oldaná meg egyedül ezt a feladatot. Vírustámadás esetén a „Szerény” felhasználók kérnének a legnagyobb számban (66,4%) segítséget, amit a „Védendő” (64%) és a „Veszélyes” (61.2%) csoportok követnek. A „Magabiztos” csoport esetében a meglévő szakértelem indokolja a 43,1%-os eredményt. A „Hatóságot értesíti” válaszcsoport eredményének elemzése során a legmagasabb értéket a „Magabiztos” csoport (15,3%) érte el, amit a „Védendő” csoport (10%) és a „Szerény” csoport (14,5%) követ. A legalacsonyabb értéket az előbbi válaszcsoportban a „Veszélyes” csoport (9,3%) mutatta.



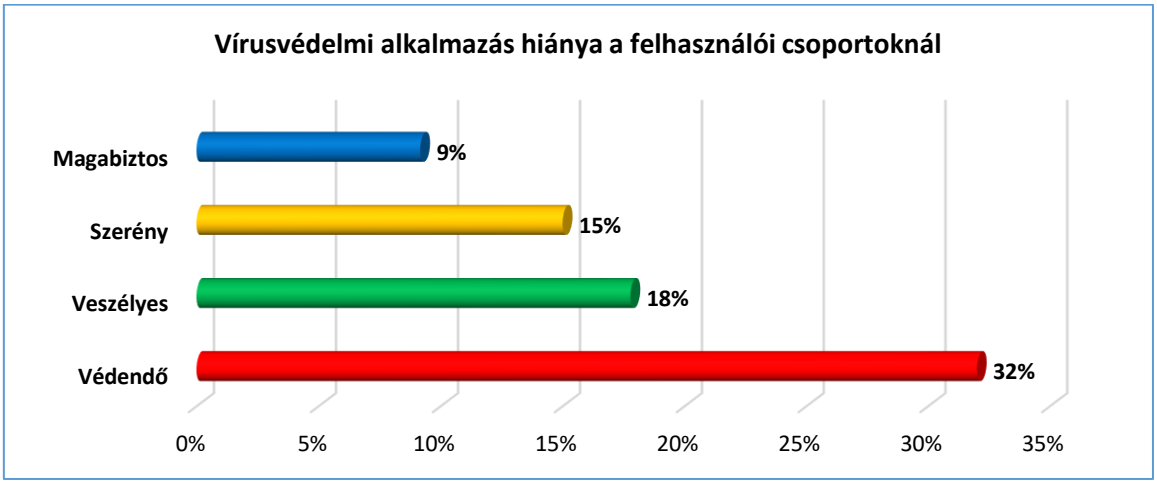
52. ábra A felhasználók tevékenységének vizsgálata vírustámadás esetén (forrás: saját kérdőíves felmérés; készítette a szerző)

A felmérésem alapján megállapítható, hogy a felhasználók a biztonságtudatosságuknak és a digitális kompetenciájuknak, valamint az informatikai ismereteiknek megfelelően tevékenykednének esetleges vírustámadás esetén. Míg az önmaga által végrehajtott kármentés a „Magabiztos” csoport esetében a tudásszintjük miatt érthetően magas, addig ugyanez aggasztó és ezáltal kockázatos a „Veszélyes” csoport esetében, akik nem rendelkeznek semmilyen informatikai végzettséggel. Pozitívan értékelendő, hogy a felhasználók nagy számban valamilyen segítséget kérnének szakemberektől, azonban negatív viselkedésnek tekinthető, hogy a hatóságokat az esetleges víruseszkalálódás megelőzése érdekében csak kevés

számban értesítenék. Szintén negatívan értékelendő, hogy a „Védendő” csoport 14%-a nem tenne semmit vírustámadás esetén [78].

5.1.2 Kapcsolat a felhasználó besorolása és a vírusvédelem között

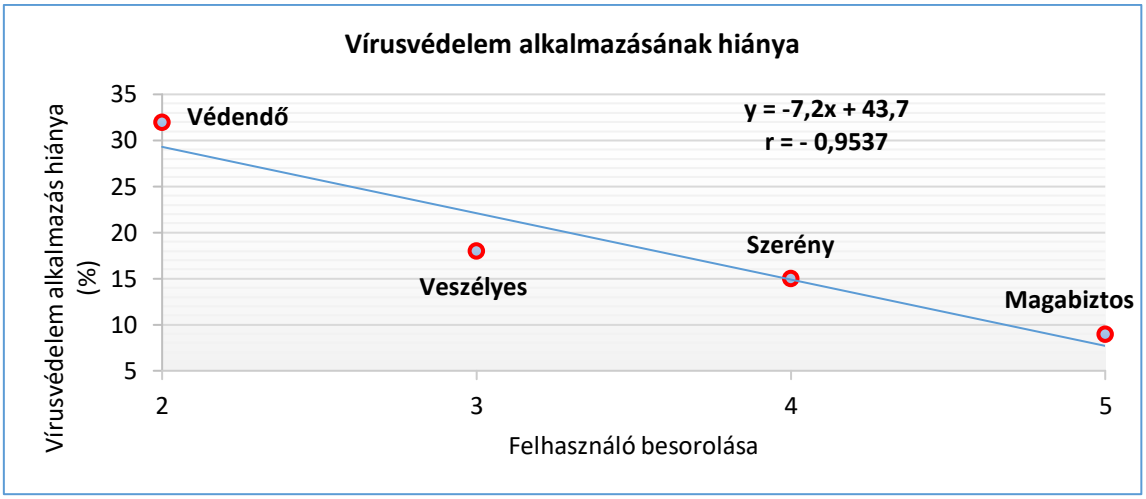
Az alábbi részben a felhasználó besorolása, valamint a vírusvédelem alkalmazásának hiánya között kerestem kapcsolatot. A korábban általam definiált négy felhasználói csoport vírusvédelmének helyzetét vizsgálva arra az eredményre jutottam, hogy a különböző felhasználói csoportok nagyon eltérő módon alkalmazzák a vírusvédelmi megoldásokat. Jól látható, hogy a „Védendő” csoportba tartozók körében kiugróan magas, 32% a vírusvédelmi alkalmazások hiánya. A „Veszélyes” (18%) és a „Szerény” (15%) csoportok körében már alacsonyabb az aránya azoknak, akik nem rendelkeznek vírusvédelmi alkalmazásokkal. A „Magabiztos” csoport tagjai esetében magasnak mondható a 9%-os eredmény, mivel az ebbe a csoportba tartozók magasnak mondták a kompetenciaszintjüket és a tudatosságukat, valamint ezen csoport tagjainak mindegyike rendelkezik valamilyen informatikai végzettséggel.



53. ábra A felhasználó besorolása és a vírusvédelem alkalmazás hiányának rangsora (forrás: saját kérdőíves felmérés; készítette a szerző)

Az eredményből jól látszik (53. ábra), hogy a felhasználók mindegyik csoportja esetében szükséges a folyamatos és/vagy ismétlődő jellegű biztonságtudatossági képzés a magasfokú biztonság elérése, megtartása érdekében [79]. A korrelációs együttható abszolút értéke jó egyezést mutat a lineárishoz (|r|=0,9537), mivel a korreláció előjele negatív, ebből látszik, hogy a felhasználó egyre magasabb besorolási értéke szerint egyre alacsonyabb a vírusvédelem hiánya, az ebből kiszámított determinációs együttható pedig 90,95%, mely azt mutatja, hogy az értékek jól illeszkednek a lineáris függvényre, tehát közöttük erős kapcsolat van (54. ábra). A kutatási eredményeim alapján megállapítom, hogy a vírusvédelem alkalmazása és a felhasználó

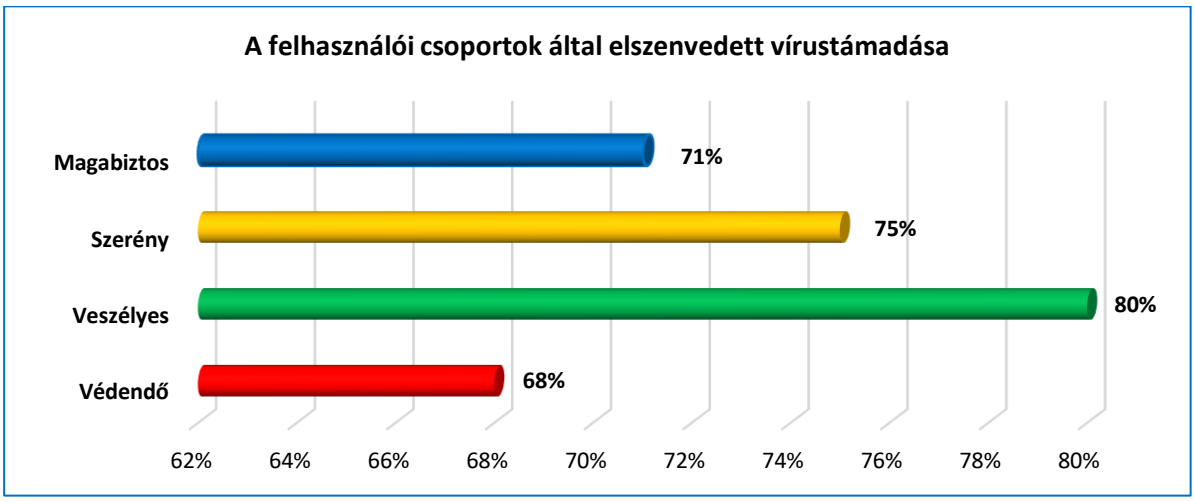
besorolási szintje közötti kapcsolat közel lineáris, tehát a magasabb képzettségű felhasználók nagyobb számban alkalmaznak vírusvédelmet.



54. ábra A felhasználó besorolása és a vírusvédelem alkalmazásának hiánya közötti korreláció (forrás: saját kérdőíves felmérés; készítette a szerző)

5.1.3 Kapcsolat a felhasználó besorolása és a vírustámadások között

Az alábbi korreláció vizsgálatát azért végeztem el, mert kerestem az összefüggést a biztonságtudatossággal és a digitális kompetenciával kapcsolatos felhasználói besorolás, valamint az informatikai ismeretek és a vírustámadások előfordulása között (55. ábra).

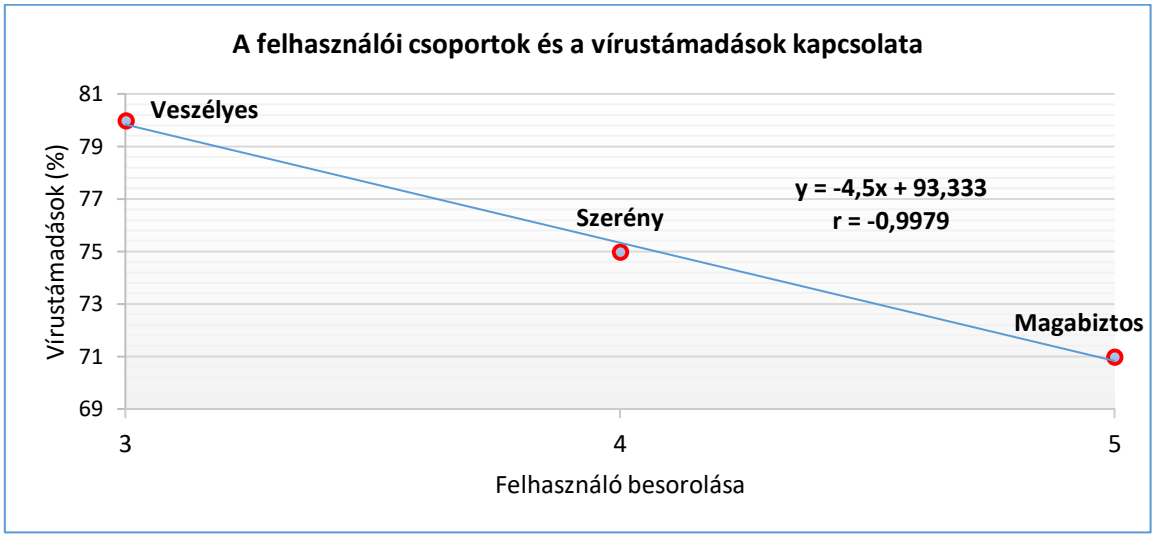


55. ábra Kapcsolat a felhasználó besorolása és a vírustámadások között (forrás: saját kérdőíves felmérés; készítette a szerző)

Az általam definiált felhasználói csoportoknál a vírustámadások előfordulását vettem alapul az „Érte már vírus-, és/vagy egyéb rosszindulatú támadás az Ön eszközét/eszközeit?” kérdés esetében. Az értékelés során a válaszok közül az „Igen” mellett a „Nem tud róla” válaszokat vettem figyelembe, vélelmezve, hogy ha nem tudja, attól még előfordulhatott. Jól látható, hogy mind a négy kategória esetében magas a vélt vagy valós vírustámadások száma. A „Védendő”

kategóriát érte a legkevesebb támadás (68%). Ők alacsony tudatossággal és képességgel rendelkeznek, valamint nincs informatikai végzettségük. Kevés (71%) támadás érte a „Magabiztos” kategória tagjait, ugyanis ez a kategória az, ahol a válaszadók jó kompetencia és tudatossági szintűre értékelték magukat, és rendelkeznek informatikai ismeretekkel is. Valószínűsítem, hogy ezek a felhasználók már bátrabban használják az internetet és olyan veszélyes tartalmakat is látogatnak, amelyhez egy átlag felhasználónak nem lenne bátorsága. A „Szerény” kategóriába tartozókat érte a második legtöbb (75%) vélt vagy valós vírustámadás. Ők alacsony tudatosságot és képességet jelöltek meg, viszont rendelkeznek valamilyen informatikai végzettséggel vagy oktatással. Ebben az esetben jól látszik, hogy az alacsonynak vallott biztonságtudatossági szint milyen veszélyeket hordoz magában. A „Veszélyes” csoport tagjai esetében a legmagasabb a vírustámadás elfordulása (80%). Erre a csoportra jellemző a felfedező hajlam, és ezáltal, tapasztalataik és a blogbejegyzések alapján felbátorodva tesznek veszélyes manővereket az interneten. A viselkedésük kockázatosnak mondható [163].

Az alábbi korreláció is rávilágít arra, hogy nem elegendő az egyszer megszerzett informatikai ismeret, hanem azt rendszeresen, kiemelt hangsúlyt helyezve a biztonságtudatosság növelésére, kell ismételten feleleveníteni [80]. A felhasználó a digitális rendszer szempontjából kockázatot jelent, az elszenvedett vírustámadások szerint a kockázati szint fordítottan arányos a felhasználó besorolási szintjével (56. ábra).



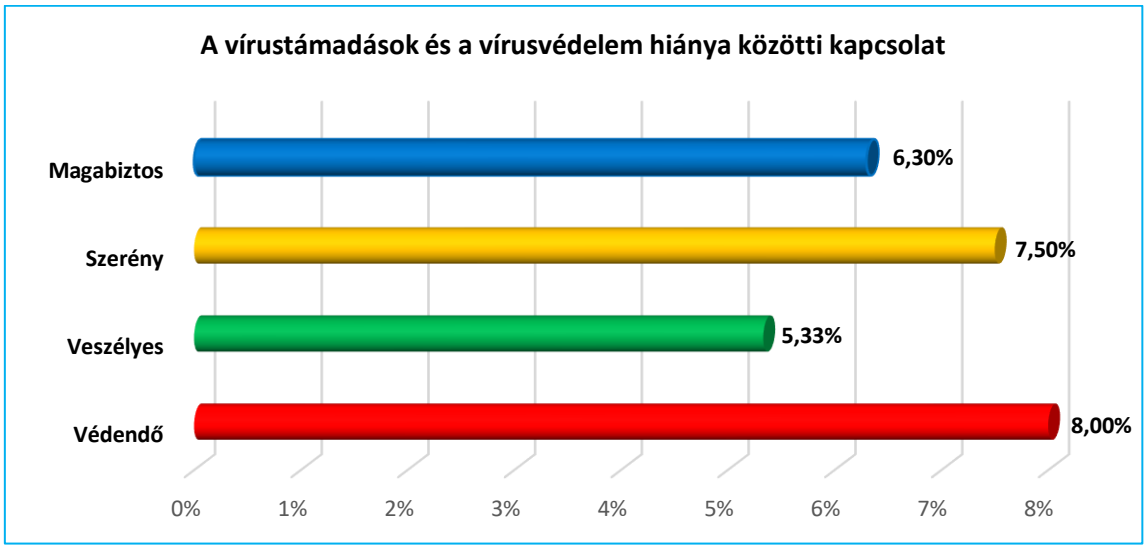
56. ábra Korreláció a felhasználó besorolása és a vírustámadások között (forrás: saját kérdőíves felmérés; készítette a szerző)

A 56. ábra alapján látható, hogy csak három csoport adatait értékeltem. A “Védendő” csoport eredményét kizártam, mivel nem egyértelmű, hogy a felhasználók kompetenciájukból adódóan képesek voltak minden vírustámadást felismerni, ezért a válaszok eredményei ebben a

korrelációban nem használhatók. Tehát az 56. ábra alaján a másik három csoport eredményeit értékeltem, a pontok lineárisra illeszkedése igen jó közelítéssel valósul meg, a korrelációs együttható |r|= 0,9979, mely fordított arányt mutat az elszenvedett vírustámadások száma és a besorolási szint között, a determinációs együttható pedig d=99,58%, ami a kapcsolat erősségét mutatja. A felhasználó besorolása és a vírustámadások közötti kapcsolat erős, erősebb, mint a felhasználó besorolása és a vírusvédelem alkalmazás hiánya közötti.

5.1.4 Kapcsolat a vírustámadások és a vírusvédelmi alkalmazások hiánya között

Az alábbi vizsgálatot annak érdekében végeztem el, hogy bemutassam a kapcsolatot a vírustámadások előfordulása és a vírusvédelem hiánya között.

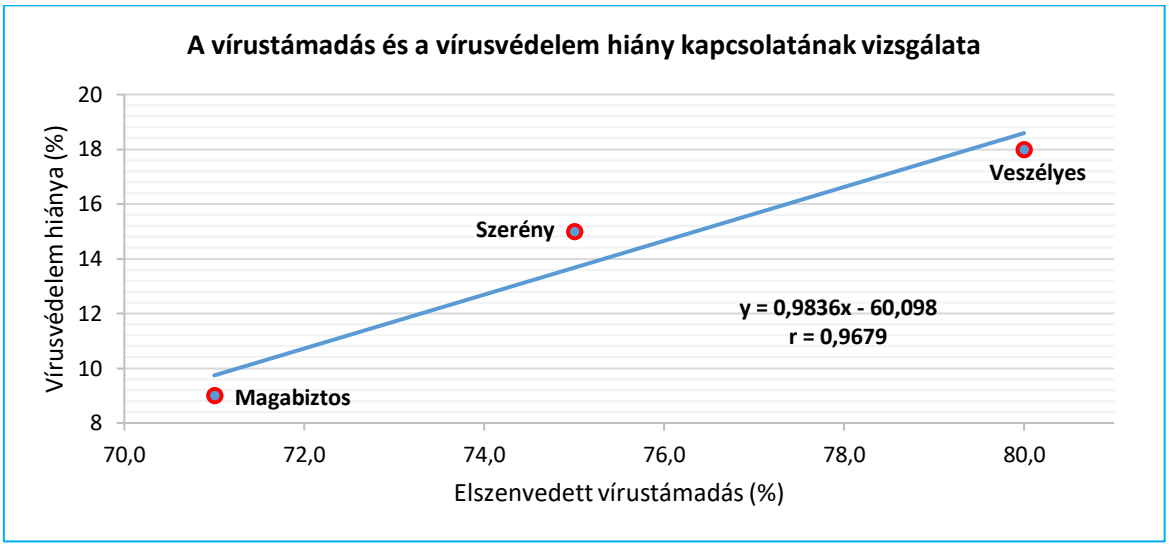


57. ábra Kapcsolat a vírustámadások és a vírusvédelem hiánya között (forrás: saját kérdőíves felmérés; készítette a szerző)

Jól látható (57. ábra), hogy a legmagasabb arány (8%) a „Védendő” csoport tagjai körében mutatható ki, ezt követi a „Szerény” csoport aránya (7,5%). Majd a második legalacsonyabb eredményt (6,3%) a „Magabiztos” csoport érte el. A legalacsonyabb eredményt (5,33%) a „Veszélyes” csoport produkálta. Összességében az látható, hogy nincs nagy eltérés a négy csoport értékelése között. A lefolytatott vizsgálat során kapott eredmények értékei között mindössze 2,67 százalékpont a különbség, amely nem mutat nagy eltérést [81].

Nem derül ki a „Védendő” felhasználói csoport kutatási eredményeiből, hogy hány felhasználót ért „lappangó” vírustámadás, melyről a felhasználó nem is tud, hiszen nem alkalmaz megfelelő vírusvédelmet, csak lassul a számítógépe, vagy csak később derül ki, hogy vírusfertőzés érte. Ezért ahogyan a 4.2.2 alfejezetben indokoltam, ezt a csoportot ebben az esetben is kizártam a korrelációs vizsgálatból. Látszik (58. ábra), hogy a vírusvédelem hiánya és a vírustámadások száma között erős korreláció van, |r|= 0,9679. Megállapítom az eredmények alapján, hogy

amennyiben a felhasználó nem használ vírusvédelmet, abban az esetben vírustámadás éri. A vírusvédelem hiánya fordítottan arányos a felhasználónak a szempontrendszer szerinti szintjével, valamint a vírusvédelem hiánya és a vírustámadások előfordulása között kutatási eredményeim alapján lineáris kapcsolatot mutattam ki [170].



58. ábra A vírustámadás és a vírusvédelem hiány kapcsolatának korrelációs vizsgálata (forrás: saját kérdőíves felmérés; készítette a szerző)

5.1.5 Összegzés

Az informatikai eszközeink vírusvédelmének kérdése kiemelten fontos. Ezért a vírusvédelmi megoldások hatékony használata nem csak a felhasználó egyéni érdeke, hanem mindenkié, aki az adott hálózat vagy rendszer részét képezi. A felmérésem alapján megállapítom, hogy a felhasználók az általam definiált szempontrendszernek megfelelően tevékenykednének esetleges vírustámadás esetén. Pozitívan értékelendő, hogy a felhasználók jelentős része kér segítséget szakemberektől, negatívan értékelendő, hogy kis számban értesítik a hatóságokat a tömeges vírusfertőzés megelőzése érdekében. Bizonyítottam, hogy a felhasználók besorolási értékének növekedésével fordítottan arányos a vírusvédelem hiánya, a kapott értékek jól illeszkednek a lineáris függvényre, tehát közöttük erős kapcsolat van [170].

Megállapítom, hogy a „Veszélyes” felhasználóknál a legmagasabb a vírustámadás elfordulása, mert vakmerően veszélyes manővereket tesznek az interneten, így a viselkedésük (nem kiszámítható) kockázatos. Továbbá a felhasználó besorolása és a vírustámadások közötti kapcsolat erősebb, mint a felhasználó besorolása és a vírusvédelem alkalmazás hiánya közötti. Valamint, hogy a kockázati szint fordítottan arányos a felhasználó besorolási szintjével.

Megállapítom, hogy ha a felhasználó nem használ vírusvédelmet, akkor vírustámadás éri. A vírusvédelem hiánya fordítottan arányos a felhasználónak a szempontrendszer szerinti

szintjével, és a vírusvédelem hiánya és a vírustámadások előfordulása között kutatási eredményeim alapján lineáris kapcsolatot mutattam ki.

Javaslom egy olyan digitális segélyhívó rendszer kialakítását, amely azoknak a felhasználóknak nyújtana segítséget, akik digitális kompetenciájukat tekintve alacsonyabb kategóriába tartoznak. Részükre tud segítséget nyújtani abban az esetben egy mesterséges intelligencia vagy kezelő személyzet, ha vírustámadás éri a felhasználó eszközét, rendszerét. Ez a segélyhívó rendszer egy gombnyomásra aktivizálódik és távoli segítségnyújtással a szakképzett személyzet késedelem nélkül beavatkozik a felhasználó rendszerének védelmében [170].

5.2 A felhasználók biztonsági adatmentésének és adatvesztésének vizsgálata

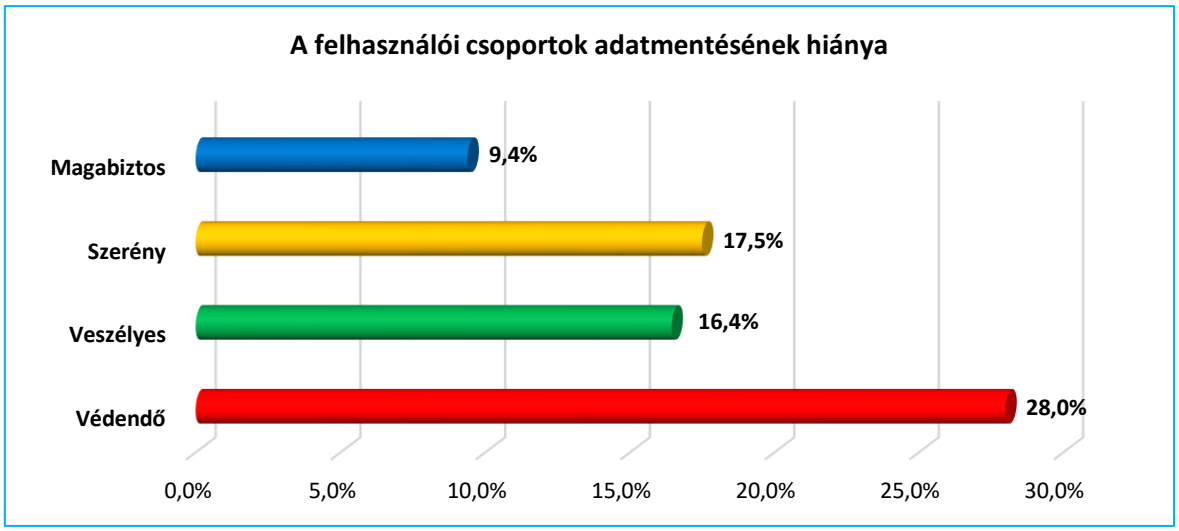
Az általam lefolytatott kérdőíves felmérés eredményeit elemezve a felhasználók biztonsági adatmentésének és az elszenvedett adatvesztésének összefüggéseit vizsgálom a már korábban általam definiált, négy felhasználói csoport tekintetében. Összefüggést keresek a felhasználók biztonságtudatossági és digitális kompetencia jellemzői, az informatikai végzettség és az adatmentési szokások, valamint az elszenvedett adatvesztések között [170].

5.2.1 A felhasználó besorolása és az biztonsági adatmentés hiányának vizsgálata

Az alábbi vizsgálatot annak érdekében végeztem el, hogy képet kapjak arról, hogy az általam definiált felhasználói csoportok milyen számban készítenek biztonsági másolatot.

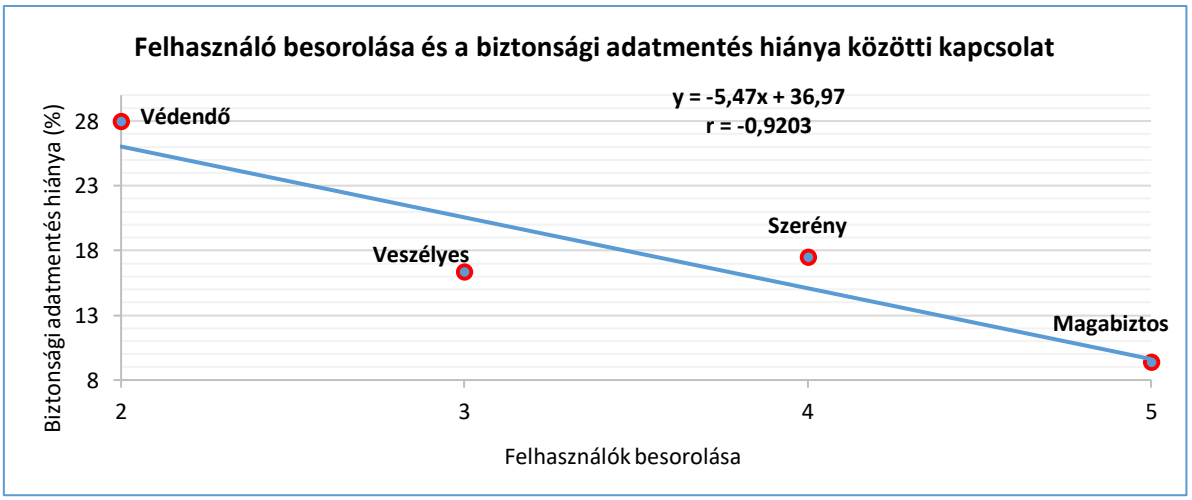
A vizsgálat során azt elemeztem, hogy az adott csoport milyen százalékos arányban nem készít biztonsági mentést (59. ábra). Az eredményekből látható, hogy a „Védendő” csoportba tartozók közül vannak a legtöbben (28%), akik nem készítenek biztonsági adatmentést. Valószínűsíthető, hogy ez a csoport az, aki nem tudja, hogy egyrészt miért is fontos a biztonsági adatmentés, másrészt nem áll rendelkezésére olyan technikai megoldás, aminek segítségével elkészíthetné az adatai mentését. A „Magabiztos” csoportba tartozók kisebb (9,4%) mértékben nem készítenek biztonsági mentést, mint a „Veszélyes” csoportba tartozók (16,4%). Ennek vélhetően az az oka, hogy az előbb említett két csoport tagjai a saját értékelésük alapján rendelkeznek a kellő biztonságtudatossággal, viszont míg a „Magabiztos” csoportnak megvan a szükséges tudása, addig a „Veszélyes” csoportnak nincs informatikai végzettsége. Így kimondható, hogy a „Magabiztos” csoport azon tagjai, akik nem készítenek biztonsági adatmentést, felelőtlenül viselkednek. Míg a „Veszélyes” csoport azon tagjai, akik nem készítenek biztonsági adatmentést, az informatikai ismeretük hiányáról tesznek tanúbizonyságot. A „Szerény” csoportba tartozók 17,5%-a nem készít biztonsági adatmentést.

Valószínűsíthető, ahogyan korábban már megállapítást nyert, hogy ennek a csoportnak vagy nincs vagy bevallottan alacsony a biztonságtudatossága, annak ellenére, hogy rendelkeznek valamilyen szintű képzésben szerzett informatikai ismerettel [172][174].



59. ábra Kapcsolat a felhasználó besorolása és a biztonsági adatmentés között (forrás: saját kérdőíves felmérés; készítette a szerző)

A felmérés alapján megállapítom ebben a vizsgálatban is, hogy a felhasználók körében szükséges a rendszeres biztonságtudatossági képzés/oktatás, mivel a biztonsági adatmentésre a végzettségnek erős hatása van, ezt a 81,54%-os értékű determinációs együttható is alátámasztja (60. ábra).



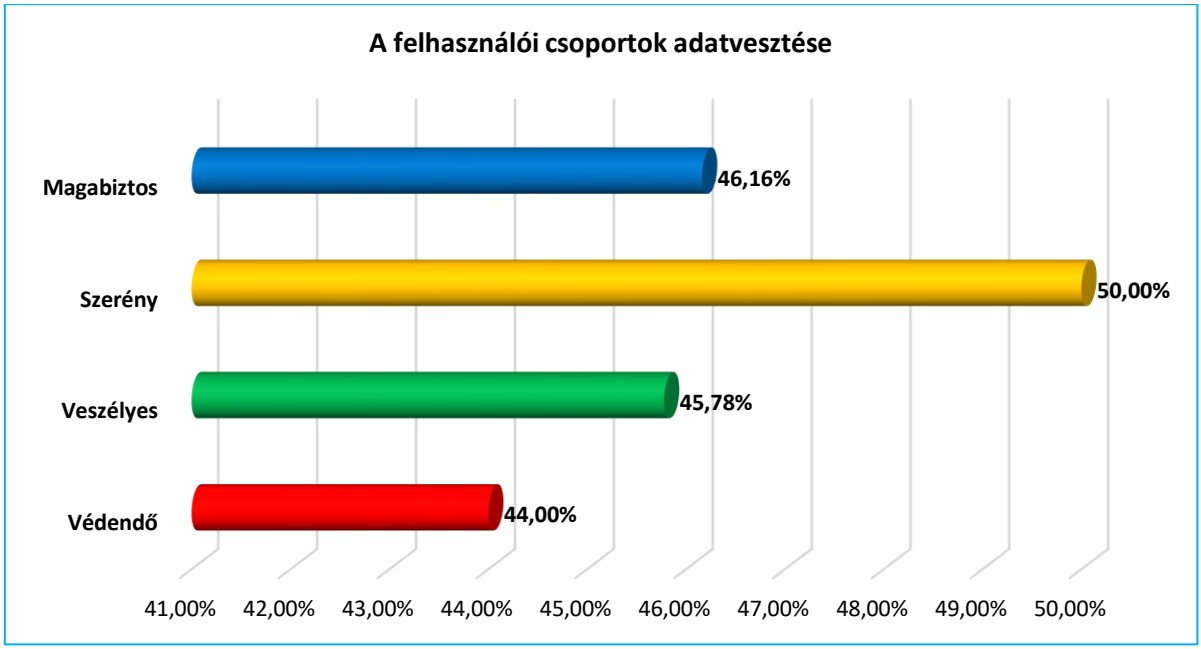
60. ábra Korreláció a felhasználó besorolása és a biztonsági adatmentés között (forrás: saját kérdőíves felmérés; készítette a szerző)

A biztonsági adatmentés hiánya és a felhasználó besorolási szintje között fordított arányosság van, a magasabb szintű felhasználók esetében alacsony a biztonsági mentés hiánya. A besorolási szint és az adatmentés hiánya lineárissal jól közelíthető, amit a korrelációs együttható

abszolút értéke (|r|=0,9203) is mutat. A negatív előjel arra utal, hogy minél jobban képzett az adott felhasználó, annál gyakoribb a fontos adatainak biztonsági mentése.

5.2.2 Korrelációs kapcsolat a felhasználó besorolása és az adatvesztés között

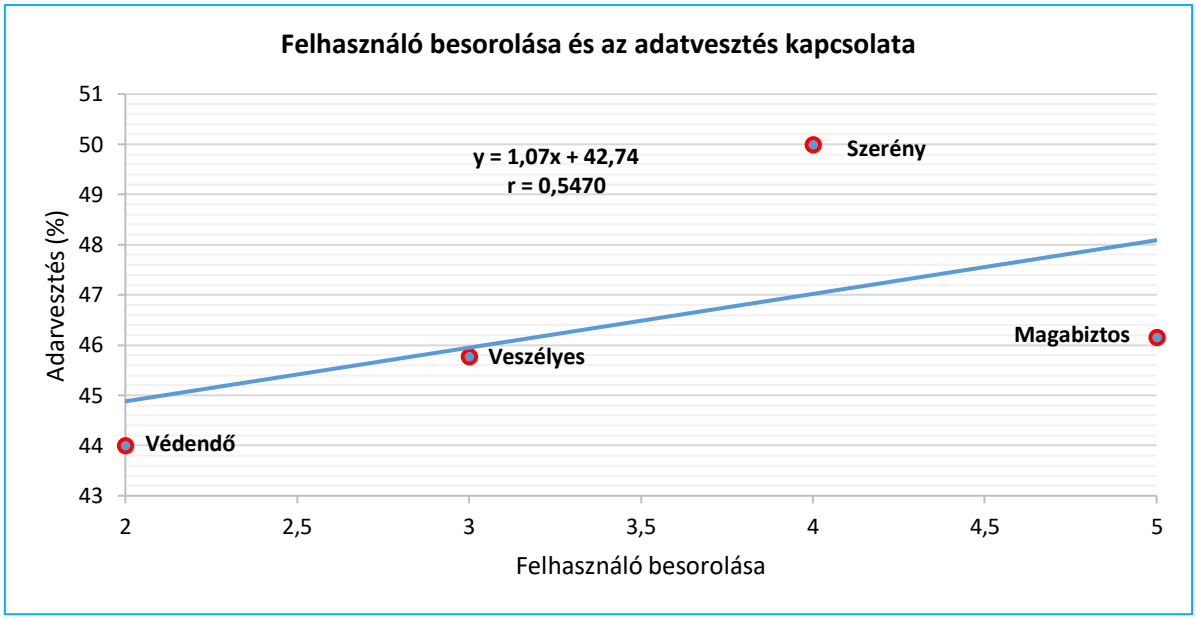
Az alábbi korrelációs vizsgálatot ez esetben azért végeztem el, mert kerestem az összefüggést a biztonságtudatosság, a digitális kompetenciával kapcsolatos besorolás, valamint az informatikai ismeretek és az adatvesztés előfordulása között (61. ábra).



61. ábra Kapcsolat a felhasználó besorolása és az adatvesztés között (forrás: saját kérdőíves felmérés; készítette a szerző)

A megalkotott négy csoport vonatkozásában végeztem el a korrelációs vizsgálatot. Ezeknél a csoportoknál az adatvesztés előfordulását vettem alapul. Jól látható, hogy a „Védendő” kategória szenvedett el a legkevesebb adatvesztést (44%). Szintén kevés adatot vesztettek a „Veszélyes” kategóriába tartozók (45,78%). A „Szerény” kategória esetében látható, hogy viszonylag magas (50%) az adatvesztés előfordulása. A bekövetkező problémát a kellő magabiztosság, valamint a kompetencia és a tudatosság hiánya okozhatja. A „Magabiztos” kategória eredménye (46,16%) magasnak tekinthető volt. Valószínűsítem, hogy ezek a felhasználók olyan sok adattal dolgoznak, ami már a nagy számok törvénye értelmében is több hibázási lehetőséget rejt magában, legyen az technikai vagy felhasználói hiba. (62. ábra) A diagramon jól látható, hogy a “Szerény” besorolású felhasználói csoport illeszkedik legkevésbé a lineáris függvényre. Az adatvesztés és a felhasználói besorolás nem írható le lineáris összefüggéssel, de a kapcsolat kimutatható a vizsgált elemek között. A fentiekben bemutatottak is megerősítik azt a feltételezést, hogy nem elegendő az egyszer megszerzett informatikai

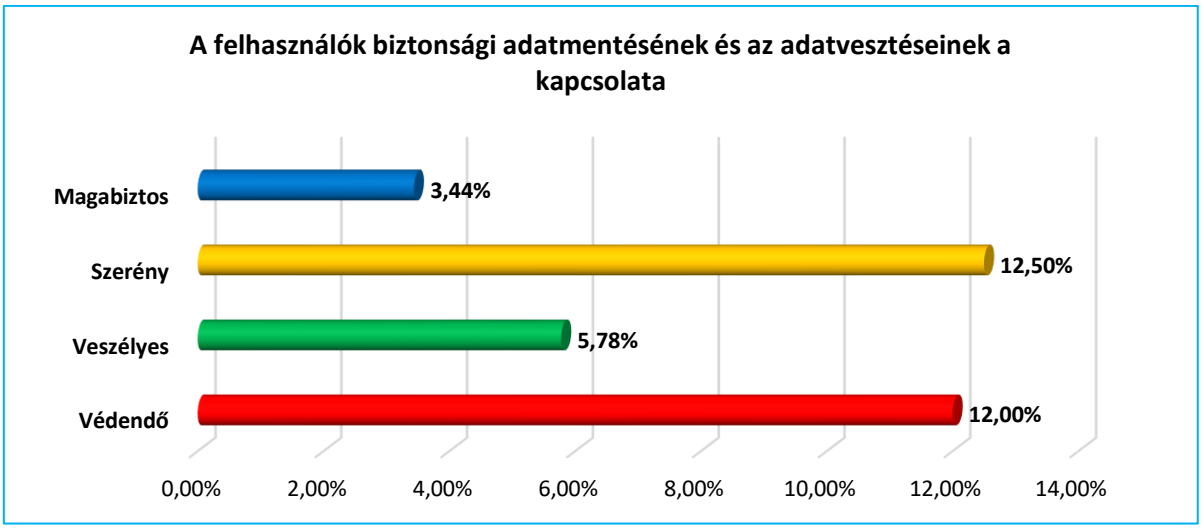
ismeret, hanem azt rendszeresen, kiemelt hangsúlyt helyezve a biztonságtudatosság növelésére, kell ismételten felelevéníteni és frissíteni [82][165].



62. ábra Kapcsolat a felhasználó besorolása és az adatvesztés között (forrás: saját kérdőíves felmérés; készítette a szerző)

5.2.3 Az el nem végzett biztonsági adatmentés és az adatvesztés kapcsolata.

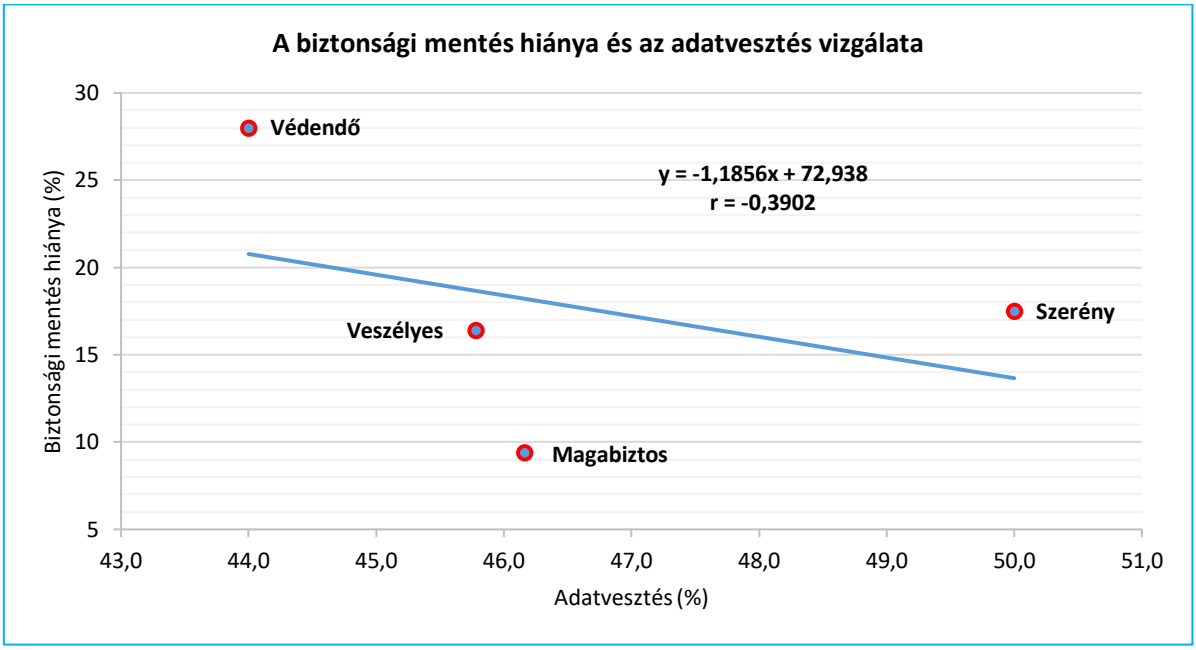
Az alábbi vizsgálatot annak érdekében végeztem el, hogy bemutassam az adatvesztések előfordulása és a biztonsági adatmentések hiánya közötti kapcsolatot.



63. ábra A biztonsági adatmentés hiányának és az adatvesztésnek az összefüggése (forrás: saját kérdőíves felmérés; készítette a szerző)

Látható (63. ábra), hogy a „Szerény” felhasználók és a „Védendő” felhasználók körében, akik alacsony biztonságtudatossággal rendelkeznek, magasabb, 12% körüli azon felhasználók aránya, akik nem végeznek adatmentést és vesztettek már adatot is. A „Veszélyes” felhasználók

esetében ez az arány megközelíti az 6%-ot, a „Magabiztos” felhasználók esetében csak 3% ez az arány. Ezzel bizonyítható, hogy azon felhasználók esetében, akiknek bevallottan magas a biztonságtudatossága, fele vagy ennél kevesebb az adatvesztés és az adatmentés hiányának az aránya, mint az alacsony biztonságtudatossággal rendelkező felhasználók esetében [83].



64. ábra A biztonsági adatmentés hiányának és az adatvesztésnek az összefüggése (forrás: saját kérdőíves felmérés; készítette a szerző)

A biztonsági mentés hiánya és az adatvesztés között közepesen erős kapcsolat van, a korrelációs együttható értéke (|r|= 0,5813), ez negatív korreláció, vagyis annál több az adatvesztés minél kevesebb a biztonsági mentés. (64. ábra) A biztonsági mentés tehát közepes erősségű hatással van az adatvesztés bekövetkezésére, mivel a determinációs együttható értéke 33,79%.

5.2.4 Összegzés

A biztonsági adatmentés jelenleg is nagyon fontos tényező, azonban ahogy haladunk előre a tudásalapú társadalom fejlődésében, egyre fontosabb lesz az adataink biztonsága és azoknak a rendelkezésre állása. Mivel az adat “a jövő olaja”, így egy újfajta erőforrásként kell rá tekintenünk, ezáltal magas értéket képvisel. Mindenki számára fontos, hogy az évek során felhalmozott és felgyülemlett hasznos adat védelme biztosított legyen. A felhasználói szintű adatmentés a felhasználó feladata és felelőssége. A művelet végrehajtása is, köszönhetően a technológia gyors fejlődésének, olyan szintű ismereteket követel meg, amelyekkel a felhasználó az adott technológiát alkalmazni tudja. Tehát egyaránt szükséges a magas szintű biztonságtudatosság, valamint az ezzel megegyező szintű digitális kompetencia is. Korrelációs számítással bizonyítottam, hogy a biztonsági adatmentésre az informatikai ismereteknek erős

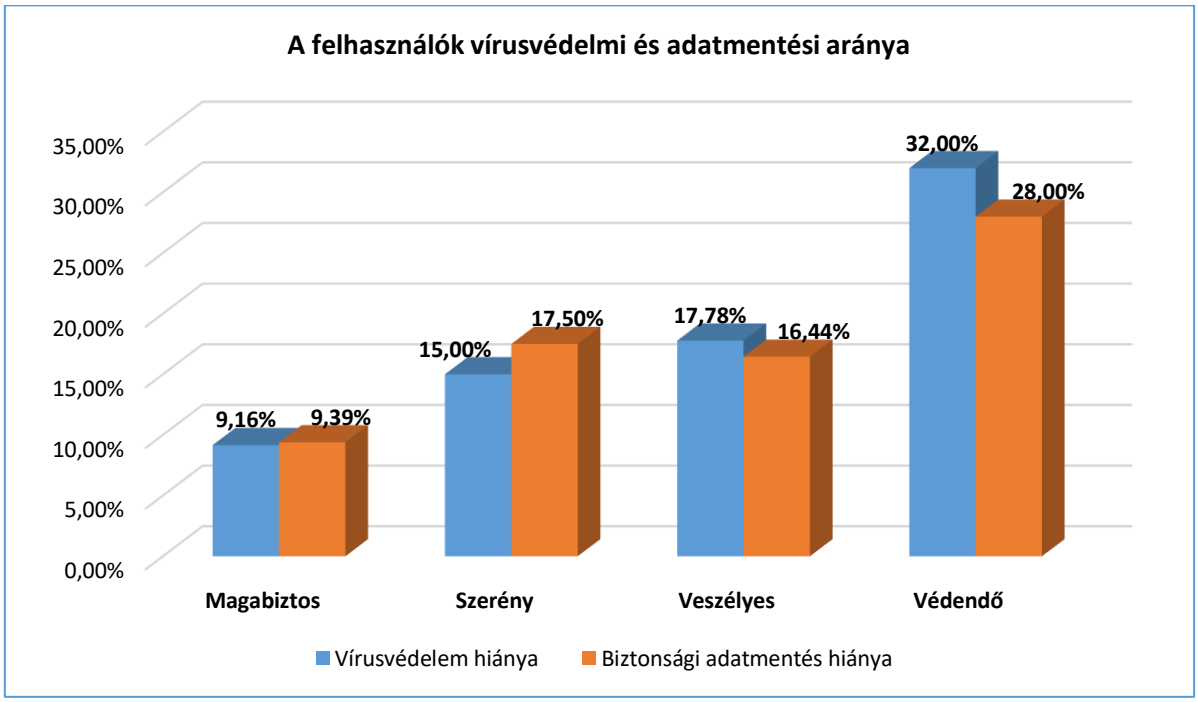
hatása van. Továbbá a biztonsági mentés hiánya és az adatvesztés között közepes erősségű kapcsolat van, annál magasabb az adatvesztés, minél kevesebb a biztonsági mentés. A biztonsági mentés tehát közepes hatással van az adatvesztés bekövetkezésére [174][175].

5.3 A felhasználók vírusvédelmi és adatmentési szokásainak vizsgálata

A felhasználók vírusvédelmi és adatmentési szokásait vizsgáltam azzal a céllal, hogy bizonyítsam azt, milyen összefüggés van a két felhasználói viselkedés között. Mivel az elmúlt évek legnagyobb biztonsági kihívása a zsarolóvírusok támadása elleni védekezés, azt gondolom, hogy elsődleges a felhasználók ilyen irányú felvilágosítása [172][173].

5.3.1 A felhasználók vírusvédelmi és adatmentési szokásainak aránya

A felhasználók csoportjait már a korábbi részekben vizsgáltam több szempont alapján. Több megállapítást is tettem a felhasználók digitális szokásairól, de további két, egymástól eltérő, de mégis összefüggő viselkedést még nem vetettem össze. A vizsgálat alapján látható (65. ábra), hogy a vírusvédelem hiánya és a biztonsági adatmentés hiánya milyen szorosan összefüggően, szinte közel azonos arányban jelenik meg az adott felhasználók esetében.

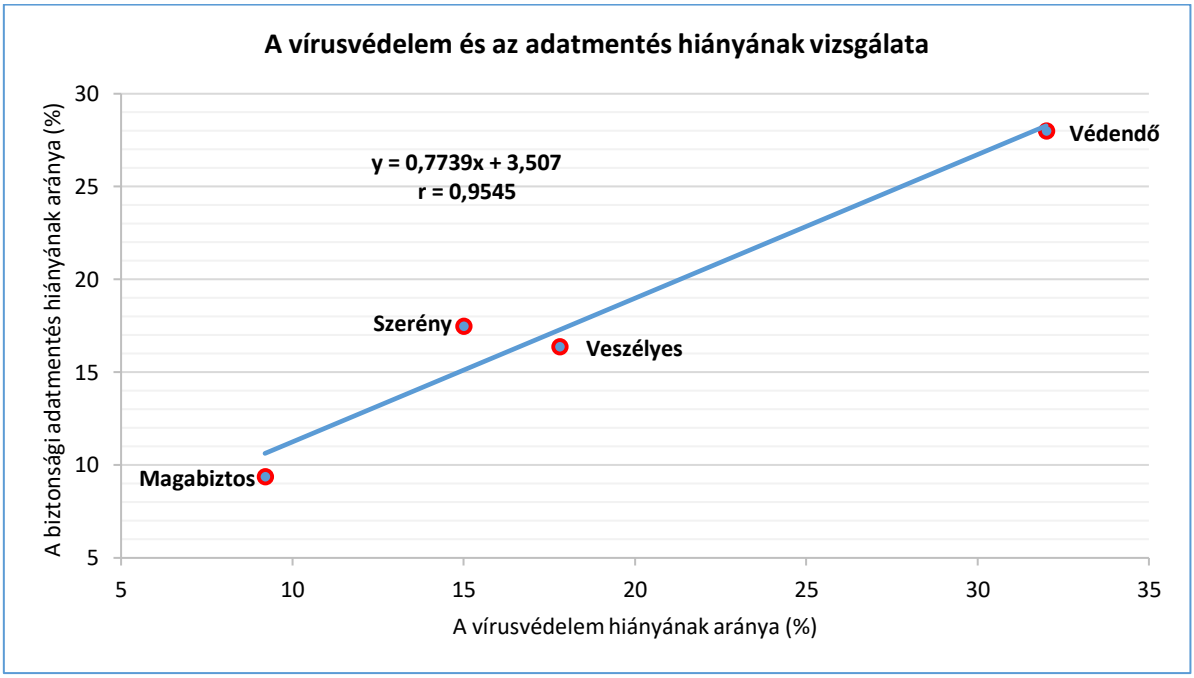


65. ábra A felhasználók vírusvédelmi és adatmentési aránya (forrás: saját kérdőíves felmérés; készítette a szerző)

Továbbá az is szembetűnő, hogy a felhasználói csoportoknak az általam felállított rangsor szerint növekszik (egy kivétellel) mindkét szokásnak az aránya. Látható, hogy a „Magabiztos” 9,16-9,39% aránypárral, a „Szerény” 15-17,5% aránypárral, a „Veszélyes” 17,78-16,44% aránypárral és a „Védendő”, kimagaslóan a többi közül, 32-28% aránypárral szerepel [157].

5.3.2 A felhasználók vírusvédelmi és adatmentési szokásainak relációja

A vírusvédelem hiánya és az adatmentés hiánya a felhasználói csoportok esetében erős kapcsolatot mutat (|r|=0,9545), a determinációs együttható értéke 94,91%, ami azt jelenti, hogy a felhasználók a két biztonsági megoldást közel azonos arányban nem használják, közöttük erős kapcsolat van. (66. ábra)

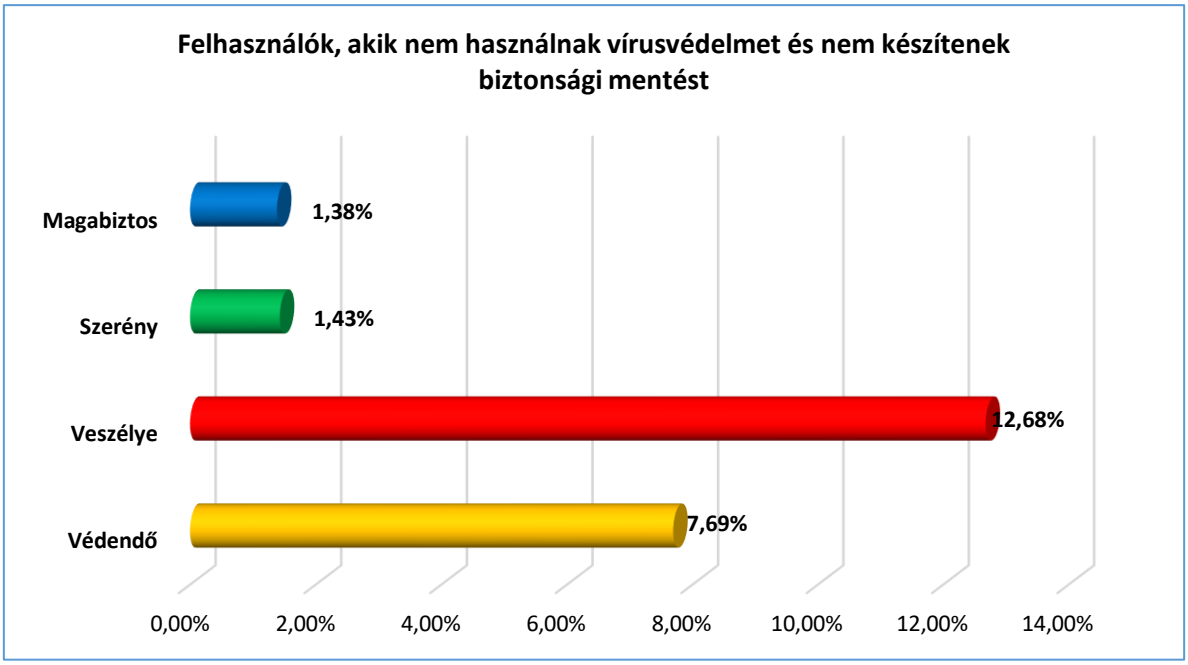


66. ábra A vírusvédelem és az adatmentés hiányának vizsgálata (forrás: saját kérdőíves felmérés; készítette a szerző)

A felhasználói csoportok ezen alkalmazásokat pedig besorolási szintjüknek megfelelően a diagramon bemutatott erős lineáris korreláció szerint nem alkalmazzák.

5.3.3 A felhasználók vírusvédelmi és adatmentési szokásai szerinti szűrés alapján

A fenti két vizsgálat olyan aránypárokat és korrelációkat mutatott, amelyek alapján jól látható a felhasználók szokásainak együttes mozgása. A mostani vizsgálattal azt mutatom meg, hogy a különböző csoportok tagjai, egyénenként hogyan viselkednek a fenti szempontok szerint. A kérdőív adatbázisában azokat a felhasználókat választottam ki, akik a „Használ vírusvédelmi-, vagy tűzfal alkalmazást azon (azokon) az eszközön (eszközökön), amin internetezik?” kérdésre nemlegesen válaszoltak, valamint a „Szokott-e készíteni az eszközén (eszközein) tárolt adatokról biztonsági másolatot?” kérdésre nemlegesen válaszoltak (67. ábra).



67. ábra Felhasználók, akik nem használnak vírusvédelmet és nem készítenek biztonsági mentést (forrás: saját kérdőíves felmérés; készítette a szerző)

A felhasználói csoportok arányai alapján kijelenthető, hogy azon felhasználók esetében jelentősebb ez az arány, akik nem rendelkeznek informatikai ismeretekkel. A „Veszélyes" felhasználók esetében több, mint 12,68%, a „Védendő" felhasználók esetében közel 7,69% ez az arány. Látható, hogy a „Magabiztos" (1,38%) és a „Szerény" (1,43%) felhasználók esetében, akik rendelkeznek informatikai ismeretekkel, nem éri el a két százalékot ez az arány [159].

5.3.4 Összegzés

A fenti vizsgálat alapján látható, hogy azon felhasználók körében, akik rendelkeznek oktatás útján megszerzett informatikai ismeretekkel, magasabb a biztonsági adatmentés és a vírusvédelem alkalmazása. Akik nem tanultak informatikát, azok körében gyakrabban előfordul, hogy se vírusvédelmet, se biztonsági adatmentést nem alkalmaznak [190].

Megállapítom, hogy egy esetleges zsarolóvírus-támadást azok szenvedhetnek el nagyobb arányban, akik nem rendelkeznek tanult informatikai ismeretekkel. Ennek a kockázati tényezőnek a korai felismerése, valamint ennek prevenciója jelentősen javíthatja akár az egyén, akár egy vállalat adatvagyonának a védelmét [176][177].

5.4 A „Veszélyes" felhasználók kiszűrése

Az általam összeállított és lefolytatott, a digitális kompetenciát és a biztonságtudatosságot felmérő nemzetközi kérdőív válaszainak kiértékelése során öt felhasználói csoportot definiáltam, amelyből négyet vizsgáltam. A felhasználói csoportok definiálásához kidolgozott

módszer- és viselkedésspecifikus szempontrendszert állítottam fel a felhasználók kockázati tényezőinek a figyelembevételével, amelynek segítségével a felhasználói szintek a későbbiekben is alkalmazhatóak.

A négy felhasználói csoport közül a „Magabiztos", a „Szerény" és a „Védendő" viselkedése a szempontrendszerbe történt besorolás alapján kiszámítható és determinisztikus. Ezzel szemben a „Veszélyes" felhasználói csoport viselkedése hektikusságot, kiszámíthatatlanságot mutat, és ahogy a fenti vizsgálatokból látható, sok esetben nem illeszkedik a besorolása szerint hozzárendelt értékhez. A felhasználói csoport elnevezése is ennek köszönhető, mert sok esetben kiszámíthatatlan, ezért veszélyes. Az általam kidolgozott szempontrendszer alkalmazásával ezt a kockázatos felhasználói csoportot könnyen be lehet azonosítani és ki lehet szűrni. Amennyiben ez megtörténik, abban az esetben ezek a felhasználók a magas kockázatosságuk miatt kiemelt figyelmet, egyéni biztonsági házirendet, speciális és gyakoribb biztonsági oktatást kaphatnak a munkaadótól vagy az iskolától. Kutatásaim eredménye alapján, ezzel a módszerrel egy adott szervezet információbiztonsági kockázatát jelentősen lehet csökkenteni, valamint ennek a szempontrendszernek az alkalmazása a szervezeti kockázatelemzésbe beépíthető. A felhasználók egyes kompetenciáinak a felmérésére és azok javítására a következőkben bemutatott keretrendszer és akadálymentesítés sikeresen alkalmazható [163].

5.5 Összefoglalás

A felhasználók módszer- és viselkedésspecifikus vizsgálatával számos olyan dologra világítottam rá, melyek a továbbiakban a téziseim bizonyítását szolgálják.

A felmérésem alapján megállapítom, hogy a felhasználók egy esetleges vírustámadás esetén a biztonságtudatosságuknak és a digitális kompetenciájuknak, valamint az informatikai ismereteiknek megfelelően reagálnak. A felhasználók viselkedését pozitívan értékeltem abból a szempontból, hogy nagy számban kérnének valamilyen segítséget szakemberektől, azt azonban negatívan minősítettem, hogy csak kevés számban értesítik a hatóságokat a vírusfertőzés terjedésének megakadályozása érdekében.

A fejezetben több felmérés esetében is megállapítom, hogy a felhasználók mindegyik csoportja számára szükséges a folyamatos és ismétlődő jellegű biztonságtudatossági képzés a magasfokú biztonság elérése, megtartása érdekében.

Számításokkal bizonyítottam, hogy minél magasabb a felhasználó besorolási értéke, annál alacsonyabb a vírusvédelem hiánya. Mivel a korrelációs együttható abszolút értéke közel egy, a vizsgálati értékek jól illeszkednek a lineáris függvényre. A korreláció előjele negatív, amiből

látszik, hogy minél magasabb besorolási értéket kapott a felhasználó annál kevésbé jelentkezik a vírusvédelem hiánya, a kiszámított determinációs együttható értéke szerint pedig közöttük erős kapcsolat van.

Megállapítom, hogy a felhasználó besorolása és a vírustámadások közötti kapcsolat erős, továbbá erősebb, mint a felhasználó besorolása és a vírusvédelem alkalmazás hiánya közötti kapcsolat.

Számításokkal bizonyítottam, hogy az elszenvedett vírustámadások alapján az alacsonyabb értékelésű felhasználók kockázatot jelentenek a digitális rendszerekre, mivel a kockázati szint értéke fordítottan arányos a felhasználó besorolási értékének szintjével.

Megállapítom az eredmények alapján, hogy amennyiben a felhasználó nem használ vírusvédelmet, abban az esetben vírustámadás éri. A vírusvédelem hiánya fordítottan arányos a felhasználó szempontrendszer szerinti szintjével, és a vírusvédelem hiánya és a vírustámadások előfordulása között kutatási eredményeim alapján lineáris kapcsolatot mutattam ki.

Bizonyítom, hogy azon felhasználók esetében, akiknek bevallottan magas a biztonságtudatossága, fele vagy ennél kevesebb az adatvesztés és az adatmentés hiányának az aránya, mint az alacsony biztonságtudatossággal rendelkező felhasználók esetében. Ha kevesebb a biztonsági mentés, akkor több az adatvesztés. A biztonsági mentés tehát közepes erősségű hatással van az adatvesztés bekövetkezésére. Számításaim alapján megállapítom, hogy a felhasználók rendszeres biztonságtudatossági képzése/oktatása erős hatással van a biztonsági adatmentés végrehajtására [162].

Megállapítom, hogy a vírusvédelem és az adatmentés együttes hiánya a felhasználói csoportok esetében erős kapcsolatot mutat, ami azt jelenti, hogy a felhasználók a két alkalmazást közel azonos arányban nem használják. A felhasználói csoportok ezen alkalmazásokat pedig besorolási szintjüknek megfelelően a diagramon bemutatott erős lineáris korreláció szerint nem alkalmazzák.

Megállapítom, hogy azoknál a felhasználóknál, akik nem rendelkeznek informatikai ismeretekkel, mind a vírustámadások aránya, mind a vírusvédelem hiánya és az adatmentés hiánya magas.

Megállapítom, hogy a „Veszélyes” felhasználói csoport viselkedése hektikusságot, kiszámíthatatlanságot mutat és sok esetben nem illeszkedik az ehhez a csoporthoz hozzárendelt

értékhez. Ezzel is bizonyítom, hogy az általam kidolgozott felhasználói szempontrendszer alkalmas a felhasználók besorolására, továbbá ennek alkalmazásával a kockázatos felhasználói csoportot könnyen be lehet azonosítani és kiszűrni. Így a magas kockázatú felhasználók, kiemelt figyelmet, egyéni biztonsági házirendet, speciális és gyakoribb biztonsági oktatást kaphatnak a munkaadótól vagy az iskolától. Kijelentem, hogy ezzel a módszerrel egy adott szervezet információbiztonsági kockázata jelentősen csökkenthető, valamint ez a szervezeti kockázatelemzésbe beépíthető.

A fenti kutatás egyes eredményei és azokból készített kapcsolatok alapján is jól látható, hogy a felhasználók biztonságtudatossági- és digitális kompetenciaszintje mennyire szerteágazó. A felállított szempontrendszer alapján elkészített korrelációk és rangsorok jól bizonyítják azt, hogy melyek azok a gyenge pontok, amelyek alapján akár kormányzati, akár társadalmi összefogással szükséges segítséget nyújtani a felhasználók számára. A felhasználók jó digitális kompetencia- és biztonságtudatossági szintje elengedhetetlen az ipari termelés optimalizálásához, valamint a jelenleg már zajló Ipar 4.0 forradalomnak a társadalom egésze számára történő kiaknázásához [84]. Ezt segítheti az a digitális kompetencia keretrendszer, amely alapján a felhasználók ismeretszintje beazonosítható. A magyar társadalom sajátosságait figyelembe vevő digitális kompetencia értékelési rendszer kidolgozásának elsődleges célja volt, hogy segítse a magyar gazdasági jólét szintjének emelését, annak fejlődését [85]. Továbbá biztosítsa a társadalom tagjainak a biztonságtudatossági szint növelését, amely a mindenki számára az újdonság erejével ható kibertér használatához szükséges [160][161][162].

6 A VVSZM[24] DIGITÁLIS KOMPETENCIA KERETRENDSZERE

A mai társadalmi berendezkedésünk része a digitalizáció. A technológia rohamos fejlődése és annak az élet minden területét behálózó mivolta elengedhetetlenné teszi a lakosság digitális ismereteinek fejlesztését. Az azonban, hogy a digitális ismeretek milyen szintűek, csak egy egységes mérési rendszer által azonosítható. Kutatásaim rámutattak arra, hogy jelenleg nincs a magyar össztársadalmi viszonyokra igazított és kidolgozott értékelési rendszer a digitális kompetencia és a biztonságtudatosság minősítésére. A disszertációm elkészítése során az Európai Unió Digitális Kompetencia Keretrendszerének és a digitális intelligencia definícióinak felhasználásával pótoltam ezt a hiányosságok, amelyet az alábbiakban mutatok be. A VVSZM Digitális Kompetencia Keretrendszer az általam megalkotott keretrendszer, amely a nevét az előző fejezetben definiált négyféle felhasználói besorolás elnevezésének kezdőbetűi alapján kapta, úgymint Védendő-Veszélyes-Szerény-Magabiztos (a továbbiakban: VVSZM) [161][163][165].

6.1 A digitális kompetencia értékelési rendszere

A digitális kompetencia értékelési szintjeit azért fontos meghatározni, mert a felhasználó kap egyfajta minősítést a saját képességeinek szintjéről, valamint az értékelő személy vagy intézmény, például a munkáltató vagy a pedagógus tudja azt, hogy az adott személy milyen szintű kompetenciával rendelkezik, valamint a kompetencián belül is az adott részterületen milyen a besorolása. A digitális kompetencia értékelése során az a cél, hogy azok a részterületek kerüljenek felszínre, amelyek elmaradnak a többitől. Továbbá az is cél, hogy a képességek szintjének a meghatározásával a felhasználó vagy az értékelő személy lássa azt az értékelés eredményéből, hogy mely területek erősítésével lehet a tudásszintet emelni, illetve melyek azok a képességek, amelyek fejlesztésére már nem kell erőforrást fordítani [49][158][159][160].

6.1.1 Előzmények

A VVSZM Digitális Kompetencia Keretrendszerének kidolgozásához az Európai Unió Digitális Kompetencia Keretrendszerének definícióit és értékelési szempontjait használtam alapnak. Kutatásaim során megtudtam, hogy 2015-ben az Európai Unió által megbízott, mintegy 120 fős, nemzetközi szakértőkből álló csoport elvégezte a digitális kompetencia szintjeinek és besorolásának kidolgozását [51]. Azonban ez a keretrendszer a munkavállalók és munkaadók hatékonyabb „egymásra találása” céljából készült. Ami alapvetően a korszerű

[24] VVSZM – Védendő, Veszélyes, Szerény, Magabiztos

tudást igénylő munkaerőpiac szempontjából nagyon előnyös, és valóban egy olyan értékelési rendszert sikerült alkotni a szakértői csapatnak, amellyel a munkavállaló viszonylag jó megközelítő értéket képes kapni a saját digitális kompetenciáját illetően. Ez a megalkotott keretrendszer nem fedi le a társadalom teljes egészét, tehát nem alkalmazható mindenkire, aki használja a digitális eszközöket és azon keresztül igénybe veszi a digitális javakat [52][60], továbbá a keretrendszer általános szempontokat foglal magába. Sajnos emiatt nem lehet ez alapján a társadalmat felmérni. Mert nincs benne olyan értékelési szempont, ami a sajátosságainkra, valamint azon társadalmi rétegekre alkalmazható lenne, akik még, vagy már nem tartoznak a munkavállalói társadalmi rétegbe [52][60]. Gondolok itt az eltérő társadalmi értékrendekre, a fizetések és azok eloszlásának alakulására, a közszféra és a versenyszféra digitalizációjának helyzetére, a társadalmi és egyéni igényekre, a felhasználók egyéb más kompetencia képességeire, mint például az idegennyelv-ismerete, a funkcionális szövegértésre, továbbá az általános műveltségre, valamint a társadalmi ingerküszöbre és az arra ható tényezőkre, ezen kívül a különböző társadalmi rétegek és korosztályok populációjára és összetételére [161][163][166]. Valamint a DJP2.0 szerint „a digitális kompetenciaszintjeinek méréséhez nem áll rendelkezésre általános eszköz, így nincs valós tudásunk a munkaerő digitális kompetenciájáról” [16].

6.1.2 Az értékelés aktualitása

A fenti tényezők figyelembevétele azért bír nagy fontossággal, mert a különböző társadalmi rétegek és korosztályok esetében más igények és elvárások lépnek fel a digitális kompetenciát illetően. Szükséges felmérni azt a korosztályt vagy felhasználói réteget, akik, mint „belépők” jelennek meg a digitális térben. Itt korosztálybeli eltérés is lehet, mert egyszer ebbe a szintbe sorolhatók azok az óvodás korú gyermekek, akik már nagy érdeklődést mutatnak a digitális eszközök iránt, valamint ide sorolhatók azok a felnőtt korúak, akik ugyan használták már a digitális eszközöket, de az eddigiek során nem mutatkozott olyan igény, ami miatt ezt a képességüket fejleszteni kellett volna. Ide sorolhatók azok az időskorúak is, akik úgy élték le az életüket, hogy eddig nem volt szükségük ilyen irányú képességek megszerzésére, viszont a modern, felgyorsult világ és a megváltozott életmód őket is rákényszeríti arra őket is, hogy ezen ismereteiket és képességeiket fejlesszék [55]. Az előző fejezetben definiált „Védendő” csoport is ebbe a kategóriába sorolható. Mert sajnos az a mondás, amely szerint „Aki kimarad, az lemarad!”, napjainkban hatványozottan érvényes. A megváltozott életvitelünk, amely a technológiákra és azok fejlődésére épül, rákényszerít mindenkit arra, hogy a digitális kompetenciáját fejlessze [86]. Ez nem minden esetben tudatosan történik, hanem az új

technológiával való találkozást követően, annak alkalmazhatósága érdekében a felhasználók kénytelenek elsajátítani azokat a szükséges ismereteket, amelyek annak működtetéséhez szükségesek. A televíziózás, valamint a televíziókészülékek hatalmas fejlődése lehet az egyik példa erre. Ezek a készülékek, mivel már digitálisak, olyan, a korábbiakhoz képest „ismeretlen" funkciókkal is rendelkeznek, amelyek használatához a felhasználónak el kellett sajátítania olyan új készségeket és fogalmakat, amelyeket korábban nem ismert [52][54]. A SMART televíziók, az internetkapcsolat segítségével már nem egyszerű televíziók, hanem komplett multimédiás szórakoztató-, információs- és kommunikációs központok [52]. Ez a technológiai fejlődés hatalmas szintbeli ugrást jelent a minőségben azoknak az embereknek, akik évtizedekig a hagyományos katódsugárcsöves tévéket használták és most annak a régi technológiának az avulása miatt „kénytelenek" ilyen új típusú eszközt vásárolni, viszont ezen eszközök használatához már nem elegendő a korábbi ismeret, azt megújítani, frissíteni szükséges [16][38][52][158][160][166].

6.1.3 Az értékelés szükségessége

A televíziós evolúció drasztikusabban mutatja be azt a technológiai „sokkot", ami éri a mai társadalmat, mint mondjuk a telefonok evolúciója. Ugyanis a telefonok esetében, amikor a 90-es évek közepétől elterjedtek a mobiltelefonok, és szinte teljesen kiszorították a hagyományos vezetékes telefonokat, már ott is új ismeretekre volt szüksége az átlag felhasználónak. Azonban az még „csak" a telefonálásra és az ahhoz tartozó ismeretek alkalmazására korlátozódott. Majd a 2000-es évek elején megjelentek az első adatmodemként is funkcionáló telefonok és a szolgáltatásban már adatforgalom is elérhető volt. Ezek a telefonok még csak számítógéphez csatlakoztatva tudtak internetelérést biztosítani [50]. Majd a SMART telefonok hozták el az igazi áttörést közvetlenül a telefonon történő internetelléréssel. Az adatforgalom sebességének növekedésével és a tartalmak szerteágazó fejlődésével a telefonunk is már inkább egy hordozható komplett multimédiás szórakoztató-, információs- és kommunikációs központ. Azoknak felhasználóknak, akik követték a technológiai evolúciót, mindig „kis dózisokban volt adagolva" az új tudás. A telefon és a TV esetében természetesen nincs szükség a digitális kompetencia minden területének birtoklására, mert ez ennél jóval szerteágazóbb és összetettebb tudás. Ez a két kiragadott példa csak nagy vonalakban mutatja be azt a problémát, aminek a felszámolása jelenleg is nagy társadalmi kihívás és kormányzati szándék. Ehhez elengedhetetlen a felhasználók tudásszintjének rendszeres felmérése [50][163][165][166].

6.2 Digitális alapkészségek

A Yuhyun Park [53] szerint 8 fontos digitális alapkészség létezik (68. ábra). Ezek közé tartozik a digitális írástudás, a digitális kommunikáció, a digitális érzelmi érettség és intelligencia, valamint a digitális biztonság.

68. ábra A digitális intelligencia „DQ” (Digital Quality – digitális intelligencia) alkotóelemei (készítette: a szerző) [53]

Ezek részét képezi továbbá a digitális jogok ismerete, a digitális „egyéniségünk” (digitális állampolgár, vállalkozó és alkotó) és a digitális használat („use” alá sorolják a digitális egészségügyet, közösségi tevékenységet és a képernyő előtti egyéb tevékenységeket) [87]. Kutatási eredményeim alapján meggyőződésem, hogy csak 7 alapkészség létezik, mivel a Yuhyun Park [53] által megállapítottakban elkülönítve szerepel a „security” és a „safety” ágazat. Előbbibe a „hagyományos” kibervédelmet sorolják, a másikba pedig a digitális kapcsolattartással, tartalommal kapcsolatos kockázatok kivédését [88]. Kutatásaim azonban arra engedtek következtetni, hogy ezt a két területet együtt kell kezelni és nem lehet egymástól ilyen élesen elkülöníteni [89]. A probléma abban rejlik, hogy a digitális világ gyorsan és folyamatosan változik, miközben a kormányzati szintű gyermekvédelmi politika lassan zárkózik fel az internet veszélyeinek a kivédésére, illetve a káros hatásainak tompítására [54].

6.3 Besorolási osztályok

A digitális kompetencia egyike annak a 8 kulcskompetenciának, amit az EU az Élethosszig tartó tanulás programjában meghatároz. A digitális kompetencia egy transzverzális kulcskompetencia, amely, mint ilyen, lehetővé teszi számunkra egyéb kulcskompetenciák elsajátítását (pl. Az anyanyelven- és az idegen nyelveken folytatott kommunikáció; Matematikai kompetencia; A tanulás elsajátítása; Kulturális tudatosság) [46][53][163][166].

Kompetencia területek	Részkompetenciák
1. Információfeldolgozása	1.1 Böngészés, az információk keresése és szűrése
	1.2 Az információk kiértékelése
	1.3 Az információk tárolása és visszakeresése
2. Kommunikáció	2.1 A technológia hatása
	2.2 Az adatok tartalma és megosztása
	2.3 Részvétel az online társadalomban
	2.4 A digitális csatornák kezelése
3. Tartalom létrehozása	3.1 A tartalom fejlesztése
	3.2 A tartalmak integrációja és újbóli felhasználása
	3.3 Szerzői jogok és engedélyek
	3.4 Programozási ismeretek
4. Biztonság	4.1 Védelmi eszközök
	4.2 A személyes adat és a digitális identitás védelme
	4.3 Biztonságtudatosság
5. Problémamegoldás	5.1 A műszaki problémák megoldása
	5.2 A felhasználói igények és azok technológiai megoldásainak azonosítása
	5.3 A digitális eszközök használatával kapcsolatos fejlesztések, újítások, megoldások
	5.4 A digitális kompetencia hiányosságainak azonosítása
6. Tudásátadás	***6.1 A felhalmozott tapasztalatok átadása***
	6.2 Az elsajátított ismeretek átadása
	6.3 Saját példán, viselkedésen keresztül történő tudásátadás

69. ábra A VVSZM Digitális Kompetencia Keretrendszer értékelési szempontjai (Forrás: Saját készítésü kérdőív alapján; készítette: a szerző) [46]

Az Európai Digitális Kompetencia Keretrendszere 21 kompetenciát sorolt be öt osztályba, amit három szintre osztott [54]. Azonban ezeket a kompetenciákat és a besorolási osztályokat, valamint a besorolási szinteket az átlag (nyugat-)európai munkavállalók képességeihez igazították. A keretrendszer nem tartalmazza a régiónk társadalmainak képességeit, azon belül is a gyerekek és az időskorúak képességeit, valamint azon munkavállalók képességeit, akiknek életük során most kell a munkájukhoz először felhasználni a digitális képességeiket. Az általam összeállított és alábbiakban bemutatott osztályokat (2. számú függelék) egy, az Európai Unió Digitális Kompetencia Keretrendszerhez képest a hatodik besorolási osztállyal 6.3.6

Tudásátadási képesség és további négy kompetenciával is bővítettem a 6.3.4 Biztonsági osztályba sorolt Biztonságtudatossági képesség, és a 6.3.6 Tudásátadás osztályba sorolt: A felhalmozott tapasztalat átadásának kompetenciája, a megszerzett ismeretek átadása, a tudás átadása a saját viselkedésének és magatartásának példáján keresztül [163][166].
Az alábbiakban felsorolásra kerülnek azok a digitális kompetencia értékeléséhez szükséges osztályok, amelyek alapján a felhasználók besorolása és értékelése végrehajtható. A különböző osztályok esetében csak azokat definiálom külön, amelyeket én alkottam meg a VVSZM Digitális Kompetencia Keretrendszerhez (69. ábra). Amely osztályok és alpontjai nincsenek külön definiálva az alábbiakban, azokat az Európai Unió Digitális Kompetencia Keretrendszerében már definiálták. A teljes definíciólistát a 2. számú függelék tartalmazza.

6.3.1 Információ és adatfeldolgozás

- Adat, információ és digitális tartalom böngészése, keresése és szűrése.
- Adatok, információk és digitális tartalom értékelése.
- Adatok, információk és digitális tartalom kezelése [54][163][166].

6.3.2 Kommunikáció és együttműködés

- Interakció a digitális technológiákon keresztül.
- Digitális technológiák megosztása.
- A civil szerepvállalás a digitális technológiák révén.
- A digitális technológiákon keresztül történő együttműködés.
- Netikett.
- A digitális identitás kezelése [54][163][166].

6.3.3 Digitális tartalom létrehozása

- Digitális tartalom fejlesztése.
- Digitális tartalom integrálása és újrafeldolgozása.
- Szerzői jog és licencek.
- Programozás [54][163][166].

6.3.4 Biztonság

- Védelmi eszközök.

- Személyes adatok és magánélet védelme.
- Az egészség és a jólét védelme.
- A környezet védelme [54][163][166].
- Biztonságtudatosság.[25]

Tisztában van annak a tudatosságnak a fontosságával, hogy fel tudja mérni tetteinek a biztonságra kiható következményét [163][166].

6.3.5 Problémamegoldás

- Technikai problémák megoldása.
- Az igények és a technológiai válaszok azonosítása.
- A digitális technológiák kreatív használata.
- A digitális kompetencia-hiányok azonosítása[54][163][166].

6.3.6 Tudásátadási képesség[26]

- A felhalmozott tapasztalat átadása,

Képesség annak a tudásnak az átadására, amit a felhasználó, mint tapasztalati tőkét felhalmozott.

- A megszerzett ismeretek átadása,

Képesség annak a tudásnak az átadására, amit a felhasználó tanulmányai során ismeretként elsajátított.

- A tudás átadása a saját viselkedésének és magatartásának példáján keresztül.

A felhasználó a digitális viselkedésének és példamutatásának közvetlen környezetére gyakorolt hatása [163][166].

6.3.7 Összegzés

Az általam megalkotott VVSZM Digitális Kompetencia Keretrendszer besorolási osztályai esetében új osztályokat definiáltam. Az első ilyen osztály a “Biztonság” című osztály “Biztonságtudatosság” című alosztálya, a második a “Tudásátadási képesség” című osztály és annak “A felhalmozott tapasztalat átadása”, “A megszerzett ismeretek átadása” és “A tudás

[25] Saját eredmény
[26] Saját eredmény

átadása a saját viselkedésének és magatartásának példáján keresztül” című alosztályai voltak. A definiált osztályokkal új osztályokat alkottam a digitális keretrendszerben.

6.4 Besorolási szintek

Az Európai Uniós Keretrendszer három besorolási szintet definiál, úgymint az “Alapszintű felhasználó”, a “Középszintű felhasználó” és a “Magas szintű felhasználó”. Ezeket a szinteket, ahogy már korábban említettem, a munkavállalókra alakították ki. Nem tartalmazza azt a szintet, amit gyermekekre vagy időskorúakra, esetleg olyan munkavállalókra lehet alkalmazni, akik most kényszerülnek arra, hogy digitális eszközöket használjanak a munkavégzésükhöz. Ezért az általam megalkotott VVSZM Digitális Kompetencia Keretrendszer esetében a korábbi fejezetben megfogalmazott és definiált besorolási szinteket használom. Az Európai Unió Digitális Keretrendszere által „Alapszintű felhasználónak” elnevezett szint az általam megalkotott Keretrendszerben a “Veszélyes” szintnek felel meg, míg a „Középszintű felhasználó” a “Szerény” szintnek, és a „Magas szintű” a “Magabiztos” szintnek felel meg. Új szintként jelent meg az általam megalkotott VVSZM Digitális Kompetencia Keretrendszerben a kezdő szint, amit én “Védendő” szintnek neveztem el [163][166].

6.4.1 A “Védendő” felhasználó

Tájékoztatás és adatfeldolgozás: Ezen a szinten a kezdő felhasználó nincs tisztában az internetes keresők használatával, nincs tudatában annak, hogy az internetes tartalmak nem mindegyike megbízható. A fájlokat és tartalmakat nem minden esetben tudja menteni vagy tárolni, és újra előhívni [163][166].

Kommunikáció és együttműködés: A felhasználó tud kommunikálni másokkal mobiltelefonon, azonban az azonnali üzenetküldő szolgáltatás, VoIP (pl. Skype), email vagy chat alapfunkciók használatával nincs tisztában. Önállóan nem tud fájlokat és tartalmakat megosztani. Nincs tisztában azzal, hogy különböző szolgáltatásokat vehet igénybe interneten keresztül. Ismer néhány közösségi oldalt, de egyedül nem tudja használni, vagy a bonyolultabb műveletekre nem képes. Csak fogalmi szinten van tudatában annak, hogy digitális eszközök használatakor bizonyos kommunikációs szabályokat be kell tartani [163][166].

Digitális tartalom létrehozása: A felhasználó csak segítséggel tud létrehozni egyszerű digitális tartalmat legalább egyféle formátumban, digitális eszközök használatával. Önállóan nem képes a mások által létrehozott tartalmat szerkeszteni. Csak fogalmi szinten van ismerete arról, hogy egyes tartalmak szerzői jogvédelem alatt állhatnak. Az általa használt szoftverekhez és

alkalmazásokhoz kapcsolódó egyszerű funkciókat és beállításokat csak korlátozottan tudja alkalmazni és módosítani [163][166].

Biztonság: Nem tudja önállóan használni az eszközei védelme érdekében a különböző védelmi megoldásokat. Csak részlegesen van tisztában azzal, hogy nem minden online információ megbízható. Csak fogalmi szinten van tudatában annak, hogy a személyes adatait ellophatják, de nem ismeri a védelmi módszereket. Hallott már arról, hogy online nem szabad megadni személyes adatot. Csak fogalmi szinten tudja azt, hogy a digitális technológia túlzott használata rossz hatással lehet az egészségre. Csak általános intézkedéseket tesz az energiatakarékosságért. Nincs tisztában azzal, hogy a saját személyes viselkedésén, fokozott figyelmén és határozott fellépésén múlhat az áldozattá válás elkerülése [163][166].

Problémamegoldás: Önállóan nem képes beazonosítani azt, ha egy technikai probléma történik. Önállóan nem kezd el használni egy új eszközt, programot vagy alkalmazást. Csak korlátozott ismeretei vannak azzal kapcsolatban, hogyan kell megoldani néhány egyszerű problémát. Részleges ismeretei vannak arról, hogy a digitális eszközök segítségére lehetnek a problémamegoldásban. Nincs minden esetben tisztában azzal, hogy vannak korlátai. Amikor technológiai vagy nem technológiai problémába ütközik, a megoldásukra korlátozottan tudja használni az általa ismert eszközöket. Nincs tudatában annak, hogy rendszeresen, újra és újra naprakésszé kell tennie a digitális készségeit [163][166].

Tudásátadási képesség: Csak minimális digitális tapasztalattal bír, valamint ismeretei hiányában nem képes azt megfelelően átadni. Mivel alacsony szintű a digitális tudása, ezért nincs tisztában azzal, hogy milyen viselkedési példával képes azt átadni [163][166].

6.4.2 A “Veszélyes” felhasználó

Biztonság: Részlegesen van tisztában azzal, hogy a saját személyes viselkedésén, fokozott figyelmén és határozott fellépésén múlhat az áldozattá válás elkerülése. Eseti jelleggel részt vesz információbiztonsági képzésen, oktatáson [163][166].

Tudásátadási képesség: Alapszintű a digitális tapasztalata, valamint az alapszintű ismeretei alapján képes azt korlátozottan átadni. Az alapszintű digitális tudása alapján inkább az ösztönös védelem jellemzi, alapszinten képes átadni a tudását viselkedési példával [163][166].

6.4.3 A “Szerény” felhasználó

Biztonság: Tetteiben proaktivitás mutatkozik annak érdekében, hogy saját személyes viselkedése, fokozott figyelme és határozott fellépése alapján megelőzze és elkerülje a digitális támadásokat, károkozásokat [163][166].

Tudásátadási képesség: Közepes szintű a digitális tapasztalata, valamint a közepes szintű ismeretei alapján képes azt hatékonyan átadni. A közepes szintű digitális tudása alapján a tudatos védelem jellemzi, közepes szinten képes átadni a tudását viselkedési példával [163][166].

6.4.4 A “Magabiztos” felhasználó

Biztonság: Tetteiben proaktivitás és kockázatértékelés mutatkozik annak érdekében, hogy a saját személyes viselkedése, fokozott figyelme és határozott fellépése alapján megelőzze és elkerülje, mind a maga, mind a környezete vonatkozásában a digitális támadásokat, károkozásokat. Rendelkezik azon ismeretekkel, amelyekkel egy folyamatban lévő digitális támadást, károkozást meg tud akadályozni vagy csökkenteni tudja annak kármértékét [163][166].

Tudásátadási képesség: Magas szintű digitális tapasztalattal bír, és ismeretei alapján képes azt magas fokon átadni. Mivel magas szintű a digitális tudása, ezért minden tettére a biztonságtudatos magatartás jellemző, követendő példakép a környezete számára [163][166].

6.4.5 Összegzés

Az általam megalkotott VVSZM Digitális Kompetencia Keretrendszer négy felhasználói szintet tartalmaz. A kérdőíves felmérésem alapján a felhasználók besorolására alkalmas szempontrendszert állítottam fel, melyben négy felhasználói szintet definiáltam. Az általam megállapított 4 szint lefedi és ebből egy új, a “Védendő” szint bevezetésével teljessé teszi az egész társadalom számára a digitális kompetencia keretrendszer alkalmazhatóságát. Ezzel a keretrendszerrel, ezen belül a megalkotott új szintjeivel könnyebben felmérhető a társadalom felhasználói összetétele, aminek segítségével könnyebb a tudásszint pontosabb és hatékonyabb a fejlesztése.

6.5 Összefoglalás

Kidolgoztam a magyar sajátosságokat is figyelembe vevő, a társadalmi rétegek mindegyikére alkalmazható VVSZM Digitális Kompetencia Keretrendszert, amelyhez az Európai Unió által kidolgozott keretrendszert és a digitális intelligenciában megfogalmazottakat vettem alapul. A társadalom sajátosságait figyelembe vevő digitális kompetencia értékelési rendszer

kidolgozásának elsődleges célja, hogy segítse a magyar gazdasági jólét szintjének emelését, annak fejlődését és a társadalom magasabb színvonalra történő mielőbbi felzárkózását. Továbbá biztosítsa a társadalom tagjainak a biztonságtudatossági szint növelését, amit a mindenki számára az újdonság erejével ható kibertér tesz szükségessé [163][166].

Az általam megalkotott VVSZM Digitális Kompetencia Keretrendszerrel hatékony képzési rendszert lehet kidolgozni, melynek alapja, hogy egy adott osztályba és szintbe besorolt felhasználóhoz igazodik és az ő hiányosságait pótolja. Különösen jól alkalmazható ez azokra a felhasználókra, akiket a "Védendő" szintbe lehet besorolni, és akik jelentős része (18-24 évesek és az ennél fiatalabbak) jelenleg még az oktatási rendszerben elérhetők. Az ő korosztályuknak a kompetenciájuk szintjéhez igazodó oktatás szükséges a fentiek alapján. [90]Az idősebb generációk esetében, akiket szintén a "Védendő" szinthez soroltam, ugyancsak növelni kell a kompetencia és a tudatosság szintjét, hogy ne szakadjon szét a társadalom, és a digitális kompetencia- és a biztonságtudatosság szintje közeledjen a magasabb csoportok szintjéhez. Továbbá szükséges olyan képzés, ami ehhez a szinthez van kidolgozva az életkori sajátosságoknak megfelelően.

Kidolgoztam és bemutattam új digitális kompetencia besorolási osztályokat, valamint egy új digitális kompetencia besorolási szintet, melyeket definiáltam. A VVSZM Digitális Kompetencia Keretrendszer újdonsága a korábbiakhoz képest az, hogy tartalmaz egy új besorolási szintet, amely a „Védendő felhasználó" elnevezést kapta, és egy új osztályt és alosztályokat. A korábban már meglévő „Biztonság" osztályon belül a „Biztonságtudatosság" új alosztály lett, valamint létrejött a „Tudásátadási képesség" új osztály és annak „A felhalmozott tapasztalat átadása" és „A megszerzett ismeretek átadása" valamint „A tudás átadása a saját viselkedésének és magatartásának példáján keresztül" neveket viselő új alosztályai.

Az általam kidolgozott VVSZM Digitális Kompetencia Keretrendszer segítségével a teljes társadalom felhasználóinak digitális kompetenciaszintjét a korábbiaknál pontosabban lehet besorolni, ami a képzés és az oktatás hatékonyságát növeli.

7 A DIGITÁLIS KOMPETENCIA HIÁNYOSSÁGAINAK KOMPENZÁLÁSA SZOFTVERERGONÓMIAI ESZKÖZÖKKEL

A mai digitális világban rengeteg információt kell feldolgoznunk nap mint nap. A biztonságunk ezeknek az információknak a gyors és pontos értelmezésén múlik. Amennyiben az információkat nem tudjuk megfelelő reakcióidőn belül feldolgozni, akkor esélyes, hogy olyan döntést hozunk, ami kihat a biztonságunkra. Az ábra alapú információfeldolgozás gyorsabb és egyszerűbb, mint a szövegesé. Ahogyan a közúti közlekedésben, úgy az infokommunikációs eszközök esetében is jól lehetne alkalmazni egy egyezményes jelzésrendszert. Kora gyermekkortól kezdődően, a közlekedési szabályok és a közlekedési jelzések oktatásának mintájára, ezeket az információs eszközök által használt jelzéseket is lehetne oktatni [90]. Az informatikai készségek és képességek szintje ez esetben alacsonyabb is lehet, ezért szélesebb társadalmi körben alkalmazható rendszert szükséges kidolgozni. Ez a megoldás az infokommunikációs eszközök használata esetében „akadálymentesítés" lehet minden felhasználó számára. De nagy segítséget tud nyújtani minden olyan felhasználónak is, akik valamilyen oknál fogva az átlagtól eltérő képességekkel rendelkeznek. Ilyenek például a gyengénlátók, az olvasási nehézséggel küzdők, az idegen nyelven nem beszélők, az időskorúak és azon gyermekkorúak, akik korukból adódóan olvasni még nem tudnak [91]. A felhasználást tekintve számos olyan környezetben is alkalmazható, ahol gyors, azonnali döntésre van szükség. Ilyen lehet a rendvédelmi, a mentés-irányítási, katasztrófavédelmi és katonai alkalmazás, ahol adott esetben egy többnemzetiségű művelet zajlik [92]. Szabványok alkalmazásával kialakítható egy olyan ábrázolási rendszer, aminek segítségével az infokommunikációs eszközöket használók széles köre biztonságban érezheti magát [93]. Ebben a részben egy egyszerű felmérés alapján mutatom be, milyen és mekkora különbség van a képi és szöveges információk feldolgozásának hatékonysága között, valamint ajánlásokat teszek a digitális kompetenciai területén meglévő hiányosságok szoftver-ergonómiai kompenzálására [156][157][158][159].

7.1 Az információ áramlása és feldolgozási sebessége

A modern kori információtovábbítás sebessége és mértéke az elmúlt 100-150 évben jelentősen felgyorsult az addig megszokotthoz képest. Ugyanis az azt megelőző időszakban a tömegtájékoztatás és az információ nagyon szűk kört ért el, vagy jelentősen torzult az információ, mire az emberekhez elért. Az ennél korábbi időszakot a nyomtatott sajtótermékek

és könyvek jellemezték. Az írástudatlanoknak, akik nagy számban voltak jelen a társadalomban, a hivatalos tájékoztatást Magyarországon például az úgynevezett „kisbíró” rendszer biztosította, akik „kidobolták” az aktuális tudnivalókat. Az egységes Morse távíró és a Morse kód (szabadalmaztatva: 1837) használatával az információk már nagy sebességgel, gyorsan terjedtek a kiépített infrastruktúrán. A telefon feltalálását (szabadalmaztatva: 1876) követően és a magyar vonatkozású, Puskás Tivadar tervei alapján megépített telefonközpontok (Boston, 1878) és azok különböző szolgáltatásai révén, mint például a telefonhírmondó (szabadalmaztatva: 1892), már széles körben lehetett az információt gyorsan és fogyasztható formában eljuttatni az emberek számára [94][95][96]. Majd megjelentek a Tesla-Marconi-Popov nevéhez köthető első szikratávírók az 1900-as évek elején, melyek már rádióhullámok segítségével továbbították az információt [97]. Ennek köszönhető például, hogy az 1920-as években indultak el az első kereskedelmi rádiók – Budapesten 1925-ben –, amelyek már széles körben szinte mindenki számára tudtak információt szolgáltatni. Ez teljesen átformálta a tömegtájékoztatást, az információtovábbítást. A fényképészet megszületésével (Francia Akadémia, 1839) az információk képalkotási technológiák által történő rögzítése és továbbítása segítette a nyomtatott információk útján történő információtovábbítást [98]. A mozgóképrögzítés, (szabadalmaztatva: 1895) majd a filmszínházak elterjedése (Budapesten az első nyilvános filmvetítés 1896-ban volt) és a technológia fejlődése, a színes filmek (az első színes film vetítése 1917-ben volt), majd a hangosfilmek (az első hangosfilmet 1927-ben vetítették) esetében elsősorban a szórakoztatás volt a legfontosabb cél, ami mellett a hírközlés és a dokumentálás is szerepet kapott [99]. A televízió elterjedése (Németország 1935, Magyarország 1954-től kezdeti tesztidőszak, majd 1957-től műsorszórás) már sokkal szélesebb rétegek számára biztosította az információhoz való hozzáférést. Az informatika, ami a különböző eszközökkel – de különösen a számítógéppel – megvalósított információkezeléssel, azaz az információ megszerzésével, gyűjtésével, feldolgozásával, tárolásával, sokszorosításával és továbbításával foglalkozik, az 1940-es évektől történő robbanásszerű fejlődése és töretlen népszerűsége által a társadalmi berendezkedést is megváltoztatta [100][169][171].

A tudásalapú társadalom információéhsége

Már nem ipari társadalmakról, hanem tudásalapú- és információs társadalmakról beszélünk. A számítógép elveinek Neumann János nevéhez kötődő lefektetése (USA, 1945) és az elektronikus számítógép megalkotása (EDVAC, 1949) nagyban hozzájárult ahhoz, hogy ma a teljes életünket behálózza az informatika és az információs technológia [101]. A személyi

számítógépek (PC), az operációs rendszerek, az internet és szolgáltatásai a különböző eszközök segítségével a teljes társadalom számára elérhetővé váltak. A világon jelenleg közel 3,5 milliárdan érik el az internetet és ebből 2,3 milliárd ember tartozik valamilyen közösségi portálhoz. Az emberiség 2007-ben egy év alatt 1,5 Exabájt (1,5x1018) digitális adatot hozott létre, ami megegyezik azzal az információmennyiséggel, amit addig 5000 év alatt állított elő. Mindezt 1 Terrabit/sec sebességű hálózaton tudtuk továbbítani. Napjainkban az információ előállításának mennyisége és annak továbbítási sebessége messze túllépte a tíz évvel korábbit. Jelenleg 2,5 Exabájt adat keletkezik naponta (!) és 43 Terrabit/sec adattovábbításra vagyunk képesek. Érdekesség, hogy ezen a sebességű hálózaton egy HD minőségű mozifilmet 0,2 másodperc alatt lehet letölteni. Az emberiség jelenleg 150 millió iPhone telefont és 5 millió laptopot használ. A szélessávú internetet az internetfelhasználók 93%-a veszi igénybe, az USA-ban 99,73% a lefedettség. Jól látható, hogy a mai világunkban az információhoz való hozzáférés bárki számára gyorsan és egyszerűen rendelkezésre áll [102][169][171].

7.2 Az információ feldolgozásának problémája, mint biztonsági kihívás

Az informatikai eszközök megjelenítő felületét nézve vizuális és audiovizuális formában férünk hozzá az információkhoz. Szövegek, képek, hanganyagok és videók formájában áll rendelkezésünkre az információ [103]. Az információt megjelenítő elektronikus eszközök „kommunikálnak” velünk. Ami azt jelenti, hogy különböző üzenetek formájában döntést várnak vagy tájékoztatják a felhasználót. A felhasználó döntését hajtják végre az előre definiált módon. Ezek általában úgynevezett felugró ablakok segítségével történnek [104]. Ahhoz, hogy a felhasználó a döntését meghozza és az üzenetben a részére felajánlott parancsot kiadja, előtte tájékozódnia szükséges [105]. A tájékoztató információ általában a felugró ablakban található meg. Jelenleg ezek az információk általában szöveges formátumban állnak rendelkezésre [106]. A szöveges üzenetek jó esetben a felhasználó saját anyanyelvén, de rosszabb esetben idegen nyelven tájékoztatják a felhasználót [107]. Előfordulhat az is, hogy bár a felhasználó anyanyelvén kapja a tájékoztatást, de adott esetben azért nem érti a szakkifejezéseket, mert nincs olyan szintű szakmai ismerete vagy azért, mert az általános műveltsége és az írás-olvasási kompetenciája alacsony szintű, vagy egyáltalán nem tud olvasni (például még nem iskoláskorú gyermek), analfabéta [108]. De az is elképzelhető, hogy olvasási nehézsége van, ami jelenleg nagy számban előforduló jelenség. Az az eset is lehetséges, hogy látás élesség hiányában, segédeszköz (szemüveg, kontaktlencse) nélkül nem tudja pontosan elolvasni az adott üzenetet [163]. Ebben az esetben a felhasználó a tájékoztatásban szereplő információhoz nem fér hozzá vagy nem érti meg azt. Ez kritikus szintű biztonsági probléma [109]. Legalább olyan szintű,

mint például az autóvezetés esetében a közlekedési táblák, lámpák jelzéseinek nem megfelelő ismerete vagy téves értelmezése [110][169][171].

7.3 Jogszabályok, ajánlások és szabványok az akadálymentesítésről és a szoftverergonómiáról

A felhasználók biztonságos eszköz- és internethasználatának növelése érdekében az alábbiakban bemutatom az általam felkutatott és hipotéziseim bizonyítása során figyelembe vett jogszabályokat, ajánlásokat és szabványokat.

7.3.1 Jogszabályok és nemzetközi ajánlások az akadálymentesítéssel kapcsolatban.

Az alábbiakban a nemzetközi ajánlásokat és a hazai jogszabályokat mutatom be, a kutatásom eredménye alapján az alábbiakban leírt digitális akadálymentesítési javaslatom jogi oldalról történő megerősítése céljából.

- A fogyatékossággal élő személyek jogairól szóló ENSZ egyezmény

A magyar Országgyűlés a 2007. évi XCII. törvényben [136] hirdette ki azt az ENSZ által megfogalmazott egyezményt, mely többek között kimondja, hogy a fogyatékossággal élő emberek hátrányos megkülönböztetése az emberi méltóság súlyos megsértése. Az Egyezmény 9. cikke kimondottan megköveteli, hogy a részes államok biztosítsák, hogy a fogyatékossággal élő személyek másokkal teljesen egyenlő alapon, akadálymentesen férjenek hozzá az új információs és kommunikációs technológiákhoz, beleértve az internetet is. Az akadálymentes hozzáférés hiánya ugyanis meggátolhatja a fogyatékossággal élőket abban, hogy teljeskörűen élvezzék emberi jogaikat.

- Az Európai Unió Alapjogi Chartája

Az Európai Unió Alapjogi Chartájának az Egyenlőségről szóló címéhez [137] tartozó 21. és 26. cikke értelmében **tilos a fogyatékosság alapján történő megkülönböztetés**, illetve el kell ismerni és tiszteletben kell tartani a fogyatékkal élő személyek jogát a beilleszkedésre.

- Magyarország Alaptörvénye

Magyarország Alaptörvénye [138] szerint Magyarország az alapvető jogokat mindenkinek bármely megkülönböztetés, így például fogyatékosság szerinti különbségtétel nélkül biztosítja. Magyarország az esélyegyenlőség megvalósulását külön intézkedésekkel segíti.

- A fogyatékos személyek jogairól és esélyegyenlőségük biztosításáról szóló törvény

Az Alaptörvénnyel és a nemzetközi jog szabályaival összhangban álló, a fogyatékos személyek jogairól és esélyegyenlőségük biztosításáról szóló 1998. évi XXVI. törvény [139] alapján a fogyatékos személynek kikényszeríthető (alanyi) joga van a közérdekű információkhoz való hozzáférésre, valamint a közszolgáltatásokhoz való egyenlő esélyű hozzáférésre.

- Az egyenlő bánásmódról és az esélyegyenlőség előmozdításáról szóló törvény

Habár az Alaptörvényre és a nemzetközi jog szabályaira tekintettel meghozott 2003. évi CXXV. törvényben [140] közvetlenül nem szerepel nevesítve az infokommunikációs esélyegyenlőség, áttételesen mégis szerepel benne például azokon a szolgáltatásokon keresztül, amelyeket az interneten keresztül is nyújtanak.

- A közérdekű adatok elektronikus közzétételére vonatkozó kormányrendelet

A 305/2005. (XII. 25.) korm. rendelet [141] érdekessége, hogy jól ábrázolja, mit is ért a jogalkotó egy honlap akadálymentessége alatt. A rendelet alábbi pontja a következőket tartalmazza:

„5.§ (3) A közzétételre szolgáló honlapot úgy kell kialakítani, hogy az a széles körben elterjedt, valamint a vakok és gyengénlátók által széles körben használt eszközökkel is olvasható legyen.”

7.3.2 Az akadálymentesítésre vonatkozó szabványok

Az alábbi részben azokat a nemzetközi szabványokat kívánom bemutatni, amelyek a honlapok akadálymentesítésére vonatkoznak, és a bennük foglaltak a digitális akadálymentesítési tervezetem kidolgozását segítik.

- WCAG 2.0 (ISO/IEC 40500:2012) szabvány

A W3C által összeállított WCAG 2.0 web akadálymentesítési útmutató sokáig csak iparági ajánlás volt, de a szakma mindig, de-facto szabványként tekintett rá. Aztán 2012 októberében a nemzetközi szabványügyi testület ISO/IEC 40500:2012 [142] számon nemzetközi szintű hivatalos (de-jure) szabvánnyá emelte. Eddig egy olyan hatályos magyar jogszabály volt életben, amiben konkrétan a WCAG 2.0 ajánlásra hivatkoznak, ez a 62/2011. (XI. 10.) NEFMI rendelet [143].

- MSZ EN 301 549:2014 szabvány

Az „Európai közbeszerzési ICT-termékek és -szolgáltatások hozzáférhetőségi követelményei” címmel közzétett szabvány az első olyan európai és magyar szabvány, [144] amely az infokommunikációs technológiák akadálymentességét írja le. Célja, hogy a közbeszerzésekben érdekelt felek erre a szabványra hivatkozhassanak a digitális eszközök, weboldalak, szoftverek akadálymentességének biztosítása során.

7.3.3 Szoftver-ergonómiára vonatkozó szabvány, avagy ISO 9241

Ez a szabvány támpontokat ad a fejlesztőknek ahhoz, hogy ergonomikus rendszert tudjanak létrehozni. Az ISO 9241-es szabvány célja a képernyős munka jó ergonómiai kialakításának előmozdítása és annak biztosítása, hogy a képernyős berendezések alkalmazói ezeket megbízhatóan, eredményesen, hatékonyan és kényelmesen kezelhessék. Az ISO 9241 foglalkozik a hardver, szoftver és környezetük jellemzőire vonatkozó azon követelményekkel és javaslatokkal, amelyek hozzájárulnak a használhatósághoz, illetve harmonizálnak az ergonómiai elvekkel [111][169][171].

- ISO 9241-1 (1997): Általános bevezetés

A bevezető rész információkat tartalmaz az ISO 9241-ről, és áttekintést ad a szabvány első hat részéről. Felsorol néhány olyan IEC-szabványt, amelynek a biztonsági szempontok megértéséhez hasznosak, és megmagyarázzák a használati minőségre irányított megközelítésmódot, amely az ISO 9241-re érvényes. Néhány segédletet ad arra vonatkozóan, hogyan kell az ISO 9241-et alkalmazni [145].

- ISO 9241-11 (1998): Használhatóság

A használhatóságra vonatkozó tanács magyarázza azt a módot, amelyben a felhasználót, a felszerelést, a feladatot és a környezetet az egész rendszer részeként kellene leírni, és megadja, hogy melyik használhatóságot lehet előírni és értékelni [146].

- ISO 9241-13 (1998): Felhasználói támogatás

Javaslatokat ad a felhasználói interfészek tervezéséhez és értékeléséhez (prompt-ok, visszajelzés, állapot, online segítség és hibakezelés) [147].

- ISO 9241-14 (1997): Menürendszerek

A javaslatok tartalmazzák a menü szerkezetét, a navigálást, választási lehetőségeket és végrehajtást, és a menü ábrázolását (különböző technikákkal, például ablakozás, panelek, gombok, mezők stb.) [148].

- ISO 9241-15 (1997): Parancsdialógusok

Tartalmazza a parancsnyelv szerkezetét és szintaxisát, a parancs ábrázolását, az adat bekérésére és az eredményre vonatkozó szempontokat, a visszacsatolást és a segítséget [149].

- ISO 9241-16 (1999): Közvetlen manipulációs dialógusok

Tartalmazza a tárgy kezelését, a hasonlatok, az objektumok és a jellemzők tervezését. A grafikus felhasználói felület azon részeivel foglalkozik, amelyek közvetlenül vannak irányítva, és amelyeket az ISO 9241 más részei nem tartalmaznak. A szabvány a következő ajánlásokat tartalmazza: általános információk, szöveges objektumok direkt manipulációja, ablakok direkt manipulációja, irányító ikonok direkt manipulációja [150].

- ISO 9241-110 (2006) A párbeszédekre vonatkozó elvek

Az ember-számítógép párbeszéddel kapcsolatban alapelveket fogalmaz meg, s az egyes alapelvekhez konkrét alkalmazási ajánlásokat rendel, például a feladatra való alkalmasság, önmagáért beszélő legyen, kontrollálhatóság, a felhasználók elvárásainak való megfelelés, hibatűrés, testreszabhatóság, tanulhatóság [151].

- ISO 9241-112 (2017) Az információk bemutatásának elvei

Az interaktív rendszerek ergonomikus tervezési elveit határozza meg, amelyek a szoftveres információk megjelenítéséhez kapcsolódnak, például a felhasználói felület tervezők, a fejlesztők, az értékelők, a fejlesztési folyamatok irányításáért felelős projektvezetők és a vásárlók részére [152].

- ISO 9241-125 (2017) Az információ megjelenítése

Az információmegjelenítésről három témakör számos alpontjában fogalmaz meg ajánlásokat, ezek az információszervezés, a grafikus objektumok és a kódok alkalmazása [153].

- ISO 9241-302 (2008): A vizuális megjelenítések terminológiája

A vizuális kijelzőkre és azok arculatára vonatkozó követelményeket írja elő. Felsorolja a képernyőnek azokat a jellemzőit, amelyek az észlelési és felismerési teljesítményt befolyásolják. A szabványban tervezési útmutatás is található. A szabvány a következő elemekre ír elő követelményeket: monitortávolság, látásvonal szöge, látószög, karaktermagasság, vonalvastagság, a karakterek szélesség/magasság aránya, rasztermoduláció és kitöltési tényező karakterformátum, karakter-nagyság egyenletessége, karaktertávolság, szóköz, sortávolság, linearitás, derékszögűség, a képernyő fényereje, fényerőkontraszt, fényerő kiegyensúlyozás, káprázás, képpolaritás, fényerő-egyenlőség, fényerő kódolás, villanáskódolás, időbeli instabilitás (villogás), helyi instabilitás (vibrálás) és képernyőszín [154].

- ISO 9241-305 (2008) A színábrázolásokra vonatkozó követelmények

A specifikáció lefedi a következőket: alapértelmezett színkészlet, színegységesség, karaktermagasság és objektumméret, színeltérések, a szimbólumok és karakterek olvashatóságának kontrasztja, spektrálisan különleges színek, háttér és a körülvevő képi hatások és a színek száma [155][169][171].

7.3.4 Összegzés

A felhasználók részére történő segítségnyújtás az üzemeltetésben a biztonságot is növeli. Ha a felhasználó nem magabiztosan üzemelteti az eszközét, abban az esetben nő a kockázat és csökken a biztonsági szint. Az általam megállapított felhasználói szempontrendszer és a VVSZM Digitális Kompetencia Keretrendszer segítségével beazonosított felhasználói csoportok közül különösen a „Védendő” csoport tagjai számára szükséges olyan megoldást találni, aminek a segítségével lehetséges növelni a biztonságot és csökkenteni a kockázatot.

7.4 Az információ-feldolgozási probléma szoftverergonómiai megoldásának vizsgálata

Ezek a biztonsági problémák olyan kihívások, amelyek megoldása égetően szükséges. Ugyanis ma már nagyon sok ember számára elérhető az internet, nagyon sokan rendelkeznek olyan mobil eszközzel, amivel valamilyen formában elérhetik az internetet. A korábbi felmérésemből kitűnik, hogy a felhasználók nagy számban nem alkalmaznak biztonsági szoftvereket, nem készítenek biztonsági mentéseket [163]. Ezek figyelembevételével a felhasználók jelentős része kiszolgáltatott az internetes veszélyeknek. Az ok, hogy miért nem használnak megfelelő

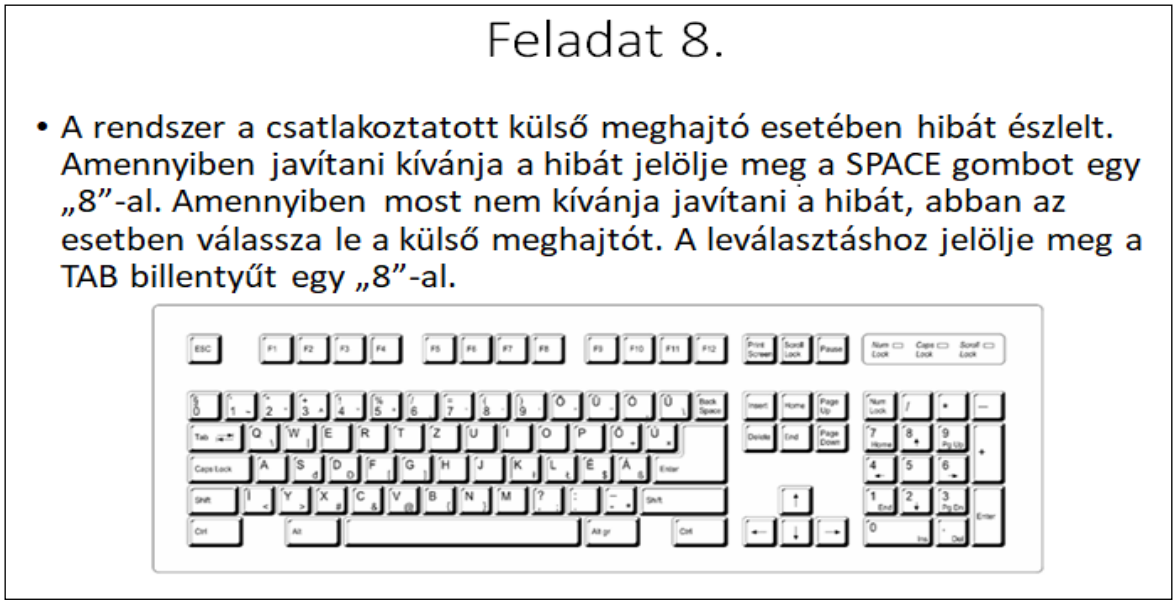
védelmi alkalmazásokat vagy miért nem készítenek biztonsági másolatot, az vagy a szükséges ismeret és tájékoztatás hiányából vagy technikai nemmegfelelőségből adódik [112][169][171].

7.4.1 A szöveges üzenet a piktogramos üzenettel összevetve

Azonban a felhasználók részére, a korábban említett problémát szem előtt tartva – ami a szöveges felugró üzenetek nem megfelelő kezeléséből adódó biztonsági rés – valamilyen formában biztonságos megoldást kell találni. Ennek a problémának a megoldására a már említett közlekedési tábla, mint nemzetközileg egységes és elfogadott jelzésrendszer mintájára, szükséges lenne kidolgozni egy olyan piktogram rendszert, aminek alkalmazásával a felhasználók számára egy-egy adott üzenet sokkal egyértelműbben megérthető lenne, mint szöveges formában [169][171]. Gyerekekkel végzett felmérés bizonyítja, hogy a gyerekekben félelmet, ijedtséget válthatnak ki a felugró szöveges ablakok, emellett az üzenetek megértéséhez, értelmezéséhez, valamint a válaszadáshoz időre lenne szükségük [113].

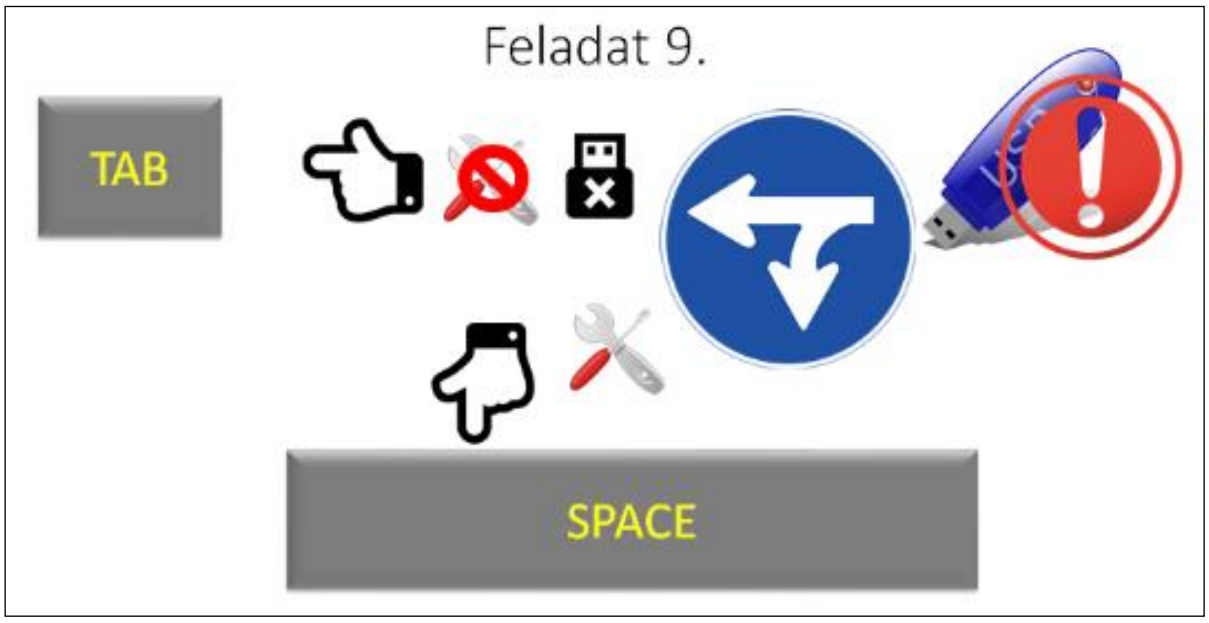
7.4.2 A tesztfeladat kidolgozása

Azt a hipotézist – hogy a felugró szöveges üzenetekkel szemben a piktogramos üzenetek értelmezése egyszerűbb rövid reakcióidő esetén – csakis egy kutatás lefolytatásával lehet alátámasztani. A kutatás egy, a felhasználók önkéntes és anonim bevonásával végzett kísérlettel indult. A kísérlet két fázisból áll.



70. ábra A szöveges feladatsor egyik feladata (forrás: saját készítésű tesztfeladat; készítette a szerző)

Elkészítettem egy olyan mintafeladatsort, ami fiktív felugró üzeneteket tartalmaz egyszer szöveges formában (70. ábra), valamint ugyanennek az általam összeállított piktogramos változatát (71. ábra).



71. ábra A piktogramos feladatsor egyik feladata (forrás: saját készítésű tesztfeladat; készítette a szerző)

A feladatsorokat egy-egy MS PowerPoint diasorba foglaltam. A diasorok 10-10 feladatot tartalmaznak a fentieknek megfelelően annyi különbséggel, hogy a feladatok nem egyformán követik egymást a két diasorban. A diasor egy-egy diája egy-egy végrehajtandó feladatot tartalmaz, amit úgy állítottam be, hogy az 5 másodpercenként automatikusan cserélje a diákat [169][171].

7.4.3 A tesztfeladat elgondolása

A feladatsorokhoz készítettem egy-egy papíralapú feladatlapot, ami tartalmazza a feladat végrehajtásának leírását és egy számítógépes klaviatúrának a rajzát (72. ábra).


Szoftverergonómia vizsgálati feladatok válaszok (szöveges)

1.0a

Nyikes Zoltán doktorandusz

nyikes.zoltan@bgk.uni-obuda.hu

Kedves Válaszadó!

Először is köszönöm, hogy a feladat kitöltésével hozzájárul a doktori kutatásaimhoz. A feladat végrehajtása kb. 2 percet vesz igénybe. Kérem, hogy a prezentációban megjelenő információk alapján cselekedjen és az alábbi billentyűzeten jelölje be az adott feladatban megadott billentyűt.

Fontos! A billentyű megjelölésének módja esetében kérem, hogy tollal és a **feladat sorszámával jelölje.** A prezentációk **5 másodpercenként** váltják egymást. Önnek ennyi ideje van a feladatot értelmezni és végrehajtani. A feladat végrehajtása anonim módon történik.

A feladat végrehajtását köszönöm! Jó munkát! 😊

72. ábra A szöveges feladatsor papíralapú feladatlapja (forrás: saját készítésű tesztfeladat; készítette a szerző)

A két feladatsorhoz tartozó feladatlap csak a címben tér el egymástól, amiben az egyiket „szöveges”, a másikat „piktogramos” felirattal láttam el, hogy meg lehessen különböztetni a kiértékelésnél a feladatlapokat. A feladatok mindegyikében egy-egy, a valósághoz közeli feladatot kell megoldani, mint például vírus észlelése esetén, annak megakadályozása céljából adott billentyűt kell megjelölni a feladatlapon. A mintafeladatokat a rendszerhiba, a vírusveszély, a biztonsági mentés és az e-mail küldés témáiban fogalmaztam meg [169][171].

A 10 feladat közül 3 esetében nem csak egy lehetőség van, hanem ott választani is lehet. Például a biztonsági mentést melyik meghajtóra készítse el, ebben az esetben három betűjel közül lehetett választani. A másik feladatnál a rendszer figyelmeztet, hogy az e-mailt vagy csatolmány nélkül küldjük el, akkor egy adott billentyűt kell megjelölni, vagy csatolmánnyal, de ilyenkor egymás után két billentyűt kell megjelölni. A harmadik esetben egy egyszerű két választási lehetőséggel bíró üzenet jelenik meg, elfogadáskor az egyik billentyűt kell megjelölni, elutasításkor egy másikat. Minden egyes feladatnál más és más billentyűt kellett megjelölni a feladat végrehajtójának amiatt, hogy ne fordulhasson elő az, hogy a kiértékelésnél nem állapítható meg a pontos válasz. A feladatok sorszámának megfelelő (arab) számot kellett a végrehajtás során a klaviatúra adott billentyűjére tenni tollal. A piktogramos diasorok esetében a figyelemfelhívásra vagy a veszélyhelyzetre történő utalásra minden esetben a közúti közlekedésben használt jelzőtábla jelét alkalmaztam. A megjelölendő billentyű, billentyűkombináció a dián megközelítőleg úgy volt elhelyezve, mint ahogy az a valóságban is elhelyezkedik a klaviatúrán. Olyan klaviatúra jeleket használtam, melyek az általánosan használt 101 gombos klaviatúra esetében előfordulnak és általában azonos helyen helyezkednek el [169][171].

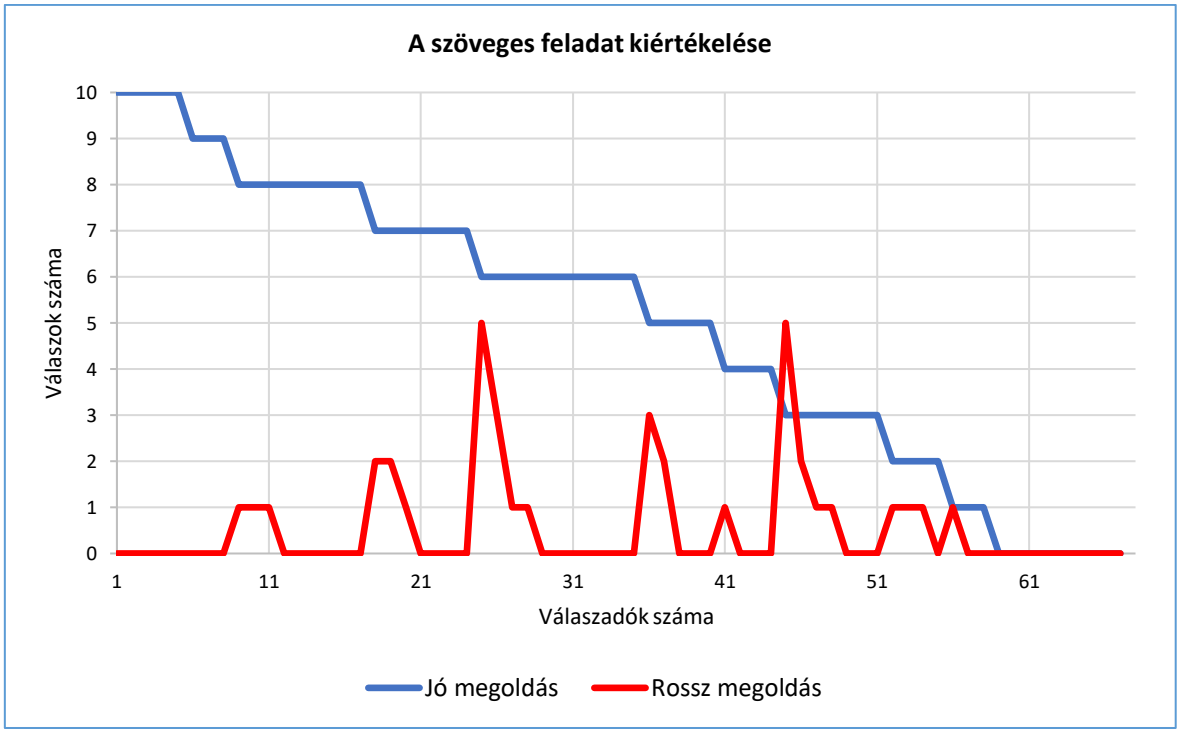
7.4.4 A tesztfeladat végrehajtása

Az előzetes kísérletet egy 67 fős, nappali és levelező tagozatos MSc-s és BSc-s hallgatókból álló csoporttal folytattam le. Először a szöveges feladatsort kellett végrehajtaniuk, majd a piktogramosat, külön-külön feladatlapra. A kapott eredményt kiértékeltem, aminek az eredményét a későbbiekben tárgyalom. Az értékelési szempontok a következők voltak. A 10 kérdésre 10 jó választ lehetett adni. A végrehajtás esetében jó válasznak számított a feladatban megadott billentyű jelének megjelölése. Amennyiben egy feladatban több billentyűt is meg lehetett jelölni, de a feladat szempontjából csak egyet, vagy csak egy billentyűkombinációt kellett, és a válaszadó többet is megjelölt a lehetőségekből, abban az esetben azt hibaként értékeltem. Továbbá hibának számított az értékelés során a téves billentyű megjelölése is. Nem tekintettem hibának azt, ha a feladatnak megfelelő billentyűt jelölte meg a válaszadó, de nem a

korábban említett, a feladat sorszámának megfelelő számjeggyel, hanem bármilyen más jelöléssel. Ezt nem is értékeltem külön [169][171].

7.4.5 A kapott eredmények kiértékelése

A szöveges feladatsor kiértékelése esetében jól látható, hogy csak 5 kitöltés lett 100%-os és hibátlan (73. ábra).

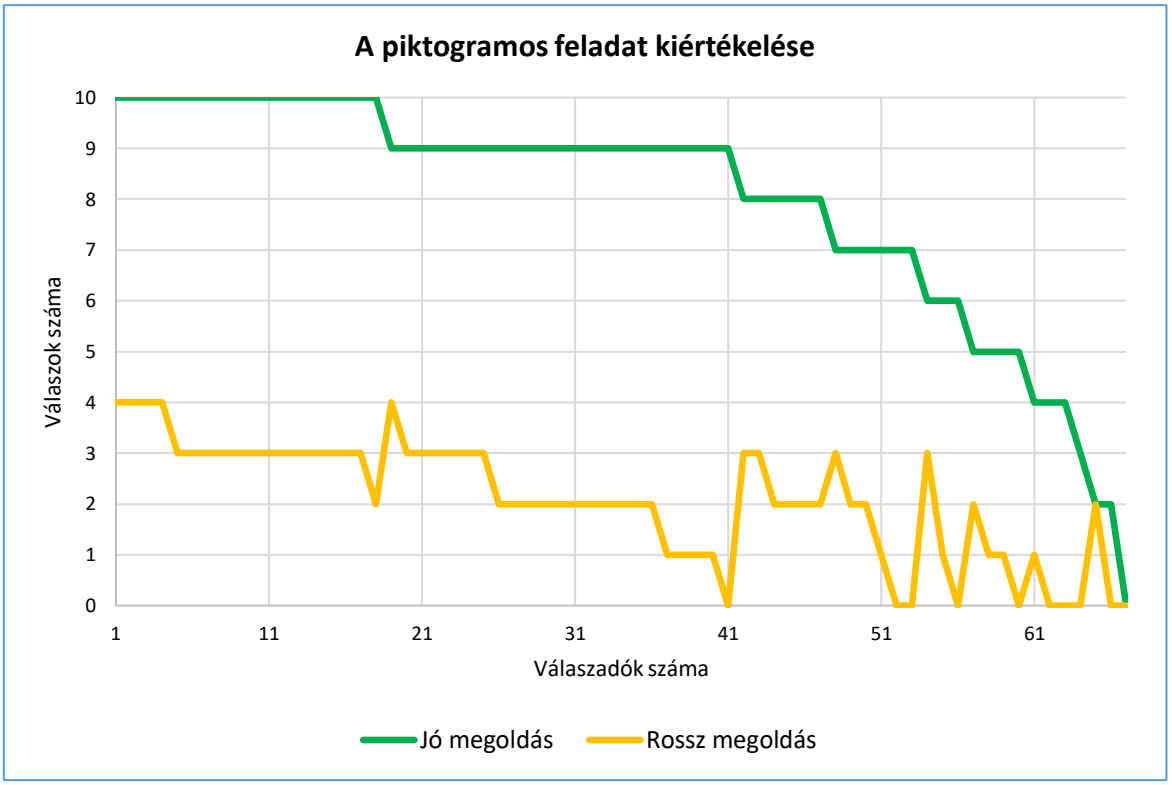


73. ábra A szöveges feladat kiértékelésének diagramja (forrás: saját készítésű tesztfeladat; Készítette a szerző)

90%-os eredményt csak 3 válaszadónak sikerült elérnie, amiből mind hibamentes volt. 80%-os jó eredményt viszont 9 válaszadó ért el, itt már csak 6 válaszadónak volt hibamentes a feladata. 70%-os eredményt 7 válaszadó esetében lehetett mérni, amiből csak 4 válaszadónak nem volt hibája. 60%-os eredmény 11 válaszadó esetében volt, amiből 7 válaszadó esetében volt hibátlan [169][171].

Az ábrából jól látszik, hogy a szöveges feladat esetében minimum 50%-os és e feletti eredményt összesen 40 válaszadónak sikerült elérni, ami a válaszadók közel 60%-át jelenti. Látható, hogy 9 válaszadó volt, aki valami oknál fogva nem adott semmilyen választ, ez a válaszadók közel 13%-a volt.

A piktogramos feladatsor kiértékelése esetében megfigyelhető, hogy 18 kitöltés lett 100%-os, ebből sajnos minimum 2 hiba is volt 1 kitöltés esetében, a többi esetben ennél több volt (74. ábra).

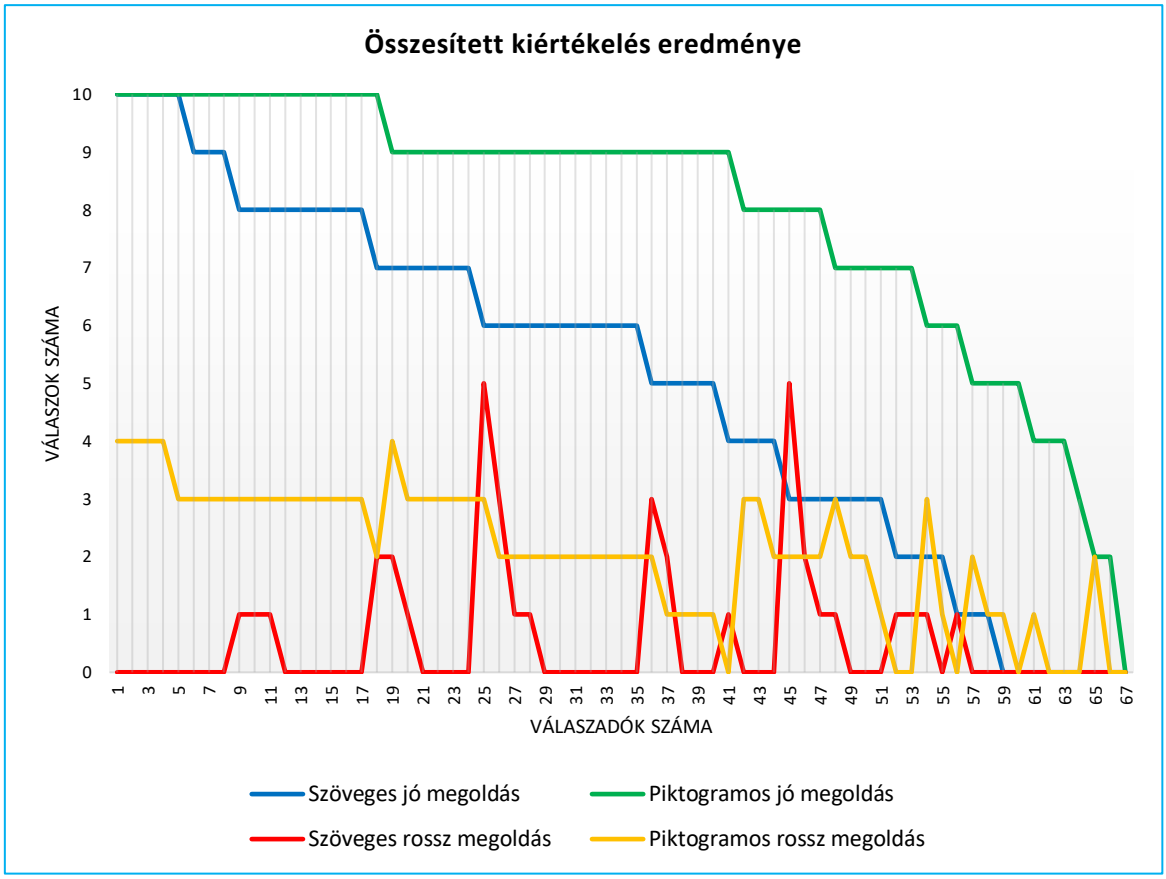


74. ábra A piktogramos feladat kiértékelésének diagramja (forrás: saját készítésű tesztfeladat; Készítette a szerző)

A 90%-os jó eredményt 23 válaszadónak sikerült elérnie, viszont itt is csak 1 válaszadónak volt hibátlan feladata, a többinek voltak hibás jelölései. Az ábrából látható, hogy minimum 50%-os és e feletti eredményt összesen 60 válaszadónak sikerült elérni, ami a válaszadók 89%-át jelenti. A válaszadók közül ebben a feladattípusban 1 válaszadótól kaptam vissza olyan feladatlapot, amin nem volt válasz. Látható, hogy 10 válaszadó volt, aki nem adott rossz választ, ez a válaszadók közel 15%-át jelenti.

Az összesített eredményből (75. ábra) egyértelműen kitűnik, hogy a szöveges és piktogramos feladatok eredményességét tekintve sokkal jobb eredmények születtek a piktogramos feladat esetében. A feladatokat ugyanannyi egységidő alatt hajthatták végre. Ez azt jelenti, hogy a szöveges feladatot nem értették meg olyan gyorsan, mint a piktogramosat.

A hibásan megoldott feladatok esetében vélelmezem azt, mivelhogy a piktogram- és jelölésrendszer még nincs kialakítva, ezért a válaszadók nem tudták pontosan értelmezni az eldöntendő feladatokat, így minden gombot megjelöltek, ami a feladatban fel volt tüntetve. A piktogramos feladatok rossz válaszai szinte mind az eldöntendő kérdések esetében születtek, mert megjelöltek többet is a feltüntetettek közül. Míg a szöveges feladatok esetében a rossz válaszoknál olyan gombokat is megjelöltek, amelyek nem voltak feltüntetve [171].



75. ábra Az összesített kiértékelés diagramja (forrás: saját készítésű tesztfeladat; Készítette a szerző)

7.4.6 Összegzés

Kidolgoztam egy tesztfeladatsort, aminek a segítségével végrehajtottam a kutatást. Az ennek a kiértékeléséből kapott eredmények bizonyítják, hogy a felhasználók pontosabb információfeldolgozásra képesek, amennyiben az informatikai eszközük szöveges üzenetek helyett piktorgramos üzenetek segítségével kommunikál velük. A fenti eredmények alapján bizonyítottam, hogy a felhasználók biztonsága növelhető az általam kidolgozott megoldás használatával, ezáltal a kockázat is jelentősen csökkenthető. Kutatásomban a szöveges üzenetek mellett vagy azok helyett alkalmazandó piktogramos tesztüzenetek kidolgozásánál figyelembe vettem az aktuális szoftverergonómiai szabványokat. A tesztfeladatok kiértékeléséből kirajzolódik, hogy a felhasználók jelentős hányada a piktogramos feladatok legalább felét jól oldotta meg, ami mintegy 30%-kal volt több, mint a szöveges feladatok esetén. Továbbá a feladatot végrehajtók százalékos eloszlása azt is mutatja, hogy amíg a szöveges feladatokra a válaszadók 13%-a nem válaszolt egyáltalán, addig a piktogramosok esetében a válaszadóknak csak kevesebb, mint 1%-a nem válaszolt. Ennek a magas számnak köszönhetően bizonyítható, hogy a hipotézisem alátámasztott.

7.5 Összefoglalás

A biztonsági szint jelentősen csökken, a kockázat pedig nő abban az esetben, ha a felhasználó nem magabiztosan üzemelteti az eszközét. Az általam kidolgozott felhasználói szempontrendszer és a VVSZM Digitális Kompetencia Keretrendszer segítségével lehetséges növelni a biztonságot és csökkenteni a kockázatot a beazonosított felhasználói csoportok esetében. Különösen a „Védendő" csoport tagjai számára szükséges megfelelő megoldást találni.

Kutatást végeztem annak a hipotézisemnek az igazolására, hogy a piktogramos üzenetek alkalmasak a felhasználói biztonság növelésére (ami nevezhető akadálymentesítésnek is) gyors döntéseket igénylő helyzetekben. Tesztfeladatsort készítettem és töltettem ki átlag felhasználókkal, melynek eredményeit értékeltem. A piktogramos feladatokat a felhasználók gyorsabban és pontosabban oldották meg, mint a szöveges feladatokat azonos idő alatt, annak ellenére, hogy ezeket a piktogramos üzeneteket a kísérletben részt vevők soha nem látták még korábban.

A piktogramos feladatok kidolgozása során figyelembe vettem az szoftverergonómiára, valamint a kibertér akadálymentesítésére vonatkozó szabványokat és ajánlásokat. A mindennapi életben alkalmazott piktogramokat is felhasználtam a feladatok elkészítésekor. A felhasználók biztonságát növeli az üzemeltetésben történő segítségnyújtás. Az általam kidolgozott szoftverergonómiai alkalmazás megoldási javaslatot ad az információfeldolgozási és felhasználói reakció biztonsági kihívásaira, amely hosszútávon biztosan, de rövid és középtávon is előrelépést jelenthet a felhasználói biztonságban. A bemutatott kutatás alapján bizonyítottam, hogy a felhasználó ábraalapú információfeldolgozása gyorsabb és egyszerűbb, mint a szövegesé. Javaslom, hogy a közúti közlekedésben alkalmazott egységes, nemzetközi jelrendszer alapján kerüljön kidolgozásra az infokommunikációs eszközök esetében a közlekedési táblák jelrendszerén alapuló egyezményes ábrarendszer [168].

Kísérleti eredményeim alapján meggyőződésem, hogy a fentiekben bemutatott megoldási lehetőséggel az infokommunikációs eszközök használata „akadálymentesíthető" lehet minden felhasználó számára, nem csak az idegen nyelven nem beszélők, az időskorúak és a gyermekkorúak számára, hanem a gyengénlátók és az olvasási nehézséggel küzdők számára is.

Az általam kidolgozott megoldásnak más olyan alkalmazása is lehetséges, amihez gyors reakcióidőn alapuló döntések szükségesek. Ilyen lehet a katonai, a harctéri, a rendvédelemi és a légi irányítási alkalmazás, mentési, tűz- és katasztrófavédelmi, ügyfélhívó rendszerek,

valamint a különböző ipari, termelési területeken történő felhasználása. A szabványok adta lehetőségek felhasználásával kialakítható az az ábrázolási rendszer, ami az infokommunikációs eszközöket használók széles köre számára jelenthet nagyobb biztonságot [169][171].

A vizsgálatom alapját a disszertációmban bemutatott, általam lefolytatott kérdőíves vizsgálat eredményei, valamint azok kiértékelése és a kapott eredmények képezik. Az általam kidolgozott és bevezetésre javasolt, a fentiekben bemutatott szoftverergonómiai megoldás a szoftveres akadálymentesítés lehetőségét szolgálja, annak érdekében, hogy a társadalom minél szélesebb köre tudjon biztonságosan bekapcsolódni a kibervilágba.

Megállapítom a kapott vizsgálati eredmények alapján, hogy az általam elgondolt piktogramos üzenetfeldolgozás sokkal hatékonyabb és kevesebb hibázási lehetőséget rejt magában, mint a jelenleg alkalmazott szöveges üzenetek alkalmazása. Ez a megállapítás is a hipotézisemet bizonyítja.

ÖSSZEGZETT KÖVETKEZTETÉSEK

A kutatómunka összegzése

Irodalomkutatást végeztem a tématerület és a hozzá kapcsolódó tudományterületek (jogi, szociológiai és társadalomtudományi, generációkutatás, történelmi fejlődés, informatika, internet, információfeldolgozás, kiberbiztonság) eddig feldolgozott, valamint aktuális és releváns publikációinak körében, ami alapján hipotéziseket állítottam fel. A kutatási terület aktualitását a kormányzati törekvések is mutatják, hiszen az elmúlt néhány évben (pl. a DJP keretében) számos fejlesztés valósult meg.

A digitalizálódó világban vannak úgynevezett digitális bennszülöttek, akiknek már az okos eszközök és az internet használata természetes napi gyakorlatot jelent, míg az idősebb generációk számára akár nehézséget is okozhat. A társadalom szereplői (a kibertérben felhasználók) eltérő digitális infrastruktúrával rendelkeznek, melyet lakóhelyük nagymértékben meghatároz. A felhasználói csoportok az ismertetett tényezők hatására életük során igen különböző módon fejlődtek a kibertér használatában. A kutatásomban több szempont szerint megvizsgáltam a generációk viselkedését és bizonyítottam, hogy a különböző életkorú és infrastrukturális lehetőségekkel rendelkező csoportok eltérő digitális kompetenciával és biztoságtudatossággal rendelkeznek. A nagy különbségek miatt vannak nem kiszámítható (sztochasztikus) felhasználói attitűdök a digitális térben, ami kockázatot jelent.

Hazánk a törvényi szabályozás szempontjából igen jól lefedett, a vonatkozó törvényeket részletesen ismertettem, valamint kifejtettem, hogy a törvényi szabályozás nem elegendő önmagában kiberbiztonsági szempontból, mivel a felhasználók jelentik a legnagyobb kockázatot a kibertérben végzett műveleteikkel.

A kibertér szempontjából a felhasználót, mint kockázati elemet, mindenképpen vizsgálni szükséges. A felhasználó akkor nem jelentene kockázatot, ha előre meghatározható, tervezhető lépéseket hajtana végre. Kutatásomban rámutattam és bizonyítottam, hogy a felhasználóknak vannak sztochasztikus és közel determinisztikus viselkedésformái, melyek kapcsolatban állnak az informatikai ismereteikkel.

A hipotéziseim igazolása céljából kidolgoztam az irodalomkutatás és a tématerület legújabb eredményeinek felhasználásával egy kérdőívet, melyet eljuttattam vizsgálatom célcsoportjának több mint ezer tagjához. A visszaérkező válaszokat összegyűjtöttem, az ellentmondások kiszűrését követően az általam feldolgozásra alkalmasnak ítélt válaszokat összesítettem.

A felmérésem eredményeként kockázatalapú szempontrendszert hoztam létre a felhasználók viselkedése alapján. Megállapítom, hogy a digitális kompetencia és a biztonságtudatosság erősen függ a felhasználó informatikai képzettségétől és a biztonságtudatossági szintjétől. A felhasználókat ezért csoportokba soroltam (VVSZM).

Megállapítom, hogy a lakóhely és az életkor jelentősen befolyásolja a felhasználók digitális kompetencia és biztonságtudatossági szintjét. Kijelentem, hogy képzéssel növelhető a lakosság digitális jóléte, biztonságos internethasználatának szintje. Továbbá megállapítom, hogy a vizsgált 35 év alatti életkorú felhasználók digitális kompetenciaszintje magasabb, mint a vizsgált 35 év feletti életkorú felhasználóké. Azonban az idősebb korosztály rendelkezik magasabb fokú biztonságtudatossággal.

Felállítottam egy módszer- és viselkedésspecifikus szempontrendszert, amely alkalmas a felhasználók kockázati célú értékelésére.

A kérdéscsaládok között összefüggéseket mutattam ki a digitális kompetencia és a biztonságtudatosság fő szempontjai szerint. Az irodalomkutatás alapján felállított hipotéziseimet mérési eredményekkel, valamint az ezekből kapott olyan összefüggésekkel bizonyítottam, melyek eddig nem kerültek megállapításra. Korrelációs számítással kimutattam, hogy a vírusvédelem alkalmazásának hiánya és a vírustámadás elszenvedése között igen szoros kapcsolat van, mely lineáris illeszkedést mutat. Ennek alapján kijelentettem, hogy a felmérésben részt vevőkre egyértelműen igaz, hogy az a felhasználó, aki nem alkalmaz vírusvédelmet, vírustámadást szenved el. A válaszadók kérdésekre adott válaszai alapján bizonyítást nyert, hogy az eltérő életkorú és eltérő infrastruktúrával rendelkező csoportok igen nagy különbségeket mutatnak a digitális kompetencia és a biztonságtudatosság tekintetében.

A vizsgálati eredményeim alapján bebizonyítottam, hogy az egyre nagyobb számban előforduló internetes zaklatás, a cyberbulling, azokat a felhasználókat éri nagyobb arányban, akik kevésbé biztonságtudatosak. Azon felhasználók esetében fordul elő a legnagyobb számban, hogy maguk akarják megoldani a jelentkező problémát, avagy figyelmen kívül hagyják a zaklatást, akik alacsonynak vallották biztonságtudatossági szintjüket és a digitális kompetenciájukat. Továbbá megállapítom, hogy azon felhasználók kértek a legnagyobb számban hivatalos segítséget, akik magasnak vallották a biztonságtudatossági szintjüket és a digitális kompetenciájukat. A dolgozatban bemutatott vizsgálataim eredménye is alátámasztja azt, hogy a felhasználók biztonságtudatossági szintjét oktatásokkal/képzésekkel folyamatosan emelni szükséges.

Megállapítom, hogy erős korrelációs kapcsolat van a felhasználói csoportok vírusvédelmi és adatmentési együttesének hiánya esetében, ami azt jelenti, hogy a felhasználók ezt a két biztonsági megoldást közel azonos arányban nem alkalmazzák. Elsősorban azok a felhasználók, akik ezeknek a megoldásoknak a használatát mellőzik, a célcsoportjai azoknak a zsarolóvírus (ransomware) okozta támadásoknak, amelyek az elmúlt időszakban jelentősen megnövekedtek.

Kutatásaim eredményeként, felhasználva az EU ajánlásait és keretrendszerét, melyet az EU az összes munkavállaló besorolására alkalmaz és elkészítettem a felhasználók biztonságtudatosság és digitális kompetencia szerinti minősítésére és a társadalom egészének besorolására alkalmas keretrendszert (VVSZM). A 2. függelékben csatoltam az új keretrendszert.

Kidolgoztam a teljes társadalomra alkalmazható VVSZM Digitális Kompetencia Keretrendszert, ami a felhasználói viselkedést biztonságosabbá, objektívebbé teszi a felhasználók digitális kompetencia és biztonságtudatossági szintjének hatékony növelése érdekében. A digitális kompetencia keretrendszerbe történő besorolás alapján a kompetenciafejlesztés nagyon eredményes megoldás, ennek alkalmazására szempontrendszert dolgoztam ki, amely alapján a biztonság magasabb szintje érhető el. Az általam kidolgozott keretrendszer, mivel a társadalom minden szereplője elhelyezhető benne, alkalmas minden felhasználó besorolására.

Az általam kidolgozott VVSZM Digitális Kompetencia Keretrendszer tartalmaz egy új felhasználói besorolási szintet, amelyet a „Védendő” megnevezéssel jelöltem, és egy új osztályt, valamint több alosztályt. A korábban már meglévő „Biztonság” osztályon belül a „Biztonságtudatosság” új alosztályt, valamint a „Tudásátadási képesség” új osztály és annak „A felhalmozott tapasztalat átadása” és „A megszerzett ismeretek átadása” valamint „A tudás átadása a saját viselkedésének és magatartásának példáján keresztül” neveket viselő új alosztályait alkottam meg és definiáltam.

Megállapítom, hogy kiberbiztonsági szempontból a felhasználónak kulcsszerepe van, vagyis jelentős kockázati tényező, a kockázati szintje pedig erősen függ a digitális kompetenciájától és a biztonságtudatosságától, mely az informatikai ismeretekkel szoros összefüggésben van. A felhasználó kockázati szintje kiberbiztonsági szempontból csökkenthető a digitális kompetencia és a biztonságtudatosság növelésével, mely informatikai ismeretek oktatásával valósítható meg. A kidolgozott keretrendszer alapja lehet egy modulrendszerű oktatási tananyag fejlesztésének, így a besorolás alapján a felhasználó a saját szintjén kezdheti el a tanulást, ami lehetővé teszi a gyorsabb és hatékonyabb ismeretfejlesztést.

Bizonyítottam feltételezésemet, hogy a felhasználói támogatás szükséges, mivel a digitális alkalmazások során a gyors döntések meghozatala az átlag felhasználó számára is nehézséget okozhat, mely kockázatot jelent. Az alacsony kompetenciájú társadalmi csoportok a biztonságtudatosság és digitális kompetencia hiányosságai miatt pedig még inkább segítségre szorulnak, ezért ezeknek a társadalmi csoportoknak a vonatkozásában (a kibertér biztonságának növelése céljából) egy akadálymentesítő rendszer kidolgozásának a szükségességét állapítottam meg. A weblapok akadálymentesítése az ENSZ és az Európai Unió által előírt és vállalt kötelezettsége is az országnak. Ezt szükséges kiterjeszteni az eszközök operációs rendszereitől egészen az alkalmazási szintig. Ennek az akadálymentesítésnek a keretében a piktogramok bevezetésére és szabványosított alkalmazására tettem javaslatot, melyet saját kutatásom eredményeivel támasztottam alá, digitális eszközöket alkalmazó, eltérő kompetenciájú felhasználók részvételével végzett kísérleteim eredményeit felhasználva.

Kutatást végeztem annak a hipotézisemnek az igazolására, hogy a piktogramos üzenetek alkalmasak a felhasználói biztonság növelésére (ami nevezhető akadálymentesítésnek is) gyors döntéseket igénylő helyzetekben. Tesztfeladatsort készítettem és töltettem ki átlag felhasználókkal, melynek eredményeit értékeltem. A piktogramos feladatokat a felhasználók azonos idő alatt gyorsabban és pontosabban oldották meg, mint a szöveges feladatokat, annak ellenére, hogy ezeket a piktogramos üzeneteket a kísérletben részt vevők soha nem látták még korábban.

A piktogramos tesztfeladatok kidolgozása esetében a szoftverergonómiára, valamint a kibertér akadálymentesítésére vonatkozó szabványokat és ajánlásokat vettem figyelembe. Az általánosan alkalmazott jelölésrendszert is felhasználtam a tesztfeladatok megalkotása során. A felhasználók biztonsága növekszik, a szervezet kockázata pedig csökken az üzemeltetés közbeni segítségnyújtás esetében. Az általam kidolgozott szoftverergonómiai alkalmazás megoldási javaslatot ad az információfeldolgozási és felhasználói reakció biztonsági kihívásaira. A kutatásomban bizonyítottam azt, hogy a felhasználó szöveges információfeldolgozásával szemben az ábraalapú információfeldolgozás gyorsabb és egyszerűbb.

Új tudományos eredmények

1. **Bizonyítottam, hogy az informatikai eszközök felhasználói különböző életkorú és infrastrukturális lehetőségekkel rendelkező csoportjainak eltérő a digitális kompetenciája és a biztonságtudatossága. A kutatásom eredményei alátámasztották, hogy ez biztonsági kockázatot okoz, ezért feltétlenül szükséges a felhasználók digitális kompetenciájának és a biztonságtudatosságának fejlesztése** [156][157][158][161][163]**.**

2. **Létrehoztam egy módszer- és viselkedésspecifikus szempontrendszert, amelyben négy különböző képességszintű felhasználói csoportot határoztam meg, ennek alapján az informatikai eszköz felhasználók kockázati célú értékelése elvégezhető** [156][157][158][161][163]**.**

3. **Kidolgoztam egy új, VVSZM ("Védendő"; "Veszélyes"; "Szerény"; "Magabiztos") Digitális Kompetencia Keretrendszert, ebben definiáltam egy új felhasználói szintet („Védendő felhasználó"), amelybe besorolhatók azok az informatikai eszköz felhasználók, akiknek alacsony a digitális kompetenciája (védendők)** [156][157][158][165][166]**.**

4. **Definiáltam egy új osztályt, „Tudásátadási képesség" elnevezéssel, valamint alosztályait, továbbá a „Biztonság" osztályon belül egy új alosztályt, a „Biztonságtudatosság" névvel az általam kidolgozott VVSZM Digitális Kompetencia Keretrendszerben, ezzel elértem azt a célt, hogy a keretrendszer a teljes társadalom besorolására alkalmazható** [156][157][158][165][166]**.**

5. **Bizonyítottam, hogy az informatikai rendszerek felhasználói számára hatékony kompetencia fejlesztés szükséges, a disszertációmban kidolgozott VVSZM Digitális Kompetencia Keretrendszerbe sorolás alapján, ami a teljes társadalomra alkalmazható** [156][157][158][165][166]**.**

6. **Bizonyítottam, hogy a piktogramos üzenetek segítik az informatikai eszközök felhasználóit a könnyebb, gyorsabb és pontosabb feladatvégrehajtásban az informatikai eszközök alkalmazása során, a közösségi jog, a nemzeti jogszabályok és az akadálymentesítésre vonatkozó szabványok figyelembevételével** [161][163][169][171]**.**

Ajánlások

1. Javaslom a VVSZM digitális kompetencia keretrendszer bevezetését, mely minden generációra alkalmazható a digitális kompetencia és a biztonságtudatosság szintjének pontos megállapítása céljából annak érdekében, hogy a felhasználók elérjék és követni tudják a digitális fejlődést, mely egyre szélesebb körben alkalmazott és egyre magasabb szintű digitális kompetenciát és biztonságtudatosságot követel meg mind a hétköznapokban, mind a különböző, Ipar 4.0-nak megfelelő munkakörök betöltése esetén.

2. Javaslom a VVSZM digitális kompetencia keretrendszer szintjei szerinti csoportok számára modul rendszerű digitális ismeretek oktatását a hatékonyság és a biztonság növelése céljából. Mivel a kutatási eredményeim azt igazolták, hogy a társadalomban a digitális kompetencia és biztonságtudatosság szempontjából igen eltérő csoportokat különböztethetünk meg, melyek képzése, valamint közel azonos szintre emelése hatékonyan (költség és idő szempontjából) csak célirányosan, a megfelelő szintről indulva valósítható meg. Ezeket a digitális képzéseket a fejlődés szintjéhez igazítva folyamatosan és proaktívan fejleszteni szükséges.

3. Javaslom egy szabványos piktogramrendszer kidolgozását, szabványosítását és bevezetését a felhasználói digitális akadálymentesítés és a biztonság növelése céljából, az eszközök operációs rendszereitől egészen az alkalmazási szintig. A piktogramos rendszer alkalmazhatósága minden olyan helyen növelheti a biztonságos felhasználást, ahol az alacsony reakcióidő alkalmazási feltétel. Ennek eredményes használata lehetséges a légiirányítás, a hadművelet-harcászat, a katonaság, a rendészet, a katasztrófavédelem, a közlekedés, az egészségügy, a kritikus infrastruktúrák irányítása, valamint a gyártás esetében is. Továbbá alkalmazható még az alacsony digitális kompetenciával és biztonságtudatossággal rendelkező, idegen nyelvet nem beszélő, valamint gyermekkorú felhasználókat támogatni képes biztonságos eszköz- és kibertér használatban az Európai Uniós Digitális menetrend és a DJP 2.0 programokkal összhangban.

HIVATKOZOTT IRODALOM

[1] Michelberger, P. – Lábodi, Cs.: After Information Security – Before a Paradigm Change: A complex Enterprise Security Model, Acta Polytechnica Hungarica 9, (4) pp. 101-116., 2012, https://www.uni-obuda.hu/journal/Michelberger_Labodi_36.pdf , (letöltve: 2017. január 10.)

[2] Michelberger, P. – Beinschróth, J. – Horváth, G. K.: The Employe - An Information Security Risk, Acta Oeconomica Universitatis Selye, 2:(1) pp. 187-200., 2013

[3] Farkas, T. – Hronyecz, E.: Új biztonsági kihívások az Európai Unió tagállamaiban - koncepciófejlesztés az európai biztonságpolitikában, A XXI. Fiatal Műszakiak Tudományos Ülésszaka előadásai, pp. 157-160., 2016, https://eda.eme.ro/bitstream/handle/10598/29047/EME_21_FMTU_2016_FarkasTibor-HronyeczErika2.pdf?sequence=3&isAllowed=y , (letöltve: 2017. október 28.)

[4] Kiss, G. – Szász, A.: A Comparison of the mechanical engineering and safety engineering student's ICT attitudes at the Obuda University, TSHS Web of Conferences 26, Article Number: 01094, Number of pages: 8, 2016, DOI: https://doi.org/10.1051/shsconf/20162601094 , https://www.researchgate.net/publication/301672921_A_Comparison_of_the_mechanical_engineering_and_safety_engineering_student%27s_ICT_attitudes_at_the_Obuda_University, (letöltve: 2017. november 10.)

[5] Torres-Gastelú, C. A. – Kiss, G.: Perceptions of Students towards ICT Competencies at the University, Informatics in Education, v15 n2, pp. 319-338, 2016, ERIC Number: EJ1117298, ISSN-1648-5831, DOI: 10.15388/infedu.2016.16, https://www.mii.lt/informatics_in_education/pdf/infedu.2016.16.pdf , (letöltve: 2017. május 10.)

[6] Keszthelyi, A.: Age of Cyber Crime and Culture of Security, Science Journal Of Business And Management, 3:(1-1) pp. 39-45., 2015, https://pdfs.semanticscholar.org/e275/77c618580f305eea526d3676604cc081123b.pdf?_ga=2.20618296.1239473795.1550428066-1543191032.1550428066 , (letöltve: 2017. február 5.)

[7] Rajnai, Z. – Kerti, A.: Internetterrorisme, Kommunikáció 2007. 511 p., Budapest, Magyarország, 2007., pp. 116-119., ISBN:978-963-7060-31-1

[8] Berek, L.: Országvédelem, Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem, 2005. 120 p.

[9] Berek, L.: Biztonságtechnika, Budapest: Nemzeti Közszolgálati Egyetem, 2014. 48 p

[10] Rajnai, Z.: Információtechnológiai kutatások a védelmi szektorban; 5.Báthory-Brassai Tanulmánykötet 2. rész. Budapest: Óbudai Egyetem, 2015., ISBN 978-615-5460-38-8, pp. 423-431., https://www.academia.edu/29908057/Interoperabilitási_kérdések_és_informatikai_biztonsági_tükrében_a_közigazgatásban , (letöltve: 2017. május 20.)

[11] Európai Digitális Menetrend COM(2010)245; Az európai digitális menetrend – európai növekedés digitális alapokon, COM(2012) 784; ISBN 978-92-79-41911-9 doi:10.2775/41997, http://publications.europa.eu/resource/cellar/a64ba5f7-f0b6-450a-80e8-fd0ac4e03676.0009.02/DOC_2, (letöltve: 2017.08.01.)

[12] Európa digitális fejlődéséről szóló jelentés (EDPR), 2017 – Országprofil Magyarországról http://www.europarl.europa.eu/atyourservice/hu/displayFtu.html?ftuId=FTU_2.4.3.html, (letöltve: 2017.08.10)

[13] ENISA Threat Landscape Report 2016, 15 Top Cyber-Threats and Trends, European Union Agency for Network and Information Security (ENISA), 2017, p. 86., ISBN978-92-9204-202-8, ISSN 2363-3050, DOI 10.2824/92184, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016 , (letöltve: 2017. március 28.)

[14] ENISA Threat Landscape Report 2017, 15 Top Cyber-Threats and Trends, European Union Agency for Network and Information Security (ENISA), 2018, p. 114., ISBN 978-92-9204-250-9, ISSN 2363-3050, DOI 10.2824/967192, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017, (letöltve: 2018. március 30.)

[15] Zöld könyv az infokommunikációs szektor 2014-2020 közötti fejlesztési irányairól, Nemzeti Fejlesztési Minisztérium Infokommunikációért és Fogyasztóvédelemért Felelős Államtitkárság 2014., http://www.kormany.hu/download/b/f7/30000/Zöldkönyv%20végleges.pdf, (letöltve: 2017.08.10)

[16] A Digitális Jólét Program 2.0, Budapest, 2017., http://www.kormany.hu/download/6/6d/21000/DJP20%20Stratégiai%20Tanulmány.pdf, (letöltve: 2017.09.12)

[17] Digitális Magyarország; http://digitalismagyarorszag.kormany.hu/digitalis-magyarorszag, (letöltve: 2017.10.20.)

[18] Magyarország Digitális Gyermekvédelmi Stratégiája, 2016, http://www.kormany.hu/download/6/0e/c0000/Magyarorsz%C3%A1g%20Digit%C3%A1lis%20Gyermekv%C3%A9delmi%20Strat%C3%A9gi%C3%A1ja.pdf (letöltve: 2016. október 20.)

[19] Magyarország Digitális Oktatási Stratégiája, 2016, pp. 5-6, http://www.kormany.hu/download/0/cc/d0000/MDO.pdf , (letöltve: 2017.10.20.)

[20] Új Nemzedék Jövőjéért Program, A Kormány ifjúságpolitikai keretprogramja, 2012, http://www.ujnemzedek.com/uploads/kcfinder/files/új_nemzedék_jövőjéért_program_netes%281%29.pdf, (letöltve: 2016.08.29.)

[21] Nemzeti Stratégiák; Oktatáskutató és Fejlesztő Intézet ISBN 978-963-682-985-8, http://ofi.hu/sites/default/files/attachments/nemzeti_strategiak.pdf, (letöltve: 2017.10.21.)

[22] A 2014-2020 közötti időszak foglalkoztatáspolitikai célú fejlesztéseinek megalapozása, Melléklet az NGM/21664 /2013. kormány-előterjesztéshez, 2013, http://2010-2014.kormany.hu/download/8/4c/01000/Fogl_Strat_14-20.pdf, (letöltve: 2017.11.08.)

[23] Digitális Munkaerő Program, IVSZ, Budapest, 2016., http://ivsz.hu/wp-content/uploads/2016/09/ivsz-digitalis-munkaero-program.pdf, (letöltve: 2016.12.20.)

[24] Szűcs, E. – Kuris, Z.: A hazai és külföldi minősített adatok kezelése az összeegyeztethetőséget figyelembe véve, Biztonságtechnikai Szimpozium. Budapest, Magyarország, 2011, pp. 1-21.

[25] Good Practice in Information and Communication Technology for Education, Asian Development Bank, Mandaluyong City, 2009, ISBN 978–971–561–823–6, https://www.adb.org/publications/good-practice-information-and-communication-technology-education, (letöltve: 2017.11.10.)

[26] Joó, T.: A nemzedék fogalmáról, Kalangya, 1935, (pp.392-400), http://dda.vmmi.org/szamok/1935_05.pdf , (letöltve: 2017.10.20.)

[27] Mc.Crindle, M. – Wolfinger, E.: The ABC of XYZ: Understanding the Global Generations, University of New South Wales Press, Sidney, 2009, http://mccrindle.com.au/resources/whitepapers/McCrindle-Research_ABC-03_The-Generation-Map_Mark-McCrindle.pdf (letöltve 2017.12.15.)

[28] Zombainé Tarnótzky, K.: Generációk összehasonlítása, különös tekintettel a Z generáció és tanáraik között fellelhető különbségekre, Budapesti Gazdasági Főiskola, Szakdolgozat, 2015, http://dolgozattar.repozitorium.bgf.hu/2395/1/Zombaine_Szakdolgozat.pdf, (letöltve: 2017.05.15.)

[29] Paris, E.: Alapvetések a Z generációtudomány-kommunikációjához, TÁMOP-4.2.3-12/1/KONV-2012-0016, Tudománykommunikáció a Z generációnak, Pécs 2013, http://www.zgeneracio.hu/tanulmanyok (letöltve 2017.12.15.)

[30] Strauss, W., Howe, N.: The Fourth Turning: An American Prophecy, 1997, http://www.fourthturning.com/, (letöltve: 2017.10.20.)

[31] Győri, K. Zs.: Ki tanít kit?, Virtualitás és funkció. Kutató diákok írásai I. PTE BTK Neveléstudományi Intézet Pécs, 2013, p.33-39. http://digitalia.lib.pte.hu/, (letöltve: 2017.10.21.)

[32] Kissné András, K.: Generációk, munkaerőpiac és a motiváció kérdései a 21. században, http://www.ohe.hu/hrmagazin/cikkek/generaciok-munkaeropiac-es-a-motivacio-kerdesei-a-21-szazadban#_ftn3 (letöltve: 2017.10.19.)

[33] Tari, A.: Y generáció, Jaffa Kiadó, 2010, ISBN: 9789639971202

[34] Tari, A.: Z generáció, Tericum Kiadó 2011, ISBN: 9789639971202

[35] Abonyi-Tóth, A – Turcsányi-Szabó M.: A digitális tudás fejlesztésének lehetőségei, Educatio Társadalmi Szolgáltató Nonprofit Kft., 2015., ISBN 978-963-9795-92-1, http://dl-sulinet.educatio.hu/download/letoltheto-dokumentumok/Digitalis-irastudas.pdf (letöltve: 2016. 10. 11.)

[36] Az egész életen át tartó tanuláshoz szükséges kulcskompetenciák, 2009. jún. 17., www.ofi.hu/tudastar/nemzetkozi-kitekintes/egesz-eleten-at-tarto, (letöltve: 2015. 12. 07.)

[37] Catts, R. – Lau, J.: Towards Information Literacy Indicators. Conceptual framework paper. UNESCO, Paris, 2008, https://books.google.hu/books/about/Towards_information_literacy_indicators.html?id=S2WPDAEACAAJ&redir_esc=y, (letöltve: 2017.10.26.)

[38] Nemzeti Infokommunikációs Stratégia 2014-2020, http://2010-2014.kormany.hu/download/b/fd/21000/Nemzeti%20Infokommunik%C3%A1ci%C3%B3s%20Strat%C3%A9gia%202014-2020.pdf, (letöltve: 2016. 10. 10.)

[39] Tongori, Á.: Az IKT-műveltség fogalmi keretének változása, SZTE Neveléstudományi Doktori Iskola, Iskolakultúra 2012/11, http://epa.oszk.hu/00000/00011/00170/pdf/EPA00011_Iskolakultura_2012-11_034-047.pdf, (letöltve: 2017.10.11.)

[40] Koltay, T.: Digitális írástudás – Web 2.0 – pedagógia, http://www.tani-tani.info/101_koltay (letöltve: 2016. 10. 8.)

[41] Koltay, T.: Médiaműveltség, média-írástudás, digitális írástudás www.mediakutato.hu/cikk/2009_04_tel/08_mediamuveltseg_digitalis_irastudas, (letöltve: 2015. 12. 05.)

[42] Online kormányzati, közigazgatási és e-egészségügyi szolgáltatások terjedésének és a Digitális Jólét Program kiterjesztésének elősegítése, KIFÜ, http://kifu.gov.hu/itfp/projektek/online_kormanyzati_kozigazgatasi , (letöltve: 2018. június 10.)

[43] Agarwal, P. K.: A Vision of the Future, a Northeastern University Silicon Valley előadásanyaga, http://www.ncsl.org/documents/nalit/NALIT-A_Vision_of_the_Future.pdf , (letöltve: 2018. január 30.)

[44] Rajnai, Z.: Információbiztonság tudatosság, Kolozsvár, Erdélyi Múzeum Egyesület (EME); Óbudai Egyetem, 2017. pp. 37-43., Műszaki Tudományos Közlemények - 7., ISBN:978-963-449-018-0, https://eda.eme.ro/bitstream/handle/10598/29758/XXII_FMTU_06-Rajnai-plen.pdf?sequence=3 , (letöltve: 2018. március 3)

[45] Michelberger, P. – Dombora, S.: A felhasználói profil szerepe az információbiztonságban, Pro Publico Bono: Magyar Közigazgatás; A Nemzeti Közszolgálati Egyetem Közigazgatás-Tudományi Szakmai Folyóirata 3:(4) pp. 34-50., 2015, http://real.mtak.hu/33739/1/PPB_15_4_Tudomanyos_lathatosag_u.pdf , (letöltve: 2017. október 15.)

[46] Recommendation of The European Parliament and of The Council of 18 December 2006 on key competences for lifelong learning (2006/962/EC), http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32006H0962&from=HU , (letöltve: 2017.03.20)

[47] Tokody, D. – Flammini, F.: Smart Systems for the Protection of Individuals, Key Engineering Materials, Vol. 755, pp. 190-197, 2017, DOI: 10.4028/www.scientific.net/KEM.755.190, https://www.scientific.net/Paper/Preview/525154 (letöltve: 2017.08.21.)

[48] Dombora, S. – Michelberger, P.: Információbiztonság szerepe az üzleti folyamatokban, Műszaki és Menedzsment Tudományi Közlemények, 1:(1) p. &. 11 p., 2016, https://www.researchgate.net/publication/306042003_Informaciobiztonsag_szerepe_az_uzleti_folyamatokban , (letöltve: 2017. szeptember 4.)

[49] Lazányi, K.: Stressed Out by the Information and Communication Technologies of the 21st Century, Science Journal Of Business And Management, 4:(1-1) pp. 10-14. 2016,

http://article.sciencepublishinggroup.com/pdf/10.11648.j.sjbm.s.2016040101.12.pdf (letöltve: 2017.02.06)

[50] Measuring Digital Skills across the EU: EU wide indicators of Digital Competence, 2014, https://ec.europa.eu/digital-single-market/en/news/measuring-digital-skills-across-eu-eu-wide-indicators-digital-competence (letöltve: 2017.02.06)

[51] A common European Digital Competence Framework for Citizens. Europen Commision, Europen Union, 2016, https://www.openeducationeuropa.eu/sites/default/files/DIGCOMP%20brochure%202014%20.pdf (letöltve: 2017.02.06)

[52] Gutiérrez Porlán, J. – Serrano Sánchez, J. L.: „Evaluation and development of digital competence in future primary school teachers at the University of Murcia", Journal of New Approaches in Educational Research, 5(1), 51-56. doi: 10.7821/naer.2016.1.152 https://naerjournal.ua.es/article/view/v5n1-8?platform=hootsuite (letöltve: 2017.02.06)

[53] Digital competences - Self-assessment grid, European Union, 2015 http://europass.cedefop.europa.eu/sites/default/files/dc-en.pdf , (letöltve: 2017.01.21)

[54] Vuorikari, R. – Punie, Y. – Carretero, S. – den Brande, L. V.: „DigComp 2.0: The Digital Competence Framework for Citizens", 2016, DOI: 10.2791/11517, ISBN: 978-92-79-58876-1, http://www.ecdl.cz/data/ECDL-DIGCOMP-update.pdf (letöltve: 2017.03.20)

[55] Ermalai, I. L.: IT Gaining Ground in Learning, Advanced Engineering Forum, Vols. 8-9, pp. 37-44, 2013, DOI: 10.4028/www.scientific.net/AEF.8-9.37, https://www.scientific.net/AEF.8-9.37 , (letöltve: 2017.03.20)

[56] Porumb, C. – Porumb, S. – Orza, B. – Vlaicu, A.: Blended Learning Concept and its Applications to Engineering Education, Advanced Engineering Forum, Vols. 8-9, pp. 55-64, 2013, DOI: 10.4028/www.scientific.net/AEF.8-9.55, https://www.scientific.net/AEF.8-9.55, (letöltve: 2017.03.20)

[57] Safer Internet Day Report - Have your Say: Young people's perspectives about their online rights and responsibilities, Childnet International and the UK Safer Internet Centre, 2013, https://www.saferinternet.org.uk/safer-internet-day/sid-2013/have-your-say-survey-results, (letöltve: 2017.05.15)

[58] Holloway, D. – Green, L. – Livingstone, S.: Zero to Eight, Young children and their internet use, August 2013, ISSN 2045-256X http://www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx, (letöltve: 2017. 05.15)

[59] Porumb, S. – Porumb, C. – Vlaicu, A. – Orza, B.: Advanced Learning Tools for (Non) Formal Education, Advanced Engineering Forum, Vols. 8-9, pp. 65-74, 2013, DOI: 10.4028/www.scientific.net/AEF.8-9.65, https://www.scientific.net/AEF.8-9.65 (letöltve: 2017.03.20)

[60] Simon, J.: Industrial Data Acquisition Applications Using Relational Databases, IoT Environment and Multi Criteria Decision Making Systems, International Journal of Current Research in Engineering, Science and Technology 1, 2016, 34-41, https://www.researchgate.net/profile/Janos_Simon2/publication/311257938_Industrial_Data_Acquisition_Applications_Using_Relational_Databases_IIoT_Environment_and_Multi_Criteria_Decisio n_Making_Systems/links/584028d908ae8e63e61f756b.pdf, (letöltve: 2017.03.18)

[61] Tokody, D. – Schuster, Gy.: Driving Forces Behind Smart City Implementations-The Next Smart Revolution., Journal of Emerging Research and Solutions in ICT 1.2, 2016, pp. 1-16., http://eprints.fikt.edu.mk/171/, (letöltve: 2017.03.18)

[62] Pokorádi, L.: Logical Tree of Mathematical Modeling, Theory and Applications of Mathematics & Computer Science, 5:(1) pp. 20-28., 2015, https://www.researchgate.net/publication/269989786_Logical_Tree_of_Mathematical_Modeling , (letöltve: 2017. november 20.)

[63] Holtai, A. – Magyar, S. – Puskás, B.: Az informatikai üzemeltetés általános kérdései, Felderítő Szemle, 2015:(4), pp. 91-102., 2015, http://real.mtak.hu/66001/7/191_inform_2016_1_u.pdf , (letöltve: 2017. november 15.)

[64] Michelberger, P. – Dombora, S.: A possible tool for development of information security - SIEM system, EKONOMIKA 62:(1), pp. 125-140., 2016, doi:10.5937/ekonomika1601125M, https://www.researchgate.net/publication/301290084_A_possible_tool_for_development_of_information_security_SIEM_system , (letöltve: 2017. október 16.)

[65] Kerti, A.: Átviteli út biztonság, Hadmérnök, II:(4) pp., 60-65., 2007, http://www.hadmernok.hu/archivum/2007/4/2007_4_kerti.html , (letöltve: 2017. március 21.)

[66] Dobrilovic, D. – Stojanov, Z. – Jager, S. – Rajnai, Z.: A method for comparing and analyzing wireless security situations in two capital cities, Acta Polytechnica Hungarica 13:(6), pp. 67-86., 2016, https://uni-obuda.hu/journal/Dobrilovic_Stojanov_Jager_Rajnai_70.pdf ,(letöltve: 2017. április 8.)

[67] Papp, Z. – Pándi, E. – Kerti, A.: A számítógép-hálózatok elleni támadások módszertana, Kommunikáció 2009., 346 p., Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, 2009. pp. 143-154., ISBN:978 963 7060 70 0

[68] Pokorádi, L.: Rendszerek és folyamatok modellezése, Campus Kiadó, Debrecen, 2008., ISBN 978-963-9822-06-1, https://dea.lib.unideb.hu/dea/bitstream/handle/2437/85077/rendsz_foly_mod.pdf?sequence=1 , (letöltve: 2017. május 8.)

[69] Pearson korreláció jelentése és alkalmazása az SPSS-ben, oktatási segédelet, https://spssabc.hu/ketvaltozos-elemzes/korrelacio/ , (letöltve: 2018. április 21.)

[70] Korreláció, Statisztika I., oktatási segédlet, http://psycho.unideb.hu/munkatarsak/balazs_katalin/stat1/stat1ora3.pdf , (letöltve: 2018. április 21.)

[71] Pokorádi, L.: Sensitivity analysis of reliability of Systems with Complex Interconnections, Journal of Loss Prevention in The Process Industries, 32: pp. 436-442., 2014, https://www.sciencedirect.com/science/article/abs/pii/S0950423014001788?via%3Dihub , (letöltve: 2017. május 15.)

[72] Magyar, S. – Sági, N.: A kiberbűnözés legújabb trendjei, Kommunikáció 2014., Budapest, Nemzeti Közszolgálati Egyetem, 2014. pp. 183-192., ISBN:978-615-5491-94-8

[73] Torres-Gastelú, C. A. – Kiss, G. – Domínguez, A. L.: Level of ICT Competencies at the University, Procedia - Social and Behavioral Sciences, Volume 174, pp.137-142, 2015, DOI: https://doi.org/10.1016/j.sbspro.2015.01.638 , https://www.sciencedirect.com/science/article/pii/S1877042815006898 , letöltve: 2017. szeptember 7.

[74] Torres-Gastelú, C. A. – Kiss, G.: Comparison of the ICT Literacy Level of the Mexican and Hungarian Students in the Higher Education, Procedia - Social and Behavioral Sciences, Volume 176, pp. 824-833, 2015, DOI: https://doi.org/10.1016/j.sbspro.2015.01.546 , https://www.sciencedirect.com/science/article/pii/S1877042815005832 , letöltve: 2017. augusztus 5.

[75] Rajnai, Z.: Gyakorlatorientált képzés a műszaki felsőoktatásban:, Kolozsvár: Erdélyi Múzeum-Egyesület (EME), 2016, pp. 45-48., Műszaki Tudományos Közlemények 5., A XXI. Fiatal Műszakiak Tudományos Ülésszaka előadásai, https://eda.eme.ro/bitstream/handle/10598/29103/EME_21_FMTU_2016_3-Rajnai-plenaris.pdf?sequence=3&isAllowed=y (letöltve: 2017. június 15.)

[76] Keszthelyi, A.: Ethics in the Age of Cyber Crime and Cyber War, Science Journal Of Business And Management 4:(1), pp. 29-35., 2016, http://www.sciencepublishinggroup.com/journal/paperinfo?journalid=175&doi=10.11648/j.sjbm.s.2016040101.15 , (letöltve: 2017. október 8.)

[77] Magyar, S.: Az informatikai biztonságtudatosság jelentősége az adatvédelem területén, Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat Tudományos-Szakmai Folyóirata, 2015:(2), pp. 121-128., 2015, http://www.knbsz.gov.hu/hu/letoltes/szsz/2015_2_szam.pdf , (letöltve: 2017. december 3.)

[78] Michelberger, P. – Keszthelyi, A.: Információbiztonság alapjai – mesterfokon, Informatika a felsőoktatásban, Debrecen, Debreceni Egyetem Informatikai Kar, 2011., pp. 579-583., ISBN:978-963-473-461-1

[79] Simon, L. – Magyar, S.: A terrorizmus és indirekt hatása a kiberterében, Nemzetbiztonsági Szemle, 2017:(3), pp. 89-101., 2017, https://epa.oszk.hu/02500/02538/00020/pdf/EPA02538_nemzetbiztonsagi_szemle_2017_03_089-101.pdf , (letöltve: 2017. december 18.)

[80] Rajnai, Z. – Kocsis, I.: Labor Market Risks of Industry 4.0, Digitization, Robots and AI, IEEE 15th International Symposium on Intelligent Systems and Informatics : SISY 2017. Szabadka, Szerbia, New York, IEEE, 2017. pp. 343-346., ISBN:978-1-5386-3855-2, https://ieeexplore.ieee.org/document/8080580 , (letöltve: 2017. december 28.)

[81] Pokorádi L.: Komplex kapcsolatú rendszerek megbízhatóságának moduláris érzékenységelemzése, Repüléstudományi Közlemények XXVII:(1), pp. 81-89., 2015, https://www.researchgate.net/publication/283268703_KOMPLEX_KAPCSOLATU_RENDSZEREK_MEGBIZHATOSAGANAK_MODULARIS_ERZEKENYSEGELEMZESE , (letöltve: 2017. november 30.)

[82] Kerti, A.: Cyberterrorisme, Az 5. Báthory-Brassai Konferencia tanulmánykötetei. 709 p., Budapest, Óbudai Egyetem Biztonságtudományi Doktori Iskola, 2014., pp. 284-286.1-2. köt., ISBN:978-615-5460-38-8, http://www.bbk.alfanet.eu/userspace/5bbk2014_minden/5BBK2014__Kiadvany_1-2_kotet.pdf , (letöltve: 2017. szeptember 8.)

[83] Dombora, S. – Michelberger, P.: Információbiztonság szerepe az üzleti folyamatokban, International Journal of Engineering and Management Sciences 1:(1) p. &. 11 p., 2016, https://www.researchgate.net/publication/306042003_Informaciobiztonsag_szerepe_az_uzleti_folyamatokban , (letöltve: 2017. december 3.)

[84] Rajnai, Z. – Kerti, A.: A kormányzati IT rendszerek technológia-upgrade lehetősége, Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem, 2011., 132 p.

[85] Kerti, A: A vezetési és információs rendszer technikai alrendszerének vizsgálata különös tekintettel a minőségbiztosításra és az átvitelbiztonságra, 120 p. 2010., http://ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/9697/Teljes%20szöveg%21?sequence=1&isAllowed=y , (letöltve: 2016. október 18.)

[86] Keszthelyi, A.: Valódi, vagy csak annak vélt biztonság a böngészésben: SSL tanúsítványok, Taylor, Gazdálkodás- És Szervezéstudományi Folyóirat, A Virtuális Intézet Közép-Európa Kutatására Közleményei 8, (1), pp. 160-167., 2016, http://acta.bibl.u-szeged.hu/54951/ , (letötlve: 2017. december 5.)

[87] Kim, M. K. – Xie, K. – Cheng, S. L.: Building teacher competency for digital content evaluation, Teaching and Teacher Education, Elsevier, Volume 66, August 2017, Pages 309–324, https://doi.org/10.1016/j.tate.2017.05.006, http://www.sciencedirect.com/science?_ob=ShoppingCartURL&_method=add&_eid=1-s2.0-S0742051X16304140&_ts=1496105080&md5=e7240273e9c6716c47e9e5ac4baeb977 (letöltve: 2017.03.18)

[88] Kerti, A.: Az információbiztonsági kockázatkezelés oktatásának buktatói, Kommunikáció 2013. 213 p., Budapest, Nemzeti Közszolgálati Egyetem, 2013., pp. 53-60., ISBN:978-615-5305-16-0

[89] Rajnai, Z.: Mit jelent a kockázatelemzés, Kockázatelemzés, kockázatértékelés, tanulmányok az Óbudai Egyetem Biztonságtudományi Doktori Iskola kutatásaiból., 207 p. Budapest, Óbudai Egyetem, 2013., pp. 7-43., ISBN:978-615-5018-98-5

[90] Rajnai, Z.: Elektronikus adatkezelő rendszerek kockázat elemzési módszerei, A Magyar Tudomány Napja a Délvidéken 2014., 568 p., Újvidék, Vajdasági Magyar Tudományos Társaság, 2015., pp. 491-509., ISBN:978-86-88077-07-1,

[91] Rajnai, Z. – Mógor T.né: Elektronikus adatkezelő rendszerek kockázatelemzése, a kockázati módszerek bemutatása, Bolyai Szemle, 4:(2), pp. 43-59., 2014, Nemzeti Közszolgálati Egyetem, https://folyoiratok.uni-nke.hu/document/uni-nke-hu/bolyai-szemle-2014_-ev-2_-szam.original.pdf , (letöltés: 2017. október 5.)

[92] Farkas, T.: Tasks of the Hungarian Defence Forces in Disaster and Crisis Situation: Communication and information services and capabilities, 2016 New Trends in Signal Processing (NTSP), Demanovska Dolina, 2016, pp. 1-4. DOI: 10.1109/NTSP.2016.7747779,

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7747779&isnumber=7747773, letöltve: 2017. november 20.

[93] Szűcs, E.: Munkavédelmi szakmai továbbképzés mérnöktanárok részére - Fingerprint security, IESB 2011, Budapest, Óbudai Egyetem, 2011., pp. 14-18., ISBN:978-615-5018-15-2

[94] Tohoma, A.: A budapesti telefonhírmondó keletkezéséről (Puskás Tivadar és Szmaszenka Nándor alkotása), A Magyar Mérnök- és Építész-Egylet Közleménye, LXXIII. köt. 35-36. szám, 275-279 oldal, Budapest, 1939, http://dokutar.omikk.bme.hu/collections/mee/fajlok/1939-275-278.pdf, letöltve: 2017. 09.20.

[95] Kolossváry, E.: A magyar posta beruházási tervezete és az automatikus távbeszélő kiszolgálás ismertetése I-II., A Magyar Mérnök- és Építész-Egylet Közleménye, LVI. kötet 36-37., szám, 285-291 oldal, Budapest, 1922, http://dokutar.omikk.bme.hu/collections/mee/fajlok/1922-285-291.pdf, LVI. kötet 38-39. szám, 295-300 oldal, Budapest, 1922, http://dokutar.omikk.bme.hu/collections/mee/fajlok/1922-295-300.pdf, (letöltve: 2017. 09.20.)

[96] Puskás, A. – Csáky, E. – Rajnai, Z.: Puskás Tivadar, a nagy magyar feltaláló, Budapest, 2012. http://www.puskashirbaje.hu/index_html_files/Puskas_T_a_magyar_felt.pdf, (letöltés: 2017.10.01.)

[97] Koromzay, F.: Az elektromágneses hullámok és a drót nélkül való telegráfozás, A Magyar Mérnök- és Építész-Egylet Közleménye, XXXIV. kötet, IX. füzet, 205-213 oldal, Budapest, 1900, http://dokutar.omikk.bme.hu/collections/mee/fajlok/1900-205-213.pdf, (letöltve: 2017.10.01.)

[98] Szesztay, L.: A fotográfia a technikai tudományok szolgálatában. A Magyar Mérnök- és Építész-Egylet Közleménye, XXXIII. kötet III. füzet. 94-100 oldal, Budapest, 1899, http://dokutar.omikk.bme.hu/collections/mee/fajlok/1899-94-100.pdf, (letöltve: 2017. 09.21.)

[99] Bitay, E: A magyar műszaki nyelv úttörői. Debreczeni Márton műszaki öröksége, A XVI. Műszaki Tudományos Ülésszak előadásai, 39-50 oldal, Kolozsvár, 2015, Erdélyi Múzeum-Egyesület (EME), 2016, http://eda.eme.ro/bitstream/handle/10598/29732/XVI_MTU-Bitay2.pdf?sequence=3, (letöltve: 2017. 09.21.)

[100] Bagyinszki, Gy. – Bitay, E.: Bevezetés az anyagtechnológiák informatikájába. Műszaki Tudományos Füzetek 3., 213 oldal, EME, Kolozsvár/ 2007. ISBN 973-8231-65-5, ISBN 978-973-8231-65-8. http://eda.eme.ro/handle/10598/8942, (letöltve: 2017. 09.21.)

[101] Mester, Gy. – Pletl, Sz. – Pajor, G. – Rudas, I.: Adaptive Control of Robot Manipulators with Fuzzy Supervisor Using Genetic Algorithms, Proceedings of International Conference on Recent Advances in Mechatronics, ICRAM'95, O. Kaynak (ed.), Vol. 2, pp. 661–666, ISBN 975-518-063-X, Istanbul, Turkey, 1995.,

[102] Gombás, L. – Makay, K.: Mesterségünk az értelem és a védelem: Az AI és az IT közös útja, ITBN ConfExpo, 2017, https://youtu.be/RoezMok8fbY, (letöltve: 2017. október 1.)

[103] Iantovics, L.B. – Emmert-Streib, F. – Arik, S.: MetrIntMeas a novel metric for measuring the intelligence of a swarm of cooperating agents, Cognitive Systems Research, Volume 45, October 2017, 17-29, ISSN: 1389-0417, http://www.sciencedirect.com/science/article/pii/S1389041716300948, (letöltve: 2017. 09.21.)

[104] Iantovics, L.B. – Enăchescu, C.: Intelligent Complex Evolutionary Agent-Based Systems, in Proc. of the 1st Int. Conf. on Bio-Inspired Computational Methods Used for Solving Difficult Problems – Development of Intelligent and Complex Systems, BICS 2008, American Institute of Physics Proceedings, AIP 1117, 2009, 116-124 oldal, ISBN:978-0-7354-0654-4, ISSN:0094-243. http://aip.scitation.org/doi/abs/10.1063/1.3130613?journalCode=apc, (letöltve: 2017. 09.21.)

[105] Zamfirescu, C.B. – Duta, L. – Iantovics, L.B.: The Cognitive Complexity in Modelling the Group Decision Process, Special Issue on Complexity in Sciences and Artificial Intelligence, Journal: BRAIN. Broad Research in Artificial Intelligence and Neuroscience, B. Iantovics, D. Radoiu, M. Marusteri, Matthias Dehmer (Eds.). July, 2010, 66-76 oldal. https://sic.ici.ro/wp-content/uploads/2010/09/SIC_2010-3-Art6.pdf, (letöltve: 2017. 09.21.)

[106] Kovács-C, T. – Bitay, E.: The hardness control in the coated surface layer, Materials Science Forum, Vol. 729 Trans Tech Publications, Switzerland, ISSN: 1662-9752, 2013. 415–418 p. DOI: 10.4028/www.scientific.net/MSF.729.415, http://www.scientific.net/MSF.729.415, (letöltve: 2017. 09.21.)

[107] Bitay, E. – Kovács, T.: The effect of the laser surface treatments on the wear resistance, Materials Science Forum Vol. 649., Trans Tech Publications Ltd, Switzerland, ISSN:

1662-9752, 2010. 107–112 p. http://www.scientific.net/MSF.649.107, (letöltve: 2017. 09.21.)

[108] Schuster, Gy. – Tokody, D. – Mezei, I. J.: Software reliability of complex systems focus for intelligent vehicles, Vehicle and Automotive Engineering. Lecture Notes in Mechanical Engineering, 2017. ISSN: 2195-4356, pp. 309–321., Springer, Cham, DOI 10.1007/978-3-319-51189-4_28, https://link.springer.com/chapter/10.1007/978-3-319-51189-4_28, (letöltve: 2017. 09.21.)

[109] Farkas, T. – Hronyecz, E.: A digitális katona rendszer a katasztrófavédelmi műveletekben, A XXII. Fiatal műszakiak tudományos ülésszak előadásai - teljes kötet, Kolozsvár, pp. 147–150., 2017, URI: http://hdl.handle.net/10598/29767 , https://eda.eme.ro/bitstream/handle/10598/29767/XXII_FMTU_FarkasTibor-HronyeczErika.pdf?sequence=3&isAllowed=y , (letöltve: 2018. február 10.)

[110] Rodic, A. – Mester, Gy. – Stojković, I.: Qualitative Evaluation of Flight Controller Performances for Autonomous Quadrotors, 115-134, Intelligent Systems: Models and Applications, Endre Pap (Ed.), Topics in Intelligent Engineering and Informatics, Vol. 3, Part. 2, TIEI 3, ISSN 2193-9411, e-ISSN 2193-942X, ISBN 978-3-642-33958-5, e-ISBN 978-3-642-33959-2, DOI 10.1007/978-3-642-33959-2_7, Springer-Verlag Berlin Heidelberg, 2013. 115-134 oldal, https://link.springer.com/chapter/10.1007%2F978-3-642-33959-2_7?LI=true, (letöltve: 2017. szeptember 20.)

[111] Hercegfi, K.: Multimédia oktatóanyag fejlesztésének és bevezetésének minőségbiztosítási kérdései, doktori (Ph.D.) értekezés, Budapest, 2005. 24 oldal, http://erg.bme.hu/mtars/hercegfi/Hercegfi_PhD.pdf, letöltve: 2017. szeptember 20.

[112] The UX Five-Second Rules: Guidelines for User Experience Design's Simplest, https://books.google.hu/books?id=b7XrAgAAQBAJ&printsec=frontcover&hl=hu#v=onepage&q&f=false , (letöltve: 2017. szeptember 21.)

[113] Internet Use in Children, American Academy of Child and Adolescent Psychiatry, Fackt for Familie, No. 59, 2015, https://www.aacap.org/AACAP/families_and_Youth/facts_for_families/FFF-Guide/Children-Online-059.aspx , (letöltve: 2017. november 4.)

HIVATKOZOTT JOGSZABÁLYOK ÉS SZABVÁNYOK

[114] Az Európai Parlament És A Tanács Ajánlása, (2006. december 18.) az egész életen át tartó tanuláshoz szükséges kulcskompetenciákról (2006/962/EK), http://ejam.hu/sites/default/files/kepek/kepek/upload/1-Programok-tananyagok/JAM-tananyagok/5-szakmai-anyagok/Az-egesz-eleten-at-tarto-tanulashoz-szukseges-kulcskompetenciakrol.pdf, (letöltve: 2017 06.10.)

[115] Parlament és a Tanács (EU) 2016/1148 számú irányelve, https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.HUN , (letöleve: 2017. 06.12.)

[116] 1069/2014. (II.19.) Korm. határozat Magyarország Nemzeti Infokommunikációs Stratégiájáról

[117] 1631/2014. (XI. 6.) Korm. határozat a „Digitális Nemzet Fejlesztési Program" megvalósításáról

[118] 2012/2015. (XII. 29.) Korm. határozat az internetről és a digitális fejlesztésekről szóló nemzeti konzultáció (InternetKon) eredményei alapján a Kormány által végrehajtandó Digitális Jólét Programjáról

[119] 1488/2016. (IX. 2.) Korm. határozat a Gyermekek Számára Biztonságos Internetszolgáltatás megteremtéséről, a tudatos és értékteremtő internethasználatról és Magyarország Digitális Gyermekvédelmi Stratégiájáról

[120] 1456/2017. (VII. 19.) határozata a Nemzeti Infokommunikációs Stratégia (NIS) 2016. évi monitoring jelentéséről, a Digitális Jólét Program 2.0-ról, azaz a Digitális Jólét Program kibővítéséről, annak 2017–2018. évi Munkaterve elfogadásáról, a digitális infrastruktúra, kompetenciák, gazdaság és közigazgatás további fejlesztéseiről

[121] 1603/2014. (XI. 4.) számú Korm. határozat a Magyar nemzeti társadalmi felzárkózási stratégia II., Az egész életen át tartó tanulás szakpolitikájának keretstratégiája, a Köznevelés-fejlesztési stratégia, továbbá a Végzettség nélküli iskolaelhagyás elleni középtávú stratégia elfogadásáról

[122] 1672/2015. (IX. 22.) Korm. határozat a Magyar nemzeti társadalmi felzárkózási stratégia II. végrehajtásának a 2015-2017. évekre szóló kormányzati intézkedési tervéről

[123] 2009. évi CLV. törvény a minősített adat védelméről

[124] 90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről

[125] 92/2010. (III. 31.) Korm. rendelet az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairól

[126] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól

[127] 1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

[128] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

[129] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

[130] 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról

[131] 484/2013. (XII. 17.) Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről

[132] 185/2015. (VII. 13.) Korm. rendelet a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól

[133] 186/2015. (VII. 13.) Korm. rendelet a központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről

[134] 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról

[135] 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

[136] 2007. évi XCII. törvény a Fogyatékossággal élő személyek jogairól szóló egyezmény és az ahhoz kapcsolódó Fakultatív Jegyzőkönyv kihirdetéséről

[137] Az Európai Unió Alapjogi Chartája 2012/C 326/02, III. Cím: Egyenlőség

[138] Magyarország Alaptörvénye (2011. április 25.)

[139] 1998. évi XXVI. törvény a fogyatékos személyek jogairól és esélyegyenlőségük biztosításáról

[140] 2003. évi CXXV. törvény az egyenlő bánásmódról és az esélyegyenlőség előmozdításáról

[141] 305/2005. (XII. 25.) Korm. rendelet a közérdekű adatok elektronikus közzétételére, az egységes közadatkereső rendszerre, valamint a központi jegyzék adattartalmára, az adatintegrációra vonatkozó részletes szabályokról

[142] ISO/IEC 40500:2012 Information technology — W3C Web Content Accessibility Guidelines (WCAG) 2.0

[143] 62/2011. (XI. 10.) NEFMI rendelet a jelnyelvi tolmácsszolgálatok működésének és a jelnyelvi tolmácsszolgáltatás igénybevételének feltételeiről

[144] MSZ EN 301 549:2014, Európai közbeszerzési ICT-termékek és -szolgáltatások hozzáférhetőségi követelményei

[145] ISO 9241-1:1997 szabvány, https://www.iso.org/standard/21922.html, (letöltve: 2017. szeptember 21.)

[146] ISO 9241-11:1998 szabvány, https://www.iso.org/standard/16883.html, (letöltve: 2017. szeptember 21.)

[147] ISO 9241-13:1998 szabvány, https://www.iso.org/standard/16883.html, (letöltve: 2017. szeptember 21.)

[148] ISO 9241-14:1997 szabvány, https://www.iso.org/standard/16886.html, (letöltve: 2017. szeptember 21.)

[149] ISO 9241-15:1997 szabvány, https://www.iso.org/standard/16887.html, (letöltve: 2017. szeptember 21.)

[150] ISO 9241-16:1999 szabvány, https://www.iso.org/standard/16888.html, (letöltve: 2017. szeptember 21.)

[151] ISO 9241-110:2006 szabvány, https://www.iso.org/standard/38009.html,

[152] ISO 9241-112:2017 szabvány, https://www.iso.org/standard/64840.html, (letöltve: 2017. szeptember 21.)

[153] ISO 9241-125:2017 szabvány, https://www.iso.org/standard/64839.html, (letöltve: 2017. szeptember 21.)

[154] ISO 9241-302:2008 szabvány, https://www.iso.org/standard/40097.html, (letöltve: 2017. szeptember 21.)

[155] ISO 9241-305:2008 szabvány, https://www.iso.org/standard/40100.html, (letöltve: 2017. szeptember 21.)

HIVATKOZOTT SAJÁT PUBLIKÁCIÓK

[156] Nyikes, Z.: Digital Competence and the Safety Awareness Base on the Assessments Results of the Middle East-European Generations, 11th International Conference Interdisciplinarity in Engineering, INTER-ENG 2017, 2017, Tirgu-Mures, Romania, DOI: https://doi.org/10.1016/j.promfg.2018.03.130 , (letöltve: 2018.04.03.)

[157] Nyikes, Z.: A Közép-Kelet európai generációk digitális kompetencia és biztonságtudatosság vizsgálatának eredményei, Hadmérnök, XII. Évfolyam 4. szám, 2017, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, pp. 159-173, ISSN 1788-1919, http://hadmernok.hu/174_16_nyikes.pdf , (letöltve: 2017.12.4.)

[158] Nyikes, Z.: A Digitális Kompetencia Értékelési Rendszerének Egyes Kérdései, Kolozsvár, Erdélyi Múzeum Egyesület (EME); Óbudai Egyetem, 2017., pp. 323-326., Műszaki Tudományos Közlemények 7., ISBN:978-963-449-018-0, http://real.mtak.hu/54554/1/XXII_FMTU_NyikesZ1_DigitalisKompetencia_u.pdf , (letöltve: 2018.02.10.)

[159] Nyikes, Z: A biztonságtudatosság a digitális kompetencia tükrében, Műszaki Tudományos Közlemények 5, pp. 313-316., 2016 Kolozsvár, Románia, https://eda.eme.ro/bitstream/handle/10598/29092/EME_21_FMTU_2016_NyikesZoltan_A_biztonsagtudatossag.pdf?sequence=3 , (letöltve: 2017.02.21.)

[160] Nyikes, Z. – Kerti, A.: A digitális kompetencia napjainkban, Proceedings of 8th International Engineering Symposium at Bánki (IESB 2016), Budapest, Óbudai Egyetem, 2016., 56. 6 p., ISBN:978-615-5460-95-1, http://bgk.uni-obuda.hu/iesb/2016/publication/56.pdf , (letöltve: 2017. 02.22.)

[161] Nyikes, Z.: Contemporary Digital Competency Review, Interdisciplinary Description of Complex Systems, INDECS, 16(1), pp. 124-131, 2018, DOI: 10.7906/indecs.16.1.9, http://indecs.eu/index.php?s=x&y=2018&p=124-131, (letöltve: 2018.06.10.)

[162] Nyikes, Z. – Baimakova, K.V.: An Examination of the Relationship between Security Awareness and Digital Competence, Proceedings of the 6th International Conference on Applied Internet and Information Technologies, Bitola, Macedónia, St. Kliment Ohridski University, Faculty of Information and Communication Technologies, 2016. pp. 104-111., ISBN:978-9989-870-75-0, http://docplayer.net/93725380-Proceedings-of-the-6-international-conference-on-applied-internet-and-information-technologies-bitola-3-4-june-2016.html , (letöltve: 2017.05.10.)

[163] Nyikes, Z.: A biztonságtudatosság fejlesztésének egyes lehetőségei, Kolozsvár, Erdélyi Múzeum Egyesület (EME); Óbudai Egyetem, 2017., pp. 327-330., Műszaki Tudományos Közlemények 7., ISBN:978-963-449-018-0, http://real.mtak.hu/54553/1/XXII_FMTU_NyikesZ2_Biztonsagtudatossag_u.pdf , (letöltve: 2017.12.14.)

[164] Balázs, D. Á. – Nyikes, Z. – Kovács, T.: Building Protection with Composite Materials Application, Key Engineering Materials, Vol. 755, pp. 286-291, 2017, 10.4028/www.scientific.net/KEM.755.286, https://www.scientific.net/KEM.755.286.pdf , (letöltve: 2017.08.21.)

[165] Nyikes, Z.: A Digitális Kompetencia És A Biztonságtudatosság Korrelációja, Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat Tudományos-Szakmai Folyóirata, 2016, (1), pp. 82-88., http://hadmernok.hu/174_16_nyikes.pdf , (letöltve: 2018.02.10.)

[166] Nyikes, Z.: Creation Proposal for the Digital Competency Framework of the Middle-East European Region, Key Engineering Materials, ISSN: 1662-9795, Vol. 755, pp 106-111, DOI: 10.4028/www.scientific.net/KEM.755.106, https://www.scientific.net/KEM.755.106, (letöltve: 2017. 09. 21.)

[167] Nyikes, Z. – Rajnai, Z.: Big Data, As Part of the Critical Infrastructure, SISY 2015, IEEE 13th International Symposium on Intelligent Systems and Informatics, Serbia, Zrenjanin, 2015., pp. 217-222., ISBN:978-1-4673-9388-1, https://ieeexplore.ieee.org/document/7325383 , (letöltve: 2017.08.15.)

[168] Kovács, T. – Nyikes, Z. – Tokody, D.: Komplex monitoring-rendszer használata vasúti felépítmény vizsgálatában az Ipar 4.0-hoz, XVII. Műszaki Tudományos Ülésszak előadásai. ISSN 2393–1280, EME, MTK 6. szám, Kolozsvár, 2017, http://eda.eme.ro/handle/10598/30075?show=full, (letöltve: 2017. szeptember 20.)

[169] Nyikes, Z.: A szoftver-ergonómiai megoldások a biztonságtudatosság növelése érdekében, XVIII. Műszaki Tudományos Ülésszak, Műszaki tudományos közlemények 8., Kolozsvár, Románia, 2017., https://anzdoc.com/xviii-mszaki-tudomanyos-lesszak.html , (letöltve: 2018.06.10.)

[170] Nyikes, Z.: A felhasználók biztonságának növelése internetes segélyhívó rendszer alkalmazásával, Hadmérnök, XIII. Évfolyam 1. szám, 2018, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, pp. 278-285, ISSN 1788-1919, http://hadmernok.hu/181_22_nyikes.pdf , (letöltve: 2018.04.02.)

[171] Nyikes, Z.: Compensation of Digital Competence Deficiency with Software Ergonomic Tools, Interdisciplinary Description of Complex Systems, INDECS, 16(1), pp. 132-138,

2018, DOI:10.7906/indecs.16.1.10, http://indecs.eu/index.php?s=x&y=2018&p=132-138 , (letöltve: 2018.06.15.)

[172] Kerti, A. – Nyikes, Z.: Információbiztonsági kérdések a szolgálati és magántulajdonú mobil infokommunikációs eszközök esetében (1.), Honvédségi Szemle: A Magyar Honvédség Központi Folyóirata, 143:(5), pp. 75-82., 2015, ISSN 2060-1506, https://honvedelem.hu/kiadvany/52370 , (letölve: 2016.02.08.)

[173] Kerti, A. – Nyikes, Z.: Információbiztonsági kérdések a szolgálati és magántulajdonú mobil infokommunikációs eszközök esetében (2.), Honvédségi Szemle: A Magyar Honvédség Központi Folyóirata, 143:(6), pp. 85-99., 2015, ISSN 2060-1506, https://honvedelem.hu/kiadvany/53085 , (letöltve: 2016.05.10.)

[174] Nyikes, Z. – Rajnai, Z.: A BIG DATA alkalmazása a nemzeti digitális közműben, Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat Tudományos-Szakmai Folyóirata, 2015. 4. szám, pp. 103-118., 2015, ISSN 1785-1181, http://knbsz.gov.hu/hu/letoltes/szsz/2015_4_szam.pdf ,(letöltve: 2017.06.21.)

[175] Nyikes, Z.: A „Nagy Adat”, mint a létfontosságú rendszerek része, HÍRVILLÁM = SIGNAL BADGE, 6:2015/2, pp. 39-55., 2015, ISSN 2061-9499, http://www.comconf.hu/kiadvany/hirvillam_6evfolyam_2szam.pdf , (letöltve: 2017.08.09.)

[176] Nyikes, Z. – Rajnai, Z.: The Big Data and the relationship of the Hungarian National Digital Infrastructure, International Conference on Applied Internet and Information Technologies : ICAIIT 2015: Proceedings. 258 p. Zrenjanin, Szerbia: University of Novi Sad, pp. 6-12., 2015, ISBN:978-86-7672-261-7, https://www.researchgate.net/profile/Phuoc_Dai_Nguyen/publication/303338805_e-Proceedings/links/573d8a4608ae9f741b2fb839.pdf#page=19 , (letöltve: 2017.11.12.)

[177] Nyikes, Z. – Rajnai, Z.: The BIG DATA Application to the Hungarian National Digital Infrastructure, Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat Tudományos-Szakmai Folyóirata, Special issue, pp. 74-85., 2015, http://knbsz.gov.hu/hu/letoltes/szsz/2015_2_spec.pdf , (letöltve: 2017.04.10.)

.

ÁBRAJEGYZÉK

RÖVIDÍTÉSEK ÉS IDEGEN SZAVAK GYŰJTEMÉNYE

4G	vezeték nélküli adatkapcsolati technológia
Baby-boom	születési szám megnövekedése, generációs korszak
BigData	Nagy Adat – adatfeldolgozási technológia
BSc	Bachelor of Science, alapképzés
CD/DVD	Compact Disc, kompaktlemez / Digital Versatile Disc, digitális sokoldalú lemez
Chat	olyan társalgási forma, amely 2 vagy több ember között online (leggyakrabban az interneten keresztül) történik.
cloud technology	felhőalapú számítástechnika
CLV	155
connecting	folyamatosan kapcsolatban lévő, a közösségi oldalhoz kapcsolódva
cyberbullying	internetes zaklatás
DESI	The Digital Economy and Society Index - A digitális gazdasági és társadalmi fejlettséget mérő mutató
DevOps	"development" és "operations" szavak összevonása, azaz "fejlesztés" és "műveletek"; a szoftverfejlesztést (Dev) egyesíti az informatikai műveletekkel (Ops).
dirty pc	Olyan önálló számítógép, amely speciális rendszerek védelmét biztosítja
DJP	Digitális Jólét Program
DJP2.0	Digitális Jólét Program 2.0, második rész
DMP	Digitális Munkaerő Program
DNFP	Digitális Nemzet Fejlesztési Program
DOS	Digitális Oktatási Stratégia
DQ	Digital Intelligence, digitális intelligencia
DuoLingo	ingyenes, nyelvtanulásra szolgáló weboldal és mobilalkalmazás
eBay	a legnagyobb online aukciós oldal
ECDL	European Computer Driving Licence, Európai Számítógép-használói Jogosítvány
EDPR	Európa digitális fejlődéséről szóló jelentés
EDVAC	Electronic Discrete Variable Automatic Computer, elektronikus diszkrét változós automata számítógép
e-mail	electronic mail, elektronikus levél
ENSZ	Egyesült Nemzetek Szervezete
EPT	Európai Parlament és Tanács
EU	Európai Unió
EU Kids online	Európai nemzetközi kutatási hálózat.
Exabájt	SI - 1018 = 10006; Bináris – (EiB) 260
Facebook	amerikai alapítású közösségi hálózat
Felhő-tárhely	felhőalapú tároló szolgáltatás
GDP	gross domestic product, bruttó hazai termék
google	internetes keresőrendszer
google maps	a google által fejlesztett ingyenes internetes térképszolgáltatás

GoogleForm	Google Űrlapok
HD	High Density, Nagy sűrűség
hotspot	egy nyilvános, vezeték nélküli (WiFi) internet-hozzáférési pont
IBTV	2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
ICT	Infocommunication Technology, Infokommunikációs Technológia
iGo	navigációs program
IKT	Infokommunikációs Technológia
Instagram	egy közösségi hálózat, amely fényképek és rövid videók okostelefonon történő megosztásán alapul.
IoT	Internet of Things, a dolgok internete
IPAR 4.0	A 4. ipari forradalom, az ipar digitális transzformációja
iPhone	az Apple által tervezett és gyártott okostelefon
IP-kamera	Internet Protocol-t használó vagyonvédelmi kamera
ISO/IEC	International Organization for Standardization - Nemzetközi Szabványügyi Szervezet / International Electrotechnical Commission, Nemzetközi Elektrotechnikai Szabványbizottság
IST	Information Society Technology – információs társadalmi technológiák
IT	Information Technology, információs technológia
Jófogás	Magyarország egyik online apróhirdetési oldala
KKV	Kis- és Közép Vállalkozások
Knock kód	Kopogtató kód, az LG védelmi megoldása
KSH	Központi Statisztikai Hivatal
Korm. rendelet	Kormányrendelet
laptop	hordozható számítógép
lifelong learning	élethosszig tartó tanulás
LinkedIn	a világ legnagyobb üzleti közösségi hálózata
Mbps	megabit per secundum. adatátviteli sebesség mértékegysége
malware	az angol malicious software rövidítése, magyarul rosszindulatú szoftver
Messenger	a facebook üzenetküldő alkalmazása okostelefonokra/táblagépekre
Morse kód	kommunikációs kód, amely szöveges információátvitelt tesz lehetővé
Mrd	milliárd
MS PowerPoint	prezentációk készítésére alkalmas irodai program
MSc	Magister Scientiæ, mesterképzés
MSZ EN	Magyar Szabvány European Norm, európai szabvány
NATO	North Atlantic Treaty Organisation, Észak-atlanti Szerződés Szervezete
NEFMI	Nemzeti Erőforrás Minisztérium
NEPTUN	Egységes Tanulmányi Rendszer
NGA	nagy sebességű vezetékes szélessáv
NIS	Nemzeti Infokommunikációs Stratégia
NIS irányelvek	Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről
NMHH	Nemzeti Média- és Hírközlési Hatóság

Northeastern University	Egyetem, Boston, Massachusetts, USA
OECD	Organisation for Economic Cooperation and Development, Gazdasági Együttműködési és Fejlesztési Szervezet
offline	Az offline átvitt értelemben azokat a folyamatokat, fogalmakat is jelenti, amelyek működésükben az Internettől és a virtuális kibertértől független módon léteznek vagy működnek.
online	rendszerhez, hálózathoz kapcsolt
PC	Personal Computer, személyi számítógép
pendrive	USB-flash-tároló, USB-kulcs, tollmeghajtó
PhD	philosophiæ doctor, A filozófia tanítója, tudományos fokozat
PIN kód	Personal Identification Number, személyi azonosító szám, titkos kód
Rock' n' roll	zenei stílus és tánc, generációs korszak
ransomware	zsarolóvírus
safety	biztonság, veszélytelenség
security	biztonság
shadow IT	árnyékinformatika
Skype	egy világhálós telefonálóprogram, mely 100%-ig ingyenes
SMART	intelligens, okos, általában internetképes eszköz
soft skillek	puha faktorok, soft készségek
SWOT	Strengths, Weaknesses, Opportunities, Threats, analízis módszer
tablet	táblagép, hordozható számítógép
Terrabit/sec	adatátviteli sebesség mértékegysége
Tinydeal	kínai webáruház
Torrentezés	egy fájlcserélő protokoll használata
tsai	Társai
TV	televízió
Twitter	ismeretségi hálózat és mikroblog-szolgáltatás,
UNICEF	United Nations International Children's Emergency Fund, Egyesült Nemzetek Nemzetközi Gyermek Gyorssegély-alapja
USA	United States of America, Amerikai Egyesült Államok
Ügyfélkapu	a magyar kormányzat elektronikus ügyfélbeléptető és azonosító rendszere.
Vatera	Magyarország legnagyobb online piactere
Viber	egy okostelefonra készített ingyenes VoIP szolgáltatás
virtual reality	virtuális valóság
VoIP	Az internetprotokoll feletti hangátvitel – elterjedt nevén VoIP, Voice over IP vagy IP-telefónia – a távközlés egy formája
W3C	World Wide Web Consortium, egy konzorcium, mely nyílt szoftver szabványokat – „ajánlásokat", ahogy ők hívják – alkot a világhálóra
Waze	ingyenes GPS navigációs mobiltelefon alkalmazás
WCAG 2.0	Web Content Accessibility Guidelines 2.0, Web Akadálymentesítési Útmutató 2.0
weblap	számítógépes dokumentum, mely megfelel a World Wide Web számára

wifi	Wireless Fidelity; vezeték nélküli mikrohullámú kommunikációt megvalósító, széleskörűen elterjedt szabvány (IEEE 802.11)
WorldWideWeb	az interneten működő, egymással úgynevezett hiperlinkekkel összekötött dokumentumok rendszere
Yahoo	amerikai cég, amely egy internetes portált és katalógust üzemeltet
Youth	ifjúkor, fiatalkor
YouTube	nyilvános videómegosztó webhely

FÜGGELÉK

1. számú függelék

A biztonságtudatosság és a digitális kompetencia kapcsolata kérdőív

Készítette:
Nyikes Zoltán
doktorandusz hallgató
Óbudai Egyetem
Biztonságtudományi Doktori Iskola
nyikeszoli@gmail.com

1. **A felsoroltak közül Ön hol él?**
   - Fővárosban
   - Megyeszékhelyen
   - Városban
   - Községben

2. **Ön Magyarországon él?**
   - Igen
   - Nem

3. **Milyen korcsoporthoz tartozik?**
   - 18-24
   - 25-34
   - 35-50
   - 51, vagy annál idősebb

4. **Használja az internetet?**
   - Igen
   - Nem

5. **Van önnek hordozható okos eszköze? (mobiltelefon, tablet, laptop)**
   - Van
   - Nincs

6. **Szokott internetezni hordozható okos eszközön? (mobiltelefon, tablet, laptop)**
   - Igen
   - Nem

7. **A hordozható okos eszközön (több válasz is megjelölhető):**
   - Mobilinternetet használ (előfizetéshez kapottat).
   - Otthoni Wi-Fi hálózatot használ.
   - Nyílt Wi-Fi (Hotspot) hálózatot használ.
   - Vezetékes internetet használ.
   - Nem használ internetet.

8. **Milyen gyakran használja az internetet?**
   - Nem használta még.
   - Hetente párszor.
   - Naponta egyszer.
   - Naponta többször.
   - Folyamatosan használja az interneten.

9. **Beszél Ön angolul?**
   - Nem
   - Igen, "konyhanyelv" szinten.
   - Igen, alapszinten.
   - Igen, középszinten.
   - Igen, felsőszinten.
   - Igen, anyanyelvi szinten.

10. **Milyen szintűre értékeli a saját informatikai ismereteit és biztonságtudatosságát?**
    - Nincs semmilyen informatikai ismerete, nem tudja, mi az a biztonságtudatosság.
    - Használta már az internetet és hallott már a biztonságtudatosságról.
    - Rendszeresen használja az internetet, általában biztonságtudatos.
    - Az interneten kívül sok alkalmazást használ a számítógépen/okostelefonon, figyel a biztonságra.
    - Egyedül konfigurálja a számítógépet/okostelefont, általában figyelemmel követi a biztonsági trendeket.
    - A környezete kikéri az Ön véleményét az informatikai kérdésekben, naprakész ismerete van a biztonsági megoldások területén.

11. **Milyen szintű informatikai ismerettel rendelkezik? (több válasz is megadható)**
    - Van egyetemi/középiskolai informatikai végzettsége.
    - Az egyetemen/középiskolában tanult informatikát.
    - Tud programozni egy vagy több programnyelven.
    - Van ECDL vizsgája.
    - Informatikai tanfolyamot végezett.
    - Önmagától vagy ismerőse segítségével sajátította el.
    - Nem rendelkezik informatikai ismeretekkel.

12. **Használ vírusvédelmi-, vagy tűzfal alkalmazást azon (azokon) az eszközön(kön), amin internetezik?**
    - Igen
    - Nem
    - Egyéb:……

13. **A hordozható okos eszközén, használ védelmi megoldásokat? (több válasz is megadható)**
    - Nem.
    - Igen, de nem mindegyik eszközén használ védelmi megoldást.
    - Igen, minden eszközé használ védelmi megoldás.
    - Igen, feloldó-mintát.
    - Igen, jelszót/ PIN kódot/ Knock kódot/ ujjnyomat olvasót/ arcfelismerőt.
    - Igen, a telefon- és az adatok titkosítását.
    - Igen, az alkalmazások megnyitására külön feloldó kódot/mintát.

- Egyéb:……

14. Jelszavát, feloldó mintáját milyen gyakran változtatja?
- Nem szokta megváltoztatni.
- Igen, évente legalább egyszer.
- Igen, félévente legalább egyszer.
- Igen, havonta legalább egyszer.
- Igen, amikor eszébe jut.
- Igen, minden gyanús körülmény esetén.

15. Érte már vírus-, és/vagy egyéb rosszindulatú támadás az Ön eszközét/eszközeit?
- Igen.
- Nem.
- Nem tud róla.

16. **Esetleges vírustámadás, és/vagy egyéb rosszindulatú támadás esetén tisztában van** azzal, hogy mi a teendő?
- Igen, felméri a károkat, próbálja minimalizálni a kárt, értesíti a hatóságokat-, az üzemeltetőt.
- Igen, szakember segítségét kéri.
- Igen, szól a hozzáértő ismerősének, hogy segítsen.
- Megoldja egyedül.
- Nem tesz semmit.

17. Zaklatták már közösségi oldalon (pl. Facebook), vagy e-mail-ben Önt, vagy hozzátartozóját (barátját)?
- Igen, Önt.
- Igen, a hozzátartozóját/barátját.
- Nem.

18. **Mit tenne, ha zaklatnák Önt vagy hozzátartozóját, vagy mit tanácsolna ilyen esetben?** (több válasz is adható)
- Tudomást se vesz róla;
- Felhívja a zaklató, vagy gyalázkodó figyelmét, hogy fejezze be azt;
- Letiltja a zaklató profilját, e-mail-jét;
- Segítséget kér szakembertől;
- Értesíti az oldal-, szolgáltató szakembereit a zaklatásról;
- Értesíti a hatóságokat, és gondoskodik a bizonyítékok védelméről.

19. Vesztett-e el már véglegesen, pótolhatatlan digitális adatot/tartalmat? (családi fotó-videó, saját készítésű fájl, címlista)
- Igen
- Nem

20. Szokott-e készíteni az eszközén(ein) tárolt adatokról biztonsági másolatot? (több válasz is megjelölhető)
- Igen, külső, háttértárra szokott menteni (pendrive, memória kártya, külső merevlemez, CD/DVD).
- Igen, az adott eszköz belső tárolójára, elkülönítve.
- Igen, egy adott hálózat szerverére szokott menteni.

- Igen, felhő-tárhelyre szokott menteni.
- Nem szokott biztonsági mentést készíteni.
- Egyéb:……

21. Milyen gyakorisággal készít biztonsági másolatot?

- Naponta.
- Hetente.
- Havonta.
- Ritkábban.
- Csak bizonyos adatokról készít rendszertelenül. (pl. családi eseményen készült fotók esetében).
- Nem készít biztonsági másolatot.

22. Használ Ön a háztartásában okos (internetre csatlakoztatott) eszközt? (pl. TV, IP-kamera, hűtő, mosógép, vagyonvédelmi rendszer, intelligens otthon stb.)

- Nem.
- Nem tudja.
- Igen, TV-t.
- Igen, néhányat a felsoroltakból.
- Igen, többet is a felsoroltakból.
- Egyéb:……

23. Vett már részt valaha információbiztonsági oktatáson, képzésen?

- Nem.
- Nem emlékszik.
- Igen, egyszer.
- Igen, rendszeresen.

24. Ha lehetősége lenne egy ingyenes tanfolyam, vagy oktatás keretében digitális ismereteket elsajátítani, részt venne rajta?

- Igen.
- Nem.
- Nem tudja.

25. Amennyiben dolgozik, a munkájához szükséges az informatikai ismeret?

- Nem
- Igen, minimális ismeretek (betanított);
- Igen, közepes ismeretek (tanfolyam);
- Igen, magas fokú ismeretek (speciális végzettség, céltanfolyam).

26. Az internetet milyen célra használja általában? (több válasz is megjelölhető)

- Hírek, cikkek olvasására (origo, index, 444, stb.).
- Szakcikkek olvasására.
- Különböző keresők használatára (google, yahoo stb.).
- Navigációra, tájékozódásra (pl. google maps, Waze, iGo).
- E-mail-ek küldése, fogadása.
- Internetes telefonálásra (Skype, Viber, Messenger stb.).
- Chat-elésre (Skype, Viber, Messenger stb.).
- Közösségi oldalon olvasásra, posztolásra (Facebook, Twitter, LinkedIn, Instagram).

- Társkereső oldalak használatára.
- 18+ tartalmak megtekintésére.
- Torrentezésre.
- Filmnézésre (pl. YouTube).
- Játékra.
- Sportfogadásra, szerencsejátékra.
- Internetes vásárlásra/eladásra (pl. eBay, Vatera, Jófogás, Tinydeal).
- Tanulásra (pl. DuoLingo).
- Ügyintézésre (pl. Ügyfélkapu).
- Internetes bankolásra.
- Egyéb:……

27. Amennyiben javaslata, véleménye van a kérdőívvel vagy a fenti témákkal kapcsolatban, kérem, itt fejtse ki bővebben:

2. számú függelék:

A VVSZM Digitális Kompetencia Keretrendszer*

„Védendő” „Veszélyes” „Szerény” „Magabiztos”

	Védendő használó	Veszélyes használó	Szerény használó	Magabiztos használó
Tájékoztatás és adatfeldolgozás	Ezen a szinten a kezdő felhasználók nincs tisztában az internetes keresők használatával, nincs tisztában azzal, hogy az internetes tartalmak nem mindegyike megbízható. A fájlokat és tartalmakat nem minden esetben tudja menteni, vagy tárolni, és újra előhívni.	A felhasználó tud információt keresni online kereső használatával. Tudja, hogy nem minden internetes tartalom megbízható. Tud fájlokat/tartalmakat menteni, vagy tárolni (pl szöveg, képek, zene, viedók, weboldalak), és újra megnyitni őket.	A felhasználó különböző keresőket tud használni a megfelelő információ megtalálása érdekében. Keresésnél szűrőket is tud alkalmazni (pl. csak kép-, videó- vagy térképes találatok). Képes összehasonlítani a különböző forrásokat, hogy felmérje a talált információ megbízhatóságát. Fájlokba és mappákba csoportosítja az információkat, hogy utána könnyebben elérje. Biztonsági másolatot készít a lementett fájlokról és információkról.	A felhasználó képes haladó szintű keresési stratégiákat alkalmazni (pl. keresési üzemeltetők, Szerverek), hogy megbízható információt találjon az interneten. Tud internetes feed-eket használni (mint az RSS), hogy naprakész legyek a számára érdekes tartalmakból. Számos aspektusból fel tudja mérni az adott információ megbízhatóságát és érvényességét. Ismeri az információkeresés, -tárolás és -előhívás új módjait. El tudja menteni különböző formátumokban az interneten talált információkat. Tud felhőszolgáltatást használni.
Kommunikáció és együttműködés	A felhasználó tud kommunikálni másokkal mobiltelefon, azonban az azonnali üzenetküldő szolgáltatás, VoIP (pl. Skype), email vagy chat alapfunkciók használatával nincs tisztában. Önállóan nem tud fájlokat és tartalmakat megosztani. Nincs tisztában azzal, hogy különböző szolgáltatásokat vehet igénybe interneten keresztül. Ismer néhány közösségi oldalt de egyedül nem tudja használni, vagy a bonyolultabb műveletekre nem képes. Csak fogalmi szinten van tudatában annak, hogy digitális eszközök használatakor bizonyos kommunikációs szabályokat be kell tartani.	A felhasználó tud kommunikálni másokkal mobiltelefon, azonnali üzenetküldő szolgáltatás, VoIP (pl. Skype), email vagy chat alapfunkciók használatával (pl. hangüzenet, SMS, e-mail küldés és fogadás, szöveges üzenetváltás). Tud fájlokat és tartalmakat megosztani egyszerű eszközök használatával. Tudja, hogy különböző szolgáltatásokat vehet igénybe interneten keresztül (pl. hivatalos ügyintézés, banki és egészségügyi szolgáltatások). Ismeri a közösségi oldalakat és az online együttműködési eszközöket. Tudatában van annak, hogy a digitális eszközök használatakor bizonyos kommunikációs szabályokat be kell tartani (pl. hozzászólás, személyes információ megosztása esetén).	A felhasználó számos kommunikációs eszköz haladó szintű funkcióját tudja használni (pl. azonnali üzenetküldő szolgáltatás, VoIP és fájlmegosztás). Képes csoportmunka eszközöket használni, például olyan megosztott dokumentumokkal/fájlokkal dolgozni, amelyeket más hozott létre. Tud néhány online szolgáltatási funkciót használni (pl. közszolgáltatások, internetbank, online vásárlás). Információt továbbít vagy oszt meg másokkal online (pl. közösségi média eszközökkel vagy online közösségekben). Ismeri és használja az online kommunikáció szabályait ("netikett").	A felhasználó sokféle kommunikációs eszközt használ aktívan (e-mail, chat, SMS, azonnali üzenetváltás, blogok, mikroblogok, közösségi oldalak) online kapcsolattartásra. Képes létrehozni és kezelni csoportmunka eszközöket (pl. elektronikus naptár, projektkezelő rendszerek, online ellenőrző rendszerek, online táblázatkezelők). Online felületek aktív felhasználója, és számos online szolgáltatást használ (pl. közszolgáltatások, internetbank, online vásárlás). Tudja használni különböző kommunikációs eszközök haladó szintű funkcióit (pl. videókonferencia, adatmegosztás, alkalmazásmegosztás).
Digitális tartalom létrehozása	A felhasználó csak segítséggel tud létrehozni egyszerű digitális tartalmat legalább egyféle formátumban, digitális eszközök használatával. Önállóan nem képes a mások által létrehozott tartalmat	A felhasználó létre tud hozni egyszerű digitális tartalmat (pl. szöveg, táblázat, képek, hangfájlok) legalább egyféle formátumban, digitális eszközök használatával. Alapszinten tud mások által	A felhasználó létre tud hozni összetett digitális tartalmat különböző formátumokban (pl. szöveg, táblázatok, képek, hangfájlok). Különböző eszközöket/szerkesztőket tud használni	A felhasználó létre tud hozni vagy módosítani összetett multimédia tartalmat különböző formátumokban, különböző digitális felületetek, eszközök segítségével. Létre tud hozni holnapot programozási

	szerkeszteni. Csak fogalmi szinten van ismere arról, hogy egyes tartalmak szerzői jogvédelem alatt állhatnak. Az általa használt szoftverekhez és alkalmazásokhoz kapcsolódó egyszerű funkciókat és beállításokat csak korlátozottan tudja alkalmazni és módosítani.	létrehozott tartalmat szerkeszteni. Tudja, hogy egyes tartalmak szerzői jogvédelem alatt állhatnak. Az általa használt szoftverekhez és alkalmazásokhoz kapcsolódó egyszerű funkciókat és beállításokat tudja alkalmazni és módosítani (pl. alapértemezett beállítások megváltoztatása)	honlap vagy blog létrehozására sablonok segítségével (pl. WordPress). Képes alapszintű formázást készíteni az általa vagy mások által létrehozott tartalmakhoz. (pl. lábjegyzetek, táblázatok beillesztése). Tudja, hogyan kell hivatkozni és felhasználni a szerzői jogvédelem alatt álló anyagokat. Ismeri egy adott programozási nyelv alapjait.	nyelv használatával. Képes különböző eszközök haladó szintű formázási funkcióit használni (pl. körlevél, különböző formátumú dokumentumok egyesítése, haladó szintű formátumok használata, makrók). Tudja, hogyan kell a licenszeket és szerzői jogokat kezelni. Számos programozási nyelvet tud használni. Tudja, hogyan kell számítógépes eszközökkel adatbázisokat tervezni, létrehozni és módosítani.
Biztonság Biztonságtudatosság	Nem tudja önállóan használni az eszközei védelme érdekében a különböző védelmi megoldásokat. Csak részlegesen van tisztában azzal, hogy nem minden online információ megbízható. Csak fogalmi szinten van tudatában annak, hogy a személyes adataimat ellophatják, de nem ismeri a védelmi módszereket. Hallott már arról, hogy online nem szabad megadni személyes információt. Csak fogalmi szinten tudja azt, hogy a digitális technológia túlzott használata rossz hatással lehet az egészségre. Csak általános intézkedéseket teszek az energiatakarékosságért. Nincs tisztában azzal, hogy a saját személyes viselkedésén, fokozott figyelmén és határozott fellépésén múlhat az áldozattá válás elkerülése.	A felhasználó alapfunkciókat képes használni az eszközei védelme érdekében (pl. antivírus programok, jelszavak használata). Tudja, hogy nem minden online információ megbízható. Tudatában van annak, hogy a személyes adatait (felhasználónév és jelszó) ellophatják. Tudja, hogy online nem szabad megadnia a személyes információit. Tudja, hogy a digitális technológia túlzott használata rossz hatással lehet az egészségére. Alapszintű intézkedéseket tesz az energiatakarékosságért. Részlegesen van tisztában azzal, hogy a saját személyes viselkedésén, fokozott figyelmén és határozott fellépésén múlhat az áldozattá válás elkerülése. Eseti jelleggel részt vesz információbiztonsági képzésen, oktatáson.	A felhasználó biztonsági programokat telepített az eszköz(ök)re, melye(ke)t internethozzáféréshez használ (pl. antivírus program, tűzfal). Rendszeresen futtatja és frissíti ezeket a programokat. Különböző jelszavakat használ a különböző eszközökhöz és a digitális szolgáltatásokhoz való hozzáféréseknél, és rendszeresen módosítja őket. Felismeri azokat a honlapokat, vagy e-maileket, amelyek kockázatosak. Felismeri az adathalász e-maileket. Ki tudja alakítani saját online profilját, és figyelemmel követi a digitális lábnyomát. Érti a digitális technológia használatával kapcsolatos egészségügyi kockázati összefüggéseket (pl. ergonómia, függőség kialakulásának veszélye). Tisztában van a technológia környezetre gyakorolt pozitív és negatív hatásaival. Tetteiben a proaktivitás mutatkozik annak érdekében, hogy a saját személyes viselkedése, a fokozott figyelme és a határozott fellépése alapján megelőzze és elkerülje a digitális támadásokat, károkozásokat.	A felhasználó rendszeresen ellenőrzi a biztonsági beállításokat és az általa használt ezközöket és/vagy alkalmazásokat. Tudja, hogy mit kell tennie, ha a számítógépét megfertőzi egy vírus. Tudja konfigurálni vagy módosítani a digitális eszközei tűzfal- és biztonsági beállításait. Tudja, hogyan kell az e-maileket vagy a fájlokat titkosítani. Képes szűrőket beállítani, hogy a levélszemetet kiválogassák. Ésszerűen használja az információs-kommunikációs technológiát a fizikális és pszichés egészségügyi problémák elkerülése érdekében. Tisztában van a digitális technológiák mindennapi életre, online fogyasztásra és környezetre gyakorolt hatásával. Tetteiben a proaktivitás és kockázatértékelés mutatkozik annak érdekében, hogy a saját személyes viselkedése, a fokozott figyelme és a határozott fellépése alapján megelőzze és elkerülje, mint a maga, mind a környezete vonatkozásában a digitális támadásokat, károkozásokat. Rendelkezik azon ismeretekkel, amelyekkel egy folyamatban lévő digitális támadást, károkozást meg tud akadályozni, vagy csökkenteni tudja annak kármértékét.

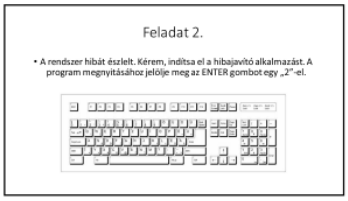
Problémamegoldás	Önállóan nem képes beazonosítani azt, ha egy technikai probléma történik. Önállóan nem kezd el használni egy új eszközt, programot vagy alkalmazást. Csak korlátozott ismeretei vannak azzal kapcsolatban, hogyan kell megoldani néhány egyszerű problémát. Részleges ismeretei vannak arról, hogy a digitális eszközök segítségére lehetnek a problémamegoldásban. Nincs minden esetben tisztában azzal, hogy vannak korlátjai. Amikor technológiai vagy nem technológiai problémába ütközik, a megoldásukra korlátozottan tudja használni az általa ismert eszközöket. Nincs tudatában annak, hogy rendszeresen, újra és újra naprakésszé kell tennie a digitális készségeit.	A felhasználó megtalálja a szükséges segítséget, ha egy technikai probléma történik, vagy egy új eszközt, programot vagy alkalmazást használ. Tudja, hogyan kell megoldani néhány egyszerű problémát (pl. program bezárása, számítógép újraindítása, program újratelepítése vagy frissítése, internetkapcsolat ellenőrzése). Tudja, hogy a digitális eszközök segítségére lehetnek a problémamegoldásban. Azzal is tisztában van, hogy vannak korlátjai. Amikor technológiai vagy nem technológiai problémába ütközik, a megoldásukra tudja használni az általa ismert eszközöket. Tudatában van annak, hogy rendszeresen, újra és újra naprakésszé kell tennie a digitális készségeit.	A felhasználó a legtöbb, digitális technológiák használatakor gyakran előforduló problémát meg tudja oldani. Képes a digitális technológiákat használni, hogy (nem-technikai) problémákat oldjon meg. Ki tud választani egy olyan digitális eszközt, amely megfelel a szükségleteinek, és fel tudja mérni annak a hatékonyságát. A programok vagy eszközök beállításainak és opcióinak áttekintésével képes a technológiai problémákat megoldani. Rendszeresen frissíti a digitális készségeit. Tisztában van a korlátaival, és igyekszik javítani a hiányosságain.	A felhasználó majdnem az összes, digitális technológia használatakor felmerülő problémát meg tudja oldani. Ki tudja választani a megfelelő eszközt, alkalmazást, szoftvert vagy szolgáltatást a (nem technikai) problémák megoldására. Ismeri az új technológiai fejlesztéseket. Érti az új eszközök működését. Rendszeresen fejleszti digitális készségeit.
Tudásátadási képesség	Csak minimális digitális tapasztalattal bír, valamint ismeretei hiányában nem képes azt megfelelően átadni. Mivel alacsony szintű a digitális tudása ezért nincs tisztában azzal, hogy milyen viselkedési példával képes azt átadni.	Alapszintű a digitális tapasztalata, valamint az alapszintű ismeretei alapján képes azt korlátozottan átadni. Az alapszintű digitális tudása alapján inkább az ösztönös védelem jellemzi, alap szinten képes átadni a tudását viselkedési példával.	Közepesszintű a digitális tapasztalata, valamint a közepesszintű ismeretei alapján képes azt hatékonyan átadni. A közepesszintű digitális tudása alapján a tudatos védelem jellemzi, Közepes szinten képes átadni a tudását viselkedési példával.	Magas szintű digitális tapasztalattal bír, és ismeretei alapján képes azt magasfokon átadni. Mivel magas szintű a digitális tudása ezért minden tettére a biztonságtudatos magatartás a jellemző, követendő példakép a környezete számára.

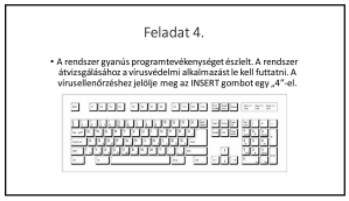
Jelmagyarázat: A sárga mezőbe írt definíciókat és elnevezéseket készítette a szerző.

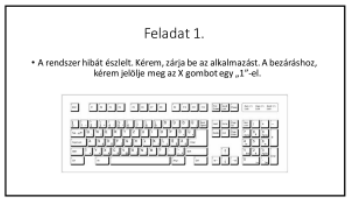
*Az Európai Unió digitális kompetencia keretrendszerének felhasználásával

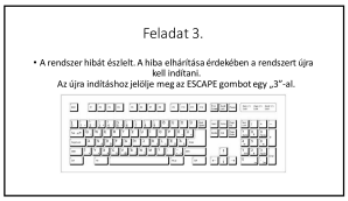
3. számú függelék:

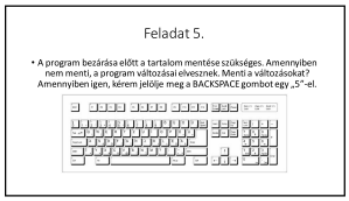
A szoftverergonómiai vizsgálat szöveges feladatlapjai:

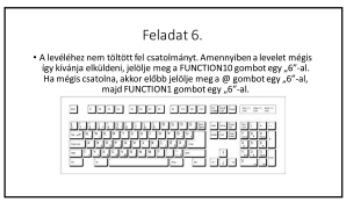


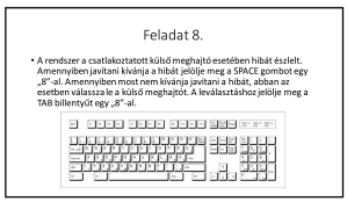


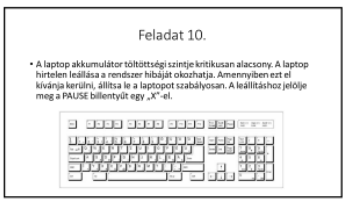


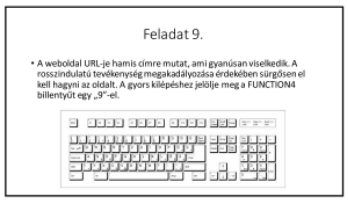




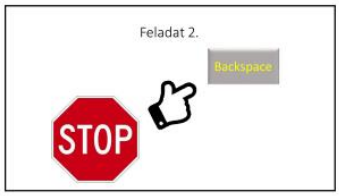


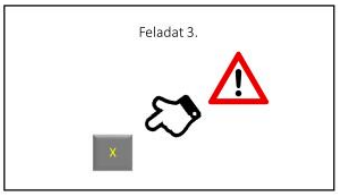


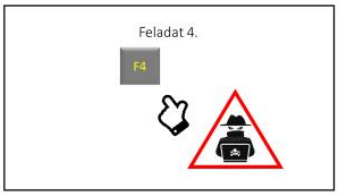


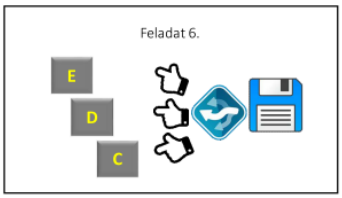


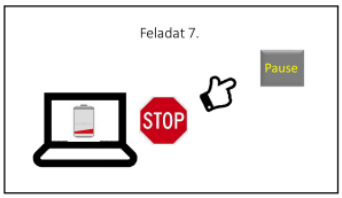
A szoftverergonómiai vizsgálat piktogramos feladatlapjai:

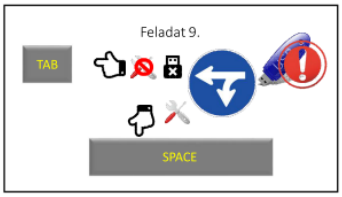












Szoftverergonómia vizsgálati feladatok

válaszok (szöveges)

1.0a

Nyikes Zoltán doktorandusz

nyikes.zoltan@bgk.uni-obuda.hu

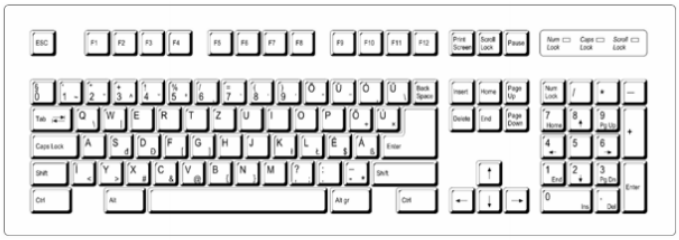
Kedves Válaszadó!

Először is köszönöm, hogy a feladat kitöltésével hozzájárul a doktori kutatásaimhoz. A feladat végrehajtása kb. 2 percet vesz igénybe. Kérem, hogy a prezentációban megjelenő információk alapján cselekedjen és az alábbi billentyűzeten jelölje be az adott feladatban megadott billentyűt.

Fontos! A billentyű megjelölésének módja esetében kérem, hogy tollal és a **feladat sorszámával jelölje.** A prezentációk **5 másodpercenként** váltják egymást. Önnek ennyi ideje van a feladatot értelmezni és végrehajtani. A feladat végrehajtása anonim módon történik.

A feladat végrehajtását köszönöm!

Jó munkát! ☺



Szoftverergonómia vizsgálati feladatok

válaszok (piktogramos)

1.0b

Nyikes Zoltán doktorandusz

nyikes.zoltan@bgk.uni-obuda.hu

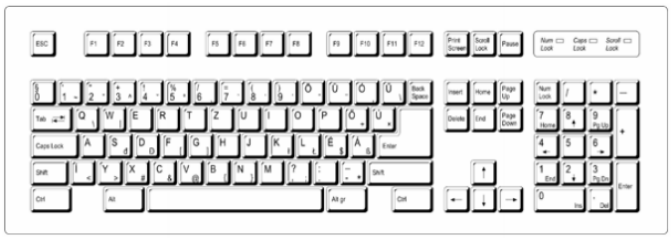
Kedves Válaszadó!

Először is köszönöm, hogy a feladat kitöltésével hozzájárul a doktori kutatásaimhoz. A feladat végrehajtása kb. 2 percet vesz igénybe. Kérem, hogy a prezentációban megjelenő információk alapján cselekedjen és az alábbi billentyűzeten jelölje be az adott feladatban megadott billentyűt.

Fontos! A billentyű megjelölésének módja esetében kérem, hogy tollal és a **feladat sorszámával jelölje.** A prezentációk **5 másodpercenként** váltják egymást. Önnek ennyi ideje van a feladatot értelmezni és végrehajtani. A feladat végrehajtása anonim módon történik.

A feladat végrehajtását köszönöm!

Jó munkát! ☺



KÖSZÖNETNYILVÁNÍTÁS

Köszönetemet szeretném kifejezni mindazoknak, akik az eddigi tanulmányaimat segítették.

Elsősorban szeretném megköszönni családomnak, feleségemnek, gyermekeimnek és édesanyámnak a kitartó támogatásukat, a sok-sok lemondásért és áldozatkészségért.

Szeretném megköszönni témavezetőmnek, Dr. habil Kerti András docens úrnak, hogy segítette és irányította a kutatásaimat. Továbbá szeretném megköszönni egyetemi konzulensemnek, Prof. Dr. Berek Lajos tanár úrnak, hogy az egyetemi tanulmányok alatt már a doktori tanulmányok megkezdésére ösztönzött és a tanulmányaim alatt végig segített túljutni a nehézségeken.

Különösen szeretném megköszönni támogatását és sok-sok segítségét Prof. Dr. Rajnai Zoltán dékán úrnak, valamint azt a rengeteg pozitív élményt, sikert, támogatást és lehetőséget, amit általa kaptam az Óbudai Egyetem Biztonságtudományi Doktori Iskolában. Szeretném megköszönni a segítségét a Biztonságtudományi Doktori Iskola, a Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar és az Óbudai Egyetem minden tanárának és munkatársának, akik a doktori tanulmányaimat valamilyen formában segítették, támogatták.

Szeretném megköszönni a támogatásukat a korábbi és jelenlegi parancsnokaimnak, vezetőimnek, szolgálati- és szakmai elöljáróimnak, valamint kollégáimnak, bajtársaimnak, hogy végig lojálisak és segítőkészek voltak.

Mindenkinek, a felsoroltak közül szeretnék a továbbiakban sok sikert, erőt és egészséget kívánni a további munkájukhoz!

Nyilatkozat a munka önállóságáról, irodalmi források megfelelő módon történt idézéséről

Alulírott **Nyikes Zoltán** kijelentem, hogy **„Az információbiztonság növelése a felhasználó támogatásának lehetőségeivel”** című benyújtott doktori értekezést magam készítettem, és abban csak az irodalmi hivatkozások listáján megadott forrásokat használtam fel. Minden olyan részt, amelyet szó szerint, vagy azonos tartalomban, de átfogalmazva más forrásból átvettem, egyértelműen, a forrás megadásával megjelöltem.

Budapest, 2019. február 25

.....
(aláírás)