



ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉSTERVEZET

MANDIC DOROTTYA

Az okoseszközök biztonságának az elemzése

Témavezető: Dr.habil.Kiss Gábor

**BIZTONSÁGTUDOMÁNYI
DOKTORI ISKOLA**

Budapest, 2025.04.05.

TARTALOMJEGYZÉK

BEVEZETÉS	4
A tudományos probléma megfogalmazása	5
Célkitűzés(ek)	6
A téma kutatásának hipotézisei.....	7
Kutatási módszerek.....	7
1. SZAKIRODALMI ÁTTEKINTÉS.....	9
1.1. Az Internet of Things kialakulása.....	9
1.2. Az Internet of Things felhasználási területei.....	10
1.3. Az okoseszközök használata a hétköznapi életben.....	13
1.4. Az okoseszközök használatának biztonsági kihívásai.....	20
2. INFORMÁCIÓBIZTONSÁG ÉS KIBERBIZTONSÁG.....	24
2.1. Információbiztonság tudatosságának fontossága.....	24
2.2. Jelszóhasználat.....	28
2.3. Európai Unió szabályozásai.....	33
3. INFORMATIKAI OKTATÁSI TANANYAG.....	36
3.1. Informatikai oktatási tananyag Magyarországon.....	36
3.2. Informatikai oktatási tananyag Szerbiában.....	40
3.3. Informatikai oktatási tananyag Szlovákiában.....	42
3.4. Részkövetkeztetések.....	43

4. KVANTITATIV KUTATÁS AZ OKOSESZKÖZ HASZNÁLÓK KÖRÉBEN	
FELMÉRÉS EREDMÉNYEINEK ELEMZÉSE.....	44
4.1. Kutatási adatok.....	44
4.2. A kérdőív.....	44
4.3. A kutatás módszertana.....	45
4.4. Kutatási lépések.....	45
4.5. Kutatási kérdések.....	46
4.6. Mann-Whitney U teszt.....	76
4.7. Részkövetkeztetések.....	84
5. ÖSSZEGZETT KÖVETKEZTETÉSEK.....	86
5.1. Új tudományos eredmények.....	86
5.2. A kutatás jelentősége.....	87
IRODALOMJEGYZÉK.....	88
TÁBLÁZATJEGYZÉK.....	99
ÁBRAJEGYZÉK.....	101
FÜGGELÉK.....	104
1. függelék-A kérdőív magyar nyelven.....	104
2. függelék-A kérdőív szerb nyelven.....	107
KÖSZÖNETNYILVÁNÍTÁS.....	111

BEVEZETÉS

Az okoseszközök használata a mindennapi életünk részévé vált, és már el sem tudjuk képzelni a hétköznapi életünket az okoseszközeink használata nélkül. Az okostelefonunkat is szinte már mindenhol magunkkal visszük, mivel különböző tevékenységeket tudunk elvégezni a használata által. Napjainkban az okoseszközöket már számos területen használják, mivel a használatuk számos előnnyel jár [1]. Az okoseszköz használók a hétköznapi életben általában azért vásárolnak különféle okoseszközöket, mert fontosnak tartják otthonukban például a kényelmet, a szórakozást, esetleg a költségmegtakarítást vagy az időmegtakarítást, vagy csak az otthonukat szeretnék biztonságosabbá és jobbá tenni. Vannak olyan okoseszköz használók, akik az egészségügyi állapotukat szeretnék figyelemmel kísérni. Mivel az okoseszközök használatának számos előnye van, egyre többen döntenek amellett, hogy okoseszközöket vásároljanak az otthonaikban, mint például okostévé, okosporszívó, okoshangszóró, okosmérleg, okoskamera, vagy egyéb okoseszközök [2]. A COVID-19 járvány nagyban hozzájárult ahhoz, hogy az elmúlt évek során megnőtt az érdeklődés a különféle okoseszközök iránt. Mivel az embereknek kényszerből otthonaikban kellett maradniuk, így sokkal több időt kellett az otthonaikban eltölteniük, mint azelőtt. Ezért sokan döntöttek úgy, hogy az okoseszközök segítségével próbálják az eltöltött időt minél elviselhetőbbé és szórakoztatóbbá tenni a járvány ideje alatt. Az IoT-eszközöknek a száma napjainkban rohamosan nő az egész világon. A Statista jelentése szerint jelenleg megközelítőleg „15 milliárd IoT eszköz van jelen, ami várhatóan 2030-ra el fogja érni a 29 milliárd IoT eszközt”. Az IoT-eszközök száma várhatóan évről évre növekedni fog, és „2030-ra várhatóan Kínában lesz a legtöbb IoT eszköz”[3]. Az IoT-eszközöket napjainkban számos területen használják, és egyre több hétköznapi eszköz és tárgy csatlakozik már az internetre [4]. A felhasználók közül vannak olyan okoseszköz használók, akik nem rendelkeznek megfelelő ismerettel arról, hogy az okoseszközök használata biztonsági kihívásokat rejthet, valamint nincs megfelelő tudásuk arról sem, hogy hogyan tudnák okoseszközeiket biztonságosan használni. A felhasználók közül vannak olyan okoseszközhasználók akik például nem tesznek semmilyen intézkedést annak érdekében, hogy az okoseszközeiket biztonságosan használják, mivel úgy gondolják, hogy nem az ő feladatuk [5]. Egyre fontosabbá vált a biztonság a mindennapi életünkben és elmondhatjuk, hogy napjainkban a kiberbűnözés jelenti az egyik legnagyobb kihívást [6]. „Az IoT-eszközök biztonságának a védelme az egyik

legnagyobb kihívást jelenti, mivel az IoT-eszközök olyan információkat gyűjtenek, melyek lehetnek például személyes, vállalati, vagy ipari információk” [7]. Mivel napjainkban egyre gyakrabban fordulnak elő a kibertámadások, és várhatóan a jövőben még nagyobb számban fognak jelen lenni az IoT-eszközök, ezért a jövőben várhatóan még több támadás fog történni az IoT-eszközök ellen [8]. Az „Internet of Things rövidítése (IoT) jelentése magyarul „dolgok internete”. Az „Internet of Things”, vagy csak rövidítve IoT alatt értünk „minden olyan dolgot és használati tárgyat, amely egy hálózaton keresztül más gépekhez csatlakozva működik” [10]. Az eszközök egymás közötti kommunikációját „Machine to Machine” (M2M) magyarul „gép-gép” kommunikációnak hívjuk [11].

A tudományos probléma meghatározása

Az okoseszközök iránti kereslet hatalmas mértékben megnőtt az elmúlt évek során, mivel a használatuk számos előnyt nyújt a mindennapi életben. Elmondhatjuk, hogy az okoseszközök használata jobbá, kényelmesebbé, biztonságosabbá és szórakoztatóbbá teheti a hétköznapi életünket, ezenkívül az egészségi állapotunkat is figyelemmel tudjuk kísérni. Emellett még számtalan új lehetőséget hordoznak magukkal az okoseszközök, ezért a gyártók próbálnak mindig újabb és újabb okoseszközöket létrehozni, hogy felkeltsék a felhasználók érdeklődését. A technológia fejlődésének köszönhetően elmondhatjuk, hogy a felhasználók igényei hatalmas változáson mentek keresztül az évek során, és ennek következtében előfordulhat, hogy a gyártóknak az elsődleges céljuk nem a biztonságosabb eszközök létrehozása. Inkább az elsődleges cél a minél nagyobb profit szerzése, és ezáltal a minél olcsóbb és gyorsabb megjelenítés kerül előtérbe. Emellett a felhasználók, akik okoseszközöket használnak a mindennapi életben sokan közülük úgy használják az okoseszközeiket, hogy még csak az alapvető ismeretekkel sem rendelkeznek arról, hogyan tudnák az okoseszközeiket biztonságosan használni. Vannak olyan okoseszköz használók, akik nem is tesznek semmilyen intézkedést annak érdekében, hogy biztonságosan használják okoseszközeiket, vagy úgy gondolják, hogy ez nem az ő feladatuk lenne. A tanulmányaim és az eddigi kutatásom során, valamint a környezetemben tapasztaltak alapján elmondhatom, hogy az okoseszköz használók nem rendelkeznek megfelelő tudással ahhoz, hogy az okoseszközeiket biztonságosan tudják használni. A dolgozatom egyik része maguk az eszközök biztonságával foglalkozik, míg a másik része a felhasználók információbiztonságának tudatlanságát vizsgálja. Sokszor megtörténik, hogy az okoseszköz használók könnyen kitalálható jelszavakat használnak,

hogy könnyen megjegyezzék, és hogy ne felejtsék el. Mivel a hosszabb jelszavakat nehezebb lenne nekik megjegyezni, ezért sokszor megtörténik, hogy a felhasználók könnyen kitalálható jelszavakat használnak, amelyek például személyes információt tartalmaznak, vagy értelmes szót. Mivel egyre több helyen kell már különböző jelszavakat használni a felhasználók sokszor használják ugyanazt a jelszót akár több helyen is. Az IoT-eszközök esetében a gyenge jelszavak súlyos következményekkel járhatnak, hiszen a támadók ezt kihasználhatják. Vannak olyan felhasználók, akik rövid jelszót használnak, míg mások inkább a hosszabb jelszót részesítik előnyben, de a többség a rövid jelszó mellett dönt, mert ezt könnyebb megjegyezni. Lényegében a rövid, valamint a hosszabb jelszó használatának is van előnye és hátránya. Az okoseszközök esetében elmondható, hogy inkább hátránya van a rövid jelszó használatának, valamint a könnyen kitalálható jelszavaknak.

Célkitűzések

Célként fogalmazom meg, hogy olyan értekezést készítek, ami segítségül szolgál az okoseszközök biztonsági kihívásainak megismerésében.

Célként tűztem ki, hogy feltérképezem a hétköznapi életben mennyire elterjedt az okoseszközök használata a felhasználók körében.

Célként fogalmazom meg, hogy feltérképezem a felhasználók rendelkeznek-e az alapvető ismeretekkel, hogy az okoseszközeiket biztonságosan tudják használni.

Célként tűztem ki, hogy összehasonlítom Magyarország, Szerbia és Szlovákia informatikai oktatási tananyagát, hogy van-e eltérés az országok informatikai oktatási tananyaga között.

Célként tűztem ki, hogy feltérképezem az okoseszköz használók jelszóhasználatának szokásait.

A téma kutatásának a hipotézisei

Hipotézis 1

Feltételezem, hogy a hétköznapi életben megnőtt az okoseszközök használatára az igény, és ezáltal megnőtt a kockázat, hogy az okoseszközöket egyre több támadás érje.

Hipotézis 2

Feltételezem, hogy az IoT-eszközök biztonságos használatához a felhasználók nem rendelkeznek még csak az alapvető ismeretekkel sem, hogy biztonságosan tudják használni az IoT-eszközöket.

Hipotézis 3

Feltételezem, hogy a Magyarországon élők információbiztonságának tudatossága magasabb, mint a Szerbiában élőknek a jelszóhasználat esetében, amikor olyan jelszót használnak, ami értelmes szót tartalmaz.

Hipotézis 4

Feltételezem, hogy a Magyarországon élők információbiztonságának tudatossága magasabb, mint a Szlovákiában élőknek a jelszóhasználat esetében, amikor olyan jelszót használnak, ami értelmes szót tartalmaz.

Hipotézis 5

Feltételezem, hogy Magyarországon, Szerbiában és Szlovákiában különbség van az információbiztonság tudatossága terén, mivel az informatikai oktatási tananyagban eltérés található az országok között.

Kutatási módszerek

A kutatási módszereknél a kutatásom módszertani alapját az irodalomkutatás, valamint az adatelemzés és az értékelésből származó eredmények alkotják. Az irodalomkutatást magyar, angol és szerb nyelven végeztem. A kutatásom célja bebizonyítani, hogy a hétköznapi életben megnőtt az okoseszközök iránti kereslet, és emiatt egyre többen használnak a hétköznapi életben különböző okoseszközöket. Ezáltal megnőtt a kockázat, hogy az okoseszközöket még több támadás érje. Ezenkívül az okoseszköz használók nem rendelkeznek megfelelő ismeretekkel ahhoz, hogy az okoseszközöket biztonságosan tudják használni, és egyre több támadás éri az okoseszközöket. Ezenkívül szeretném

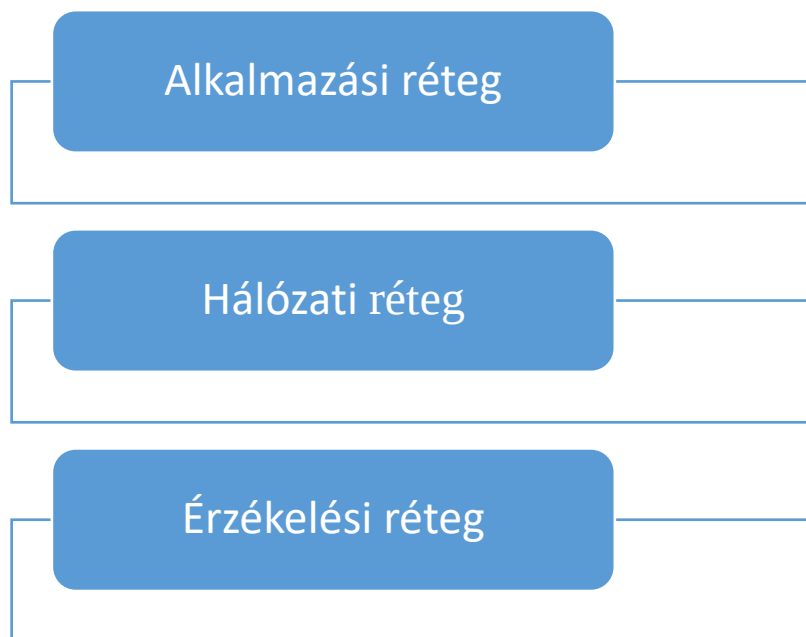
bemutatni az okoseszköz használók jelszóhasználati szokásait, valamint Magyarország, Szerbia és Szlovákia informatikai oktatási tananyagát, hogy van-e különbség az országok informatikai oktatási tananyaga között.

A kutatás lezárásra került 2024.02.03-án.

1. SZAKIRODALMI ÁTTEKINTÉS

1.1. Az Internet of Things kialakulása

Egyre nagyobb a kereslet a különféle okoseszközök iránt napjainkban, és egyre több felhasználó dönt amellett, hogy okoseszközt vásárol otthonában, vagy az egészségi állapotát szeretné figyelemmel kísérni. Az okoseszközöket már számos területen használják, mivel számtalan előnye van a használatuknak [1]. „Az első dolgok internete eszköz az 1980-as évek elején jött létre a Carnegie Mellon Egyetemen, ami egy Coca-Cola automata volt” [9]. A bevezetőben már olvashattuk, hogy az „Internet of Things rövidítése (IoT) jelentése magyarul „dolgok internete”. Az „Internet of Things” alatt értünk „minden olyan dolgot és használati tárgyat, amely egy hálózaton keresztül más gépekhez csatlakozva működik”[10]. Valamint az eszközök egymás közötti kommunikációját „Machine to Machine” rövidítve (M2M) magyarul „gép-gép” kommunikációnak nevezünk [11]. A dolgok internete megnevezést először „Kevin Ashton” használta a kilencvenes évek végén egy vállalati prezentáció során [12], [13], [14]. Kevin Ashton 1968-ban született angol kutató és filozófus. A nevéhez a Radio-frequency identification (RFID), vagy magyarul a rádiófrekvenciás azonosítás technológia által ismert, melyet a Massachusetts Institute of Technology (MIT) egyetemen fejlesztett ki. „A széles körben elfogadott definíció szerint az Internet of Things olyan fizikai tárgyak, eszközök, gépek, berendezések és más dolgok által alkotott hálózatok, amelyek rendelkeznek beágyazott elektronikával, szoftverekkel, szenzorokkal, kommunikációs egységekkel, és az interneten keresztül képesek egymással kommunikálni”[15]. A Cisco Internet Business Solution Group (IBSG) meghatározása szerint „a Dolgok internete nem más, mint amikor egy időben több eszköz csatlakozik az internetre, mint ahány ember”[16]. „A dolgok internete ma azoknak az eszközöknek a gyűjtőfogalma, amelyek hálózatba kapcsolódnak, azaz olyan csatlakoztatott eszközök, amelyek lehetnek fizikai eszközök, épületek szenzorjai, ipari vezérlőelemek, járművek elektronikai berendezései, vagy akár a lakásunkban található elektronikai eszközök is” [7]. Az IoT architektúrája általában 3 rétegből áll, de megtalálható olyan irodalom is, mely ennél több réteget is bemutat [17]. Az 1. ábrán láthatjuk az IoT architektúra 3 rétegét, ami a következő rétegekből áll: alkalmazási réteg, hálózati réteg és érzékelési réteg.



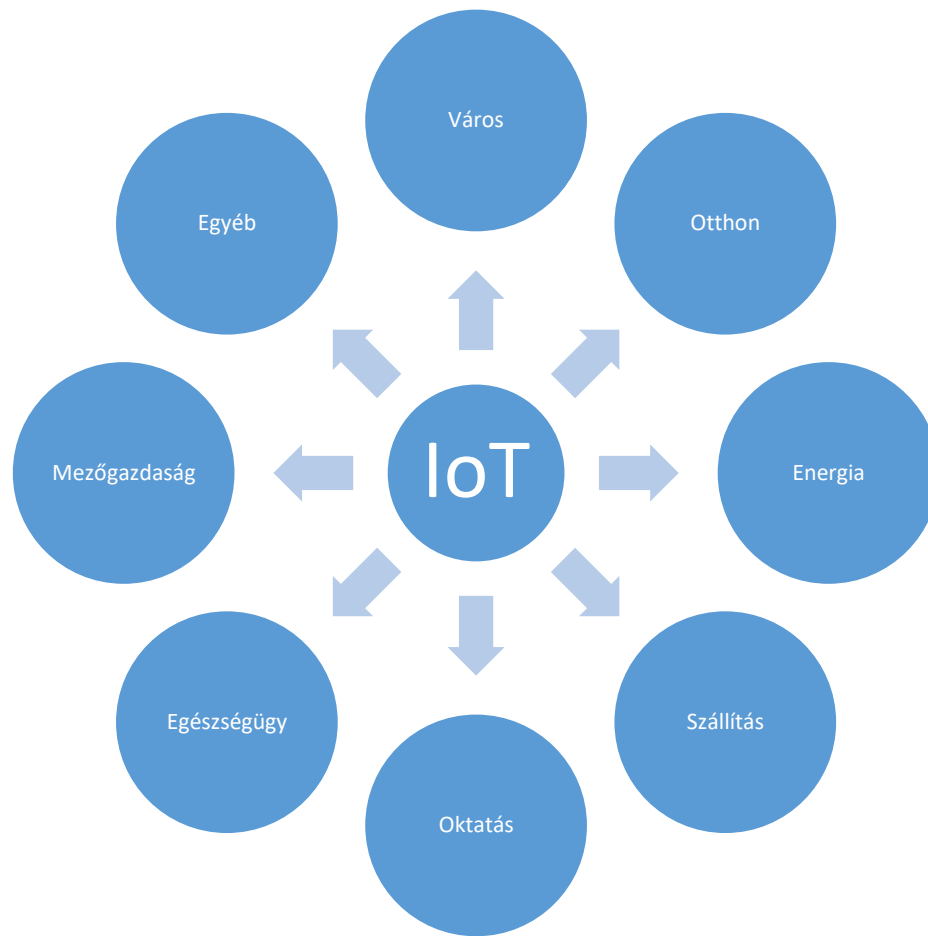
1. ábra. IoT architektúra. [21]

„Az internetet világszerte 5 milliárd ember használja, ami a világ teljes népességének a (63%)-át jelenti” [18]. A Statista 2024-es jelentése szerint 5,45 milliárd internethasználó van világszerte, ami a világ népességének (67,1%)-a [19]. Az IoT-eszközök pontos számát nehéz felbecsülni, mivel több különböző adattal is találkozhatunk arról, hogy jelenleg körülbelül mennyi IoT eszköz van jelen a világon. A Cisco jelentése szerint 2020-ra 50 milliárd eszköz fog csatlakozni az internetre [8]. Az IoT-eszközök száma az IoT Analytics elemzése szerint el fogja érni a 30,9 milliárd eszközt 2015-től 2025-ig [3]. Az okoseszközöknek rengeteg előnye van a mindennapi életünkben, és számtalan új lehetőséget kínálnak, ezért a gyártók kihasználva ezeket a lehetőségeket olyan okoseszközöket próbálnak létrehozni, amelyek minél több újdonsággal rendelkeznek, hogy felkeltsék a felhasználók figyelmét. A Capgemini Kutatóintézet felmérése szerint, amely 2023-ban készült, egyre nagyobb a kereslet a lakosság körében a különféle okoseszközök iránt [20].

1.2. Az Internet of Things felhasználási területei

„Az IoT-eszközök alkalmazását feloszthatjuk fogyasztói, kereskedelmi, ipari és infrastrukturális területekre”[21]. Ezek a területek lehetnek például az „okosvárosok, okosépületek, okosházak, okosjárművek, mezőgazdaság, egészségügy, viselhető eszközök, és egyéb területek” [20], [21]. A 2. ábrán láthatunk néhány területet, ahol alkalmazzák, mint például városok, otthonok, energia, szállítás, oktatás, egészségügy,

mezőgazdaság és egyéb területek. Láthatjuk, hogy napjainkban már számos területen használják az IoT előnyeit.



2. ábra. Az IoT alkalmazási területei. [22]

Mivel számos területen alkalmazzák az IoT előnyeit, ezért csak néhány területet említenék meg, például a városok, mezőgazdaság, egészségügy és okosotthonok.

Okosváros: Az okosvárosról elmondhatjuk, hogy az IoT fontos szerepet tölt be a városok okosságát illetően. „Az okosváros célja az ember környezetének minél élhetőbbé tétele, és ezt minél kevesebb ráfordítással minél nagyobb előnyhöz jussanak.” Ezenkívül az okosváros fő célja az ott lakók életminőségének a javítása. „Az okosváros egy olyan város, amely javítja a településen élők életminőségét, a városi közművek és szolgáltatások hatékonyságát. Biztosítja a település versenyképességét a jelen és jövő generációk szükségleteit gazdasági, társadalmi és környezeti szempontból” [23].

Okosmezőgazdaság: Az okosmezőgazdaság „célja, hogy egyesítse az elérhető technológiákat, és a különböző forrásokból nyert adatok felhasználásával segítsen optimalizálni a folyamatokat a művelésben.” Például drónos felvételek az intelligens

traktorok adatait felhasználva segítenek megkeresni azokat a területeket, ahol például csökkenteni lehet a műtrágya mennyiségét, hogy mikor és milyen növényvédő szert szükséges alkalmazni [24].

Okosegészségügy: Az egészségügyben egyre fontosabb szerepet kapnak a különféle okoseszközök. Hiszen olyan lehetőségeket nyújtanak, mint például a betegségmegelőzés, betegkövetése, vagy a betegellátás. Az okoseszközök használata az egészségügyben számos előnnyel jár. Az egészségügyi személyzet az okos orvosi eszközök által figyelemmel tudja kísérni például a krónikus betegségben szenvedő betegek állapotát, mint például a cukorbetegség vagy szívbetegség állapotát. Ezenkívül észlelni tudják, amennyiben változás következett be, és amennyiben szükséges módosítani tudnak a kezelésein. A beteg adatainak folyamatos gyűjtésével lehetőség van arra, hogy az alapján az orvosok megfontolt döntéseket tudjanak hozni a beteg diagnózisáról, valamint a további kezelésekről. Ezenkívül a mentőkocsiban a betegek kórházba szállításakor a vezeték nélküli betegfelügyeleti megoldások lehetővé teszik azt, hogy a kórházi orvosok valós időben nyomon tudják követni a beteg állapotát, és hogy meg tudják tervezni a beteg ellátását [25].

Okosotthonok: Az okosotthonok egyre népszerűbbek napjainkban, és egyre többen vásárolnak különféle okoseszközöket. Az utóbbi évek során megnőtt az érdeklődés az okosotthonokban használt okoseszközök iránt, amihez a COVID-19 járvány nagyban hozzájárult. Az okosotthon alatt olyan épületet értünk, amely magában foglalja azokat a technológiai megoldásokat, melyek által automatizálni lehet az otthonokat [23]. A felhasználók általában „a kényelem, a szórakozás és a költségmegtakarítás miatt vásárolják meg az okoseszközöket otthonaikban,” ezenkívül a biztonság növelése érdekében is, valamint az időmegtakarítás céljából.” [5]. Az okoseszközök számos előnyt nyújtanak az otthonokban, mint például az energia és költségmegtakarítás, kényelem, jobb életminőség, vagy a biztonság növelése [24]. A 3.ábrán láthatunk néhány IoT eszközt az okosotthonban, amelyek egyre népszerűbbek a felhasználók körében napjainkban, mint például az okostévé, okos zár, okosvilágítás, hangasszisztens. Az otthonokban használt IoT-eszközöknek számos előnye van.



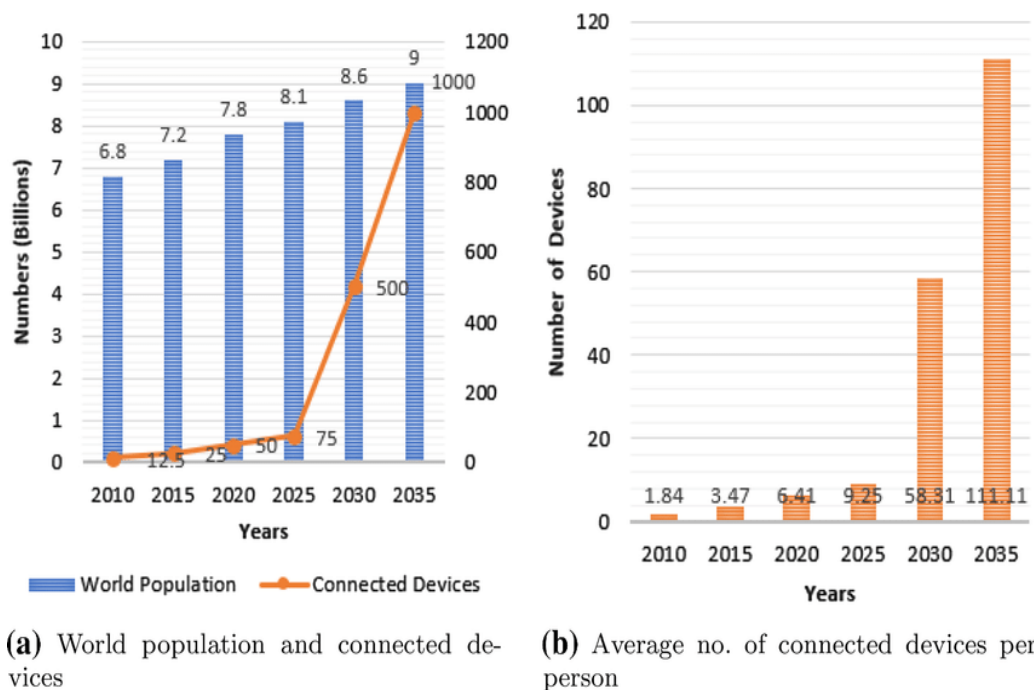
3. ábra. Az IoT használata az okosotthonban.[26]

Az okoseszközök az otthonok különböző funkcióit vezérelhetik, automatizálhatják, valamint optimalizálhatják [26]. Mivel számos előnyt nyújtanak a felhasználóknak, egyre többen vásárolnak különféle okoseszközöket. Az okoseszközök használatának számos előnye van, de nem szabad megfeledkezni arról sem, hogy biztonsági kihívásokat is hordoznak [27].

1.3. Az okoseszközök használata a hétköznapi életben

„Az IoT-eszközök száma rohamosan nő világszerte, és jelenleg megközelítőleg 15 milliárd IoT eszköz van jelen, ami várhatóan 2030-ra el fogja érni a 29 milliárd eszközt.” [28]. A koronavírus ideje alatt megnőtt az okoseszközök iránti kereslet, hiszen az embereknek az otthonaikban kellett több időt eltölteniük, mint azelőtt. Sokan közülük otthonról dolgoztak, valamint különféle online szolgáltatásokat kellett igénybe venniük. Ezenkívül sokan vásároltak különféle okoseszközöket az otthonaikba szórakoztatás céljából, hiszen a járvány ideje alatt az embereknek otthon kellett maradniuk, így próbálták elviselhetőbbé tenni az eltöltött időt.

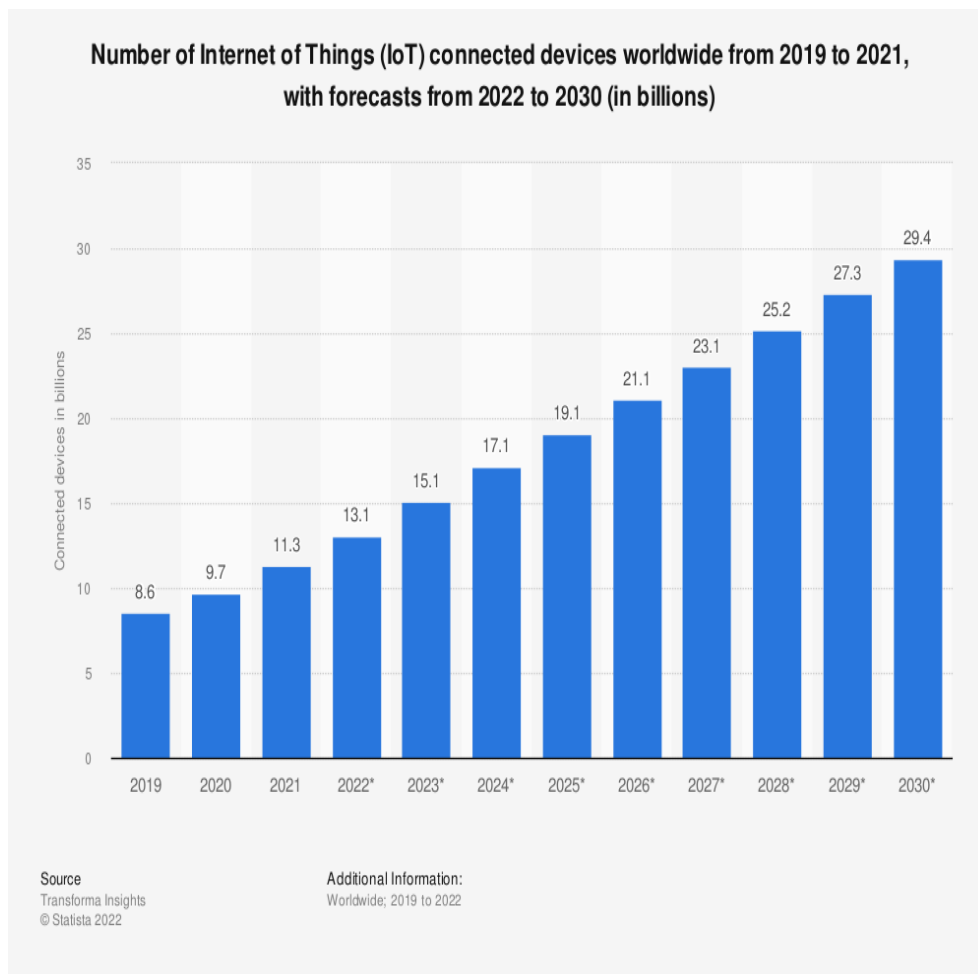
A Statista jelentése szerint 2030-ra az IoT-eszközök száma várhatóan Kínában 8,6 milliárd IoT eszköz lesz jelen, majd Kínát Európa és Észak Amerika fogja követni az IoT-eszközök számában [25]. A 4. ábra a) részénél láthatjuk a világ népességét és a csatlakoztatott eszközöket. Megfigyelhető, hogy 2010-től 2025-ig a csatlakoztatott eszközök száma folyamatosan nő, és várhatóan 2035-re a csatlakoztatott eszközök száma rohamosan meg fog nőni. A 4. ábra b) részénél látható a csatlakoztatott eszközök átlaga személyenként 2010-től 2035-ig. Megállapítható, hogy 2010-től a csatlakoztatott eszközök átlaga évenként folyamatosan nő 2025-ig, majd 2035-ben jelentős növekedés várható.



4. ábra. A világ népessége és a csatlakoztatott eszközök.[29]

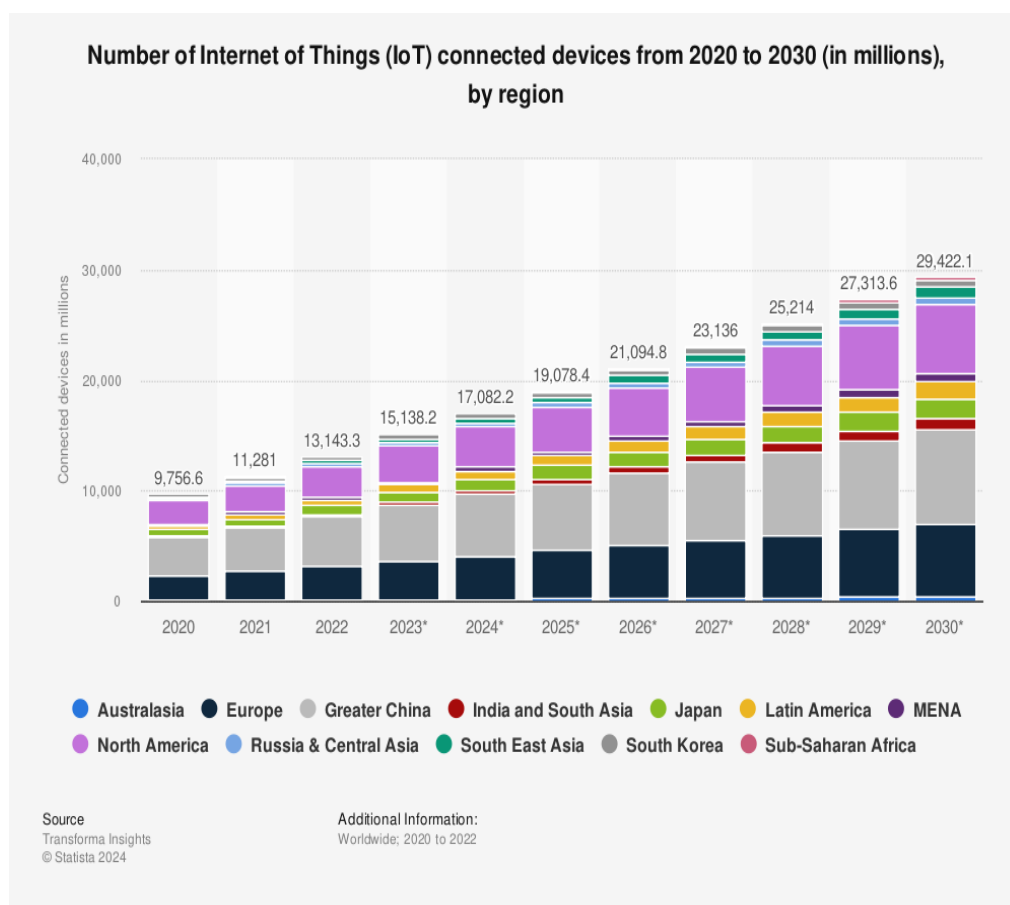
A 4. ábra a) része mutatja, hogy a csatlakoztatott eszközök száma folyamatosan nő, és várhatóan 2035-re még több csatlakoztatott eszköz fog jelen lenni. Ezáltal várhatóan a csatlakoztatott eszközök átlaga személyenként jelentős növekedést fog kísérni, amit láthatunk a b) résznél. Az 5. ábrán megtekinthető a Statista jelentése szerint az IoT-eszközök száma 2019-től 2030-ig. Megfigyelhetjük, hogy az IoT-eszközök száma folyamatosan nő, és várhatóan az IoT-eszközök száma 2030-ban drasztikusan meg fog nőni. Ez azért fontos mert láthatjuk, hogy az IoT-eszközök száma rohamosan nő napjainkban, ezáltal nő a kockázat, hogy egyre több támadás fogja érni ezeket az eszközöket. A dolgozatomban feltételezem, hogy a hétköznapi életben megnőtt az

okoseszközök használatára az igény, és ez alapján láthatjuk, hogy az IoT-eszközök száma egyre csak nő, ezáltal megnőtt a kockázat, hogy az IoT-eszközöket egyre több támadás érje.



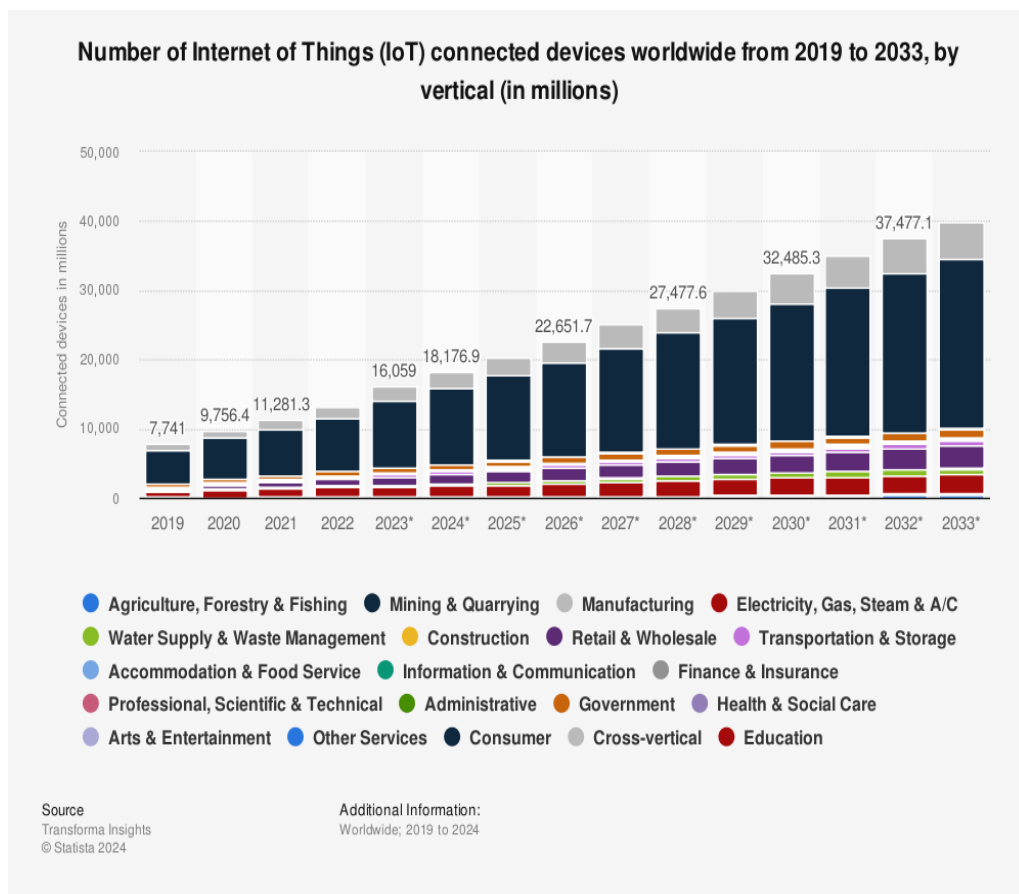
5. ábra. Az IoT-eszközök száma 2019-től 2030-ig. [28]

Az 5. ábra mutatja a Statista jelentése szerint országoként az IoT-eszközök számát 2020-tól 2030-ig. Megfigyelhetjük, hogy az IoT-eszközök száma országoként is jelentősen növekszik. Ez azért fontos, mert a dolgozatomban feltételezem, hogy a hétköznapi életben megnőtt az okoseszközök használatára az igény. Láthatjuk, hogy Európában, Kínában és Észak Amerikában igen jelentősen megnőtt az IoT-eszközök száma, és várhatóan a jövőben még több IoT eszköz fog jelen lenni. Ezáltal megnő a kockázat az IoT-eszközök elleni támadások esetében, mivel egyre több eszköz fog várhatóan csatlakozni az internetre. A 6. ábra mutatja az IoT-eszközök számát világszerte 2019 és 2033 között területenként.



6. ábra. Az IoT-eszközök száma 2020-tól 2030-ig országonként.[30]

A 7. ábrán megtekinthető területenként, hogy az IoT mennyire népszerű, és annak a növekedését 2020-tól 2030-ig. A Statista jelentése mutatja, hogy a legtöbb IoT eszköz például Kínában, Európában és Észak Amerikában található. A 7. ábrán megfigyelhető, hogy 2030-ban, mely fogyasztói területek vezetnek, és hogy a fogyasztói eszközök száma 2019-től folyamatosan nő 2033-ig. Ez alapján láthatjuk, hogy a felhasználók körében a különféle okoseszközök mennyire népszerűek.



7. ábra. Az IoT-eszközök számát világszerte 2019 és 2033 között területenként.[31]

Láthatjuk, hogy 2030-ban a fogyasztói terület fog dominálni az IoT-eszközök számát illetően, több mint 24 milliárd IoT eszközzel világszerte a Statista jelentése alapján. Az előrejelzések szerint a fogyasztói terület tovább fog növekedni a jövőben [31]. A felhasználók körében az okoseszközök használata egyre népszerűbb, és egyre többen használnak különféle okoseszközöket napjainkban. A „Huawei Technologies Hungary által végzett felmérés szerint a magyar felhasználók körében az okoseszközök használata igen népszerű, és már egyre többen használják az okoseszközeiket akár a sportoláshoz, vagy az egészségügyi funkciók méréséhez is” [32]. „Az emberek 60%-a az eszközök által mért értékek alapján orvoshoz fordulna” [33]. Az „eNet 2018-ban végzett kutatása szerint például minden tizedik felnőtt internetező Magyarországon használ már okosórát, vagy okoskarkötőt” [34]. „Az INNObyte 2021-ben végzett kutatása szerint a felhasználók egyre többen használnak okoseszközöket az otthonaikban” [35]. 2021-ben az eNet felmérése szerint Magyarországon 6,2 millióan használnak okostelefont [36]. Az okosóra egyre népszerűbb a felhasználók körében, mivel lehetőség van például a mozgást és a pulzust, valamint az alvás változásait figyelemmel kísérni [37]. A Huawei Technologies Hungary 2021-ben készített felmérést, melyben közel 8000 válaszadó vett részt. A

felmérésben azt vizsgálták, hogy mennyire népszerűek a különféle okoseszközök a magyarok körében, és hogy vásárláskor melyek a legfontosabb szempontok, amiket figyelembe vesznek a vásárlók, hogy milyen funkcióra használják az okoseszközöket. A felmérés alapján a válaszadók „63%-a használ okosórát, illetve okoskarkötőt, 54%-a rendelkezik vezeték nélküli fülhallgatóval, 12%-a rendelkezik okosmérleggel vagy vérnyomásmérővel, és 15%-a válaszolta, hogy nem használ semmilyen okoseszközt.” A válaszok alapján, ami a vásárlást illeti a felhasználóknak a legfontosabb szempontok közé tartoznak a hosszú üzemidő, ár, valamint a kényelem [32].

A 8. ábrán láthatunk különböző okoseszközöket, melyek népszerűek a felhasználók körében az otthonokban, mint például az okosmérleg, okoshűtő, hangasszisztens.



8. ábra. Okoseszközök. [38]

2021-ben a Samsung is végzett online kutatást az Impetus Research által, és a felmérésben 815 válaszadó vett részt. A válaszadók 18 és 64 év közöttiek voltak. A felmérés alapján a válaszadók 27%-a vásárolt például okostelefont, 6,5%-a játékkonzolt, és 10%-a okosórát vagy vezeték nélküli fülhallgatót. Valamint a válaszadók 17%-a új televíziót szeretne vásárolni [39].

Az INNObyte 2021-es felmérése szerint a válaszadók 83%-a rendelkezik otthonukban okoseszközzel. A válaszadók 32%-a azt válaszolta, hogy azért vásárolt okoseszközt, mert fontos számára a kényelem, 17%-a szórakozás miatt vásárolt okoseszközt, és 14%-a az energiamegtakarítás miatt. A válaszadók 93%-a szerint előnyös, ha otthonában vannak okoseszközök, 82%-a szerint kényelmes a használatuk, valamint megkönnyítik a mindennapi életet az okoseszközök használata, 49%-a pedig azt válaszolta, hogy időmegtakarítást ért el az okoseszközök használata által. Azok a válaszadók, akik azt választották, hogy nem rendelkeznek okoseszközökkel anyagi, valamint biztonsági okokkal indokolták. Egyes felhasználók például azt választották, hogy veszélyt látnak abban, hogy otthonaikban okoseszközöket használjanak [35]. 2022-ben a Deloitte felmérést végzett a digitális fogyasztói trendekről, melyben 36 ezer felhasználó vett részt világszerte, és 1000 válaszadó vett részt Magyarországon. A felmérés alapján a 18 évestől az 54 éves korig mutatott legnagyobb érdeklődést a felmérésben résztvevők az okostelefonok iránt [40]. A Nemzeti Média és Hírközlési Hatóság megbízásából 2022-ben készült felmérésben 3206 háztartás és személy vett részt. A felmérés eredménye szerint a háztartások 88%-a rendelkezik valamilyen internetezésre alkalmas eszközzel. A legnagyobb növekedést a felmérés alapján a háztartásokban az okostévék iránt tapasztalható. A felmérésben résztvevők 83%-a rendelkezik a felmérés szerint okostelefonnal [41]. A Reviews.org felmérése, amely 2022-ben készült a 18 éves, illetve ennél idősebb amerikaiak válaszai alapján a legnépszerűbb okoseszközök a személyes használatra az okostelefon, okosóra és a tablet. Az otthonukban használt okoseszközök közül pedig a legnépszerűbbek például a hangszórók, tévék, hűtők, okoscsengők és biztonsági kamerák [42]. A Digital Trends 2023-ban a legjobb otthoni okoseszközök közé sorolta a következő okoseszközöket ezekből néhányat megemlítenék például a hangasszisztenst, biztonsági kamerát, termosztátot és robotporszívót [43]. A Xiaomi tanulmánya szerint a fogyasztók körülbelül 70%-a a COVID-19 járvány ideje alatt több időt töltött otthonában, és ennek következtében okoseszközökkel próbálták az otthonukat jobbra tenni [9]. A fogyasztók 80%-a szerint előnyös, ha az otthonuk okoseszközökkel van felszerelve [44]. A Safewise adatai alapján 2020-ban az amerikaiak 85%-a vásárolt okosotthoni eszközt, és a vásárlók 75%-a 44 éves vagy fiatalabb volt. A legnépszerűbb okosotthoni eszközök az okostévé, okoshangszóró és okosvilágítás voltak. „A felmérésből ezenkívül kiderül az is, hogy az amerikaiak 55%-a vásárolt új okostévé a COVID-19 járvány ideje alatt, és a megkérdezettek 46%-a állította, hogy több pénzt költött az otthoni technikára 2020-ban, míg csak 22%-a állította, hogy kevesebb pénzt

költött.” [45]. 2021-ben a Samsung Electronics felmérést végzett az Impetus Research által Magyarországon. A felmérés szerint Magyarországon a járvány ideje alatt a felmérésben résztvevők válaszaik alapján legtöbbször okostelefont vásároltak, valamint okostévé és számítógépet. Ezenkívül a felmérésből kiderült az is, hogy a válaszadók többsége a kívánt eszközöket már a járvány előtt is szeretne volna megvásárolni, de volt olyan válaszadó, aki csak a járvány miatt vásárolt új eszközt. A válaszadók válaszaik alapján a járvány ideje alatt az okoseszközöket legtöbbször munkára, tanulásra, kapcsolattartásra vagy szórakoztatásra használták [39]. A Capgemini Kutatóintézet felmérése szerint a felhasználók 67%-a szükségesnek tartja az okoseszközök használatát. A felmérés szerint az egyik ok, amiért az okoseszközöket használják a mindennapi életben, hogy nagyobb biztonságban érzik magukat és egészségüket. A felmérés szerint, ami 2023 novemberében készült 10.000 felhasználó vett részt 13 országból, mint például Kanada, Franciaország, Németország, Olaszország, India, Japán, Spanyolország, Norvégia és az Egyesült Államok. A felmérés szerint 80%-a használja szórakozásra az okoseszközöket, 60%-a használ hangalapú asszisztenst, 33%-a használja az okoseszközöket az egészsége nyomon követése érdekében, míg 23%-a az otthoni biztonsága érdekében [32].

Az okoseszközök általános tulajdonságai:

- mindennapi életünk részévé váltak
- új lehetőségeket kínálnak
- fejlődésük rohamosan nő
- számtalan előnyük van
- pénzt, időt és energiát tudunk megtakarítani használatukkal

1.4. Az okoseszközök használatának biztonsági kihívásai

Napjainkban egyre több hétköznapi eszköz és tárgy csatlakozik az internethez [4]. Az IoT-eszközöknek a száma világszerte egyre csak nő, és egyre többen használnak napjainkban okoseszközöket. Az okoseszközök fontos szerepet kaptak a mindennapi életünkben, és a legelterjedtebb okoseszköznek az okostelefont tekintik. A becslések szerint az okostelefon használók száma 2022-ben világszerte elérte a 3,9 milliárdot [46]. Az okoseszközök használata igen hasznos a mindennapi életben, és sokszor a felhasználók azért vásárolnak okoseszközöket, mert fontos számukra például a kényelem,

a szórakozás, esetleg az otthonukat szeretnék jobbá és biztonságosabbá tenni, vagy az egészségügyi állapotukat szeretnék figyelemmel kísérni. Egyre többen használnak az otthonaikban különféle okoseszközöket, mint például az okostévét, okoshangszórót, okoskamerát [47]. Az IoT-eszközökkel kapcsolatban az egyik fő aggodalmat az internetre csatlakoztatott eszközöknek a száma jelenti, valamint a sebezhetőség, amit a bűnözők kihasználhatnak. Az IoT-eszközök hatalmas mennyiségű adatot generálnak, és ezáltal fennáll annak a veszélye, hogy illetéktelen személyek hozzáférhetnek ezekhez az adatokhoz [48]. A „hatalmas mennyiségű adat az IoT-eszközök száma milliárdos nagyságrendű, és ezek az eszközök az alaprendeltetésüknek megfelelően folyamatosan gyűjtik az információkat a környezetükből, így hatalmas mennyiségű adatot generálnak” [49]. Az okoseszköz használók közül, vannak olyan felhasználók, akik még csak az alapvető ismeretekkel sem rendelkeznek arról, hogy hogyan tudnák az okoseszközeiket biztonságosan használni, vagy úgy gondolják, hogy nem az ő feladatuk lenne, és „nem is tesznek semmilyen intézkedést az eszközök védelme érdekében”[2],[50]. „Komoly kihívást jelent a nem megfelelő felhasználói biztonságtudatosság, hiszen ezzel is hozzájárulnak a támadók sikereihez az okoseszköz használók”[49]. Az utóbbi időben egyre többet lehet hallani arról, hogy az okoseszközeinken keresztül például megfigyelhetik a szokásainkat, vagy ellophatják a személyes adatainkat. A tömeggyártásban alacsony költségvetésből készült eszközök következménye lehet, hogy gyenge biztonsági megoldásokat tartalmaznak [14]. Az IoT-eszközök az otthonokban adatokat gyűjthetnek arról, hogy például a felhasználó mikor tartózkodik otthon, és hogy milyen fogyasztási szokásai vannak [51]. Az IoT-eszközök sérülékenyek lehetnek, amelyeket a támadók kihasználhatnak, és a sebezhetőség utólagos javítása nem egyszerű feladat [52]. Az OWASP („Open Web Application Security Project“) az IoT Sérülékenységek Projektje szerint a legfontosabb IoT sérülékenységek közül néhányat megemlítenék, például gyenge jelszavak, titkosítatlan szolgáltatások, gyenge titkosítás, hiányzó frissítési mechanizmus [53]. Az IoT-eszközök esetében gyakori, hogy gyenge jelszavakat alkalmaznak, és nem mindegyik gyártó kötelezi a felhasználót, hogy módosítsa a készülék alapértelmezett jelszavát [54]. Az IoT-eszközök gyakran nem rendelkeznek erős jelszavakkal, és nem frissítik őket rendszeresen, így sebezhetőek a támadásokkal szemben [55]. A felhasználók gyakran használnak könnyen kitalálható és könnyen megjegyezhető jelszavakat, amelyek értelmes szót vagy személyes információt tartalmazhatnak, vagy ugyanazt a jelszót több helyen is használják [56]. 2013-ban az LG okostévével rendelkező tulajdonos fedezte fel, hogy az okostévé adatokat gyűjt a nézési

szokásairól akkor is, ha a funkció ki van kapcsolva. Majd később a Samsung okostévéjénél derült ki az, hogy az okostévé beszédfelismerő funkciója személyes beszélgetéseket is rögzíthet [35]. 2019-ben az FBI szakértői hatósági közleményt adtak ki az okostévékkel kapcsolatban, melyben felhívták a figyelmet, hogy az okostévék gyártója vagy a telepített alkalmazások fejlesztői az okostévéken keresztül megfigyelhetik a felhasználót [57]. 2019-ben az Amazon Echo és a Google Home okosrendszerről derült ki, hogy adatvédelmi szempontból ezek a rendszerek nem teljesen úgy működnek, ahogy kellene hiszen ezek az eszközök sokkal több adatot gyűjtenek össze, mint amire lett volna például engedélyük, hiszen olyan információkat is rögzítettek, amelyeket a tulajdonos nem szeretett volna megosztani. A Philips Hue okosvillanykörteiről is kiderült, hogy könnyen feltörhető. Mivel Kínában készülnek tömeggyártásban alacsony költségvetésből, így nehéz elkerülni, hogy ne legyenek sérülékenyek. A felhasználók körében igen népszerűek, hiszen a kamera segítségével megfigyelhetjük az otthonunkat akkor is, ha nem tartózkodunk otthon. Az olcsó IP kamerák, amelyek az otthon megfigyelésére szolgálnak az egyik legtöbbet feltört eszközök közé tartoznak a felmérések szerint [58]. Az Amazon Ring otthonokban használt biztonsági rendszerről például kiderült, hogy adatokat oszt meg a Google és a Facebookkal. A népszerű Roomba porszívóról például azt feltételezik a kutatók, hogy a Lidar technológiát használva térérzékeléshez kifejlesztett lézeres letapogatóval képes hangot érzékelni anélkül, hogy lenne mikrofonja [59]. „Az olcsó IP kamerák, amelyek az otthon megfigyelésére szolgálnak az egyik legtöbbet feltört eszközök közé tartoznak” [60]. Az IoT-eszközök növekedésével megnőtt a kibertámadások száma az IoT-eszközök iránt. A Demandsage jelentése szerint az „Internet of Things” (IoT) kibertámadások száma 2022-ben meghaladta a 112 milliót [58]. A TheatLabz 2023-as jelentése szerint az IoT-eszközök a kibertámadások elsődleges célpontjaivá váltak, hiszen a kutatócsoport felmérése szerint 2023 első félévében rohamosan nőtt az IoT ellen elkövetett malware támadások száma a 2022-es évhez képest [56]. A vírusvédelmi szoftverek napjainkban már „nem képesek tartani az iramot a kiberbűnözők által fejlesztett újabb és újabb káros szoftverekkel.” Mivel naponta számtalan újabb változat jelenik meg egyik vírusvédelmi szoftver sem tud 100%-os védelmet nyújtani. [70]. Az IT biztonság terén számos kihívással kell szembenéznünk. A növekvő mennyiségű IoT-eszközök száma komoly kihívást jelent az IT biztonság szempontjából, például számítási kapacitáskorlát, és sokszor alacsonyabb szintű védelemmel rendelkeznek ezért a támadók könnyen kihasználhatják. „A kibertámadások

szintje a digitális világ fejlődésével egyre csak növekszik az egyik legnagyobb probléma az újabb, komplexebb támadási módszerek folyamatos megjelenése” [71].

2. INFORMÁCIÓBIZTONSÁG ÉS KIBERBIZTONSÁG

„Az információs társadalomban a rendelkezésre álló információs rendszerek és szolgáltatások létfontosságú szerepet játszanak napjainkban ezért a megbízhatóságuk, valamint a biztonságuk lényeges szempont.” [61]. „A mai digitális társadalomban, amelyben együtt van jelen a virtuális és a valós környezet, fontos az egyének megfelelő és felelősségteljes bevonása, és hogy tudatában legyenek a technológia kínált lehetőségeinek és kockázatoknak” [62]. Az informatikai rendszerek esetében a digitális adatok biztonsága a legfontosabb. Ez alatt az informatikai rendszerelemek biztonságát értjük. „Az információbiztonság az információk emberi vagy gépi úton formalizált halmazának bizalmasságát, sértetlenségét és rendelkezésre állását értjük” [63]. Az információbiztonság megvalósulnak tekinthető, ha a bizalmasság, a sértetlenség, valamint a rendelkezésre állás teljesül.

Bizalmasság: a bizalmasság alatt értjük, hogy az információkat bizalmasan kell kezelni, és csak azok férhetnek hozzá, akiknek van jogosultságuk.

Sértetlenség: a sértetlenség akkor teljesül, ha az adatkezelés során az információk pontosak, teljesek, valamint megbízhatóak maradnak.

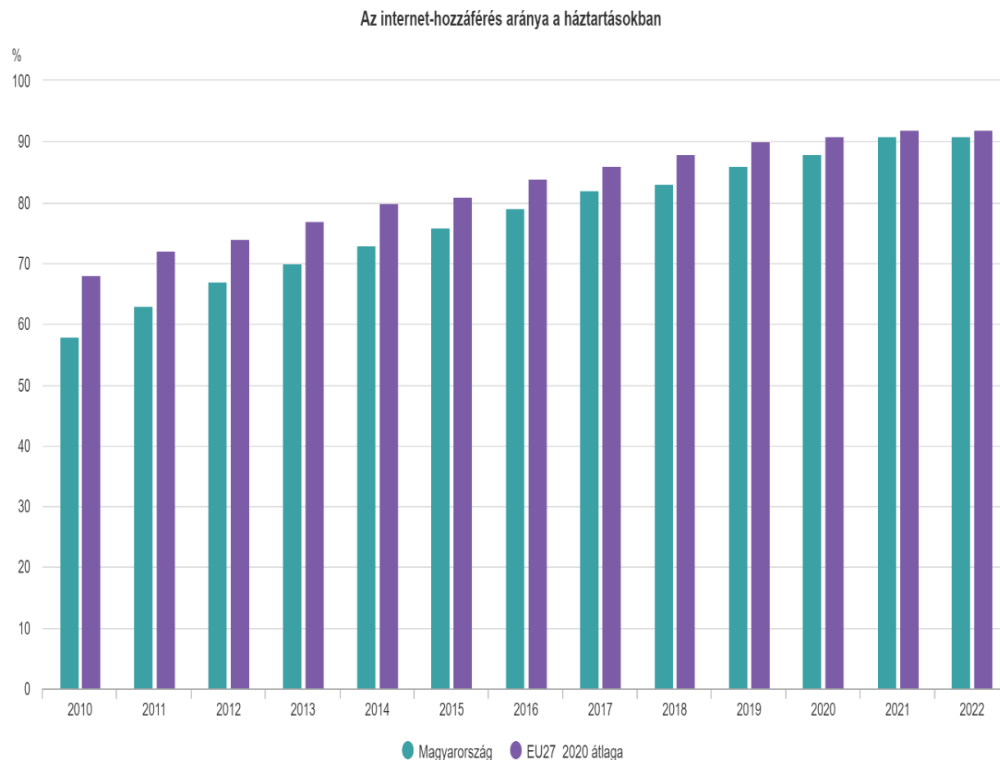
Rendelkezésre állás: az információknak és adatoknak elérhetőnek kell lenniük azok számára, akiknek van megfelelő jogosultságuk hozzá. [64]

„A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti.”[65] „A védelmet nem szabad csak a szakemberekre hárítanunk, hiszen minden felhasználónak tudatában kell lennie az őt érintő esetleges kiberfenyegetésekkel, és ezért meg kell tennie mindent a tudatos használatért” [66].

2.1. Információbiztonság tudatosságának fontossága

Elmondhatjuk azt, hogy „információs társadalomban élünk” és egyre többen használnak különféle okoseszközöket napjainkban, és várhatóan a jövőben még több okoseszköz lesz jelen az egész világon [67], [68]. A digitális technológia az élet minden területén jelen

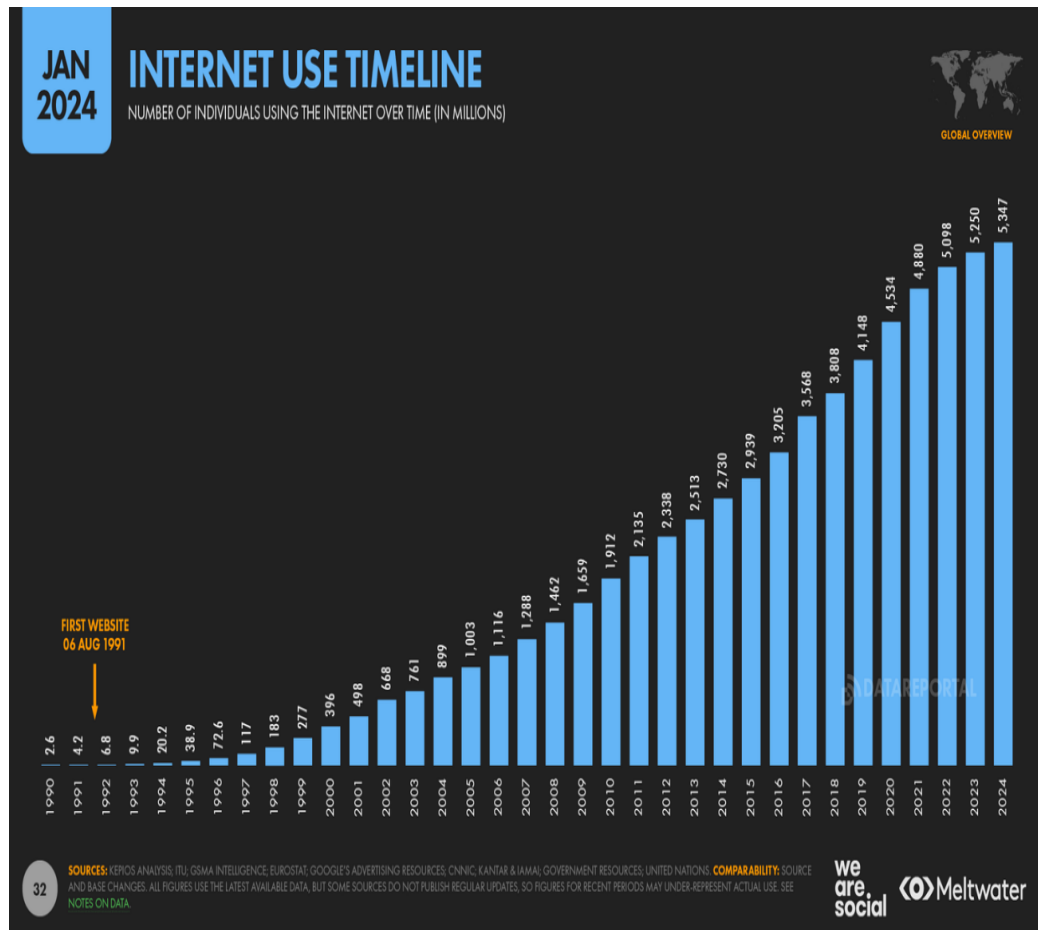
van. A koronavírus járvány alatt megnőtt az okoseszközök iránti igény, ezáltal a kibertámadások száma is megnőtt. Az információbiztonság komoly problémát okoz az egyének számára pedig számtalan megoldás, és védekezési megoldás kifejlesztésre került. „Az egyén a leggyengébb láncszem az információbiztonsági láncban”[69]. Ezért nagyon fontos az egyének biztonságtudatosságát növelni. Az információbiztonság tudatosságáról már számtalan kutatás készült, hogy mivel lehetne az egyének információbiztonság tudatosságát növelni [60]. A felmérés szerint az Európai Unióban 2020-ban a háztartások átlagosan 91%-a rendelkezik internet hozzáféréssel, addig Magyarországon 88%. Ezáltal Magyarországot megelőzik a következő országok, mint Hollandia, Németország, Finnország, Dánia, Svédország, Ausztria, Szlovénia. Magyarország után pedig a következő országok következnek, mint például Románia 86%, Szlovákia szintén 86%, Horvátország 58%, Bulgária 79% [59]. Magyarországon a Nemzeti Média és Hírközlési Hatóság (NMHH) reprezentatív kutatása szerint, amelyet 2020-ban végeztek a háztartások 71%-a felmérés szerint rendelkezik internetkapcsolattal. Magyarországon a kormány az „internetről és a digitális fejlesztésekről 2015. évi nemzeti konzultáció eredményei alapján fogadta el a magyar társadalom és a magyar nemzetgazdaság digitális fejlesztését célzó Digitális Jólét Programot, melynek egyik legfontosabb stratégiai eleme Magyarország Digitális Oktatási Stratégiája (DOS)” [70]. A 9.ábrán láthatjuk a háztartások internetellátottságát Magyarországon és az Európai Unióban 2020-ban. Láthatjuk, hogy a háztartások internetellátottsága Magyarországon és az Európai Unióban 2010-től 2022-ig folyamatosan nő.



9. ábra. A háztartások internetellátottsága 2020-ban az Európai Unióban és Magyarországon.[71]

Az Európai Unióban legtöbben az internetet a termékkel, illetve szolgáltatással kapcsolatos információk keresésére használják, valamint az e-mailek küldésére és fogadására, ezenkívül az üzenetváltásra, valamint a közösségi oldalakon való részvételre. A felmérés alapján láthatjuk, hogy Magyarországon legtöbben azt választották, hogy az e-mailek küldésére és fogadására használják. A Kantar-Hoffmann kutatócég 2022-ben felmérést végzett, amelyben 15.000 személy vett részt. A felmérés eredménye szerint a válaszadók 71%-a mobiltelefonon vagy okostelefonon szokta az internetet használni, 48%-a laptopon, 35%-a asztali számítógépen, 15%-a tableten, 8%-a TV képernyőn, és 2%-a válaszolta, hogy játékkonzolon. A felmérésben legtöbben azt választották, hogy 52% vezetékes interneten keresztül csatlakozik az internethez, 50% mobiltelefonon vagy okostelefonon Wi-fi kapcsolattal, és 43% mobilinternet előfizetéssel [72]. A Statista jelentése szerint 2024 áprilisában világszerte 5,44 milliárd internethasználó volt, ami a világ népességének 67,1%-át jelenti [52]. A Nemzeti Média és Hírközlési Hatóság 2023. május 1-től 2024. április 30-ig tartó időszak jelentése szerint Magyarországon a háztartások 84%-a rendelkezik internettel, és már az okostelefonon használt mobilinternet használata utolérte az otthoni internet szintjét. A jelentés szerint a háztartásokban használt internet 73%, míg a mobilinternet használat 75% [60]. Az ITU, a GSMA Intelligence, az

Eurostat és a különböző szervek legfrissebb adatainak elemzése szerint 2024 elején 97 millió új felhasználó lett a tavalyi évhez képest [53]. A 10. ábrán láthatjuk az internet használat idővonalát 1990-től 2024-ig. Láthatjuk, hogy az internethasználat az évek során egyre csak nő.



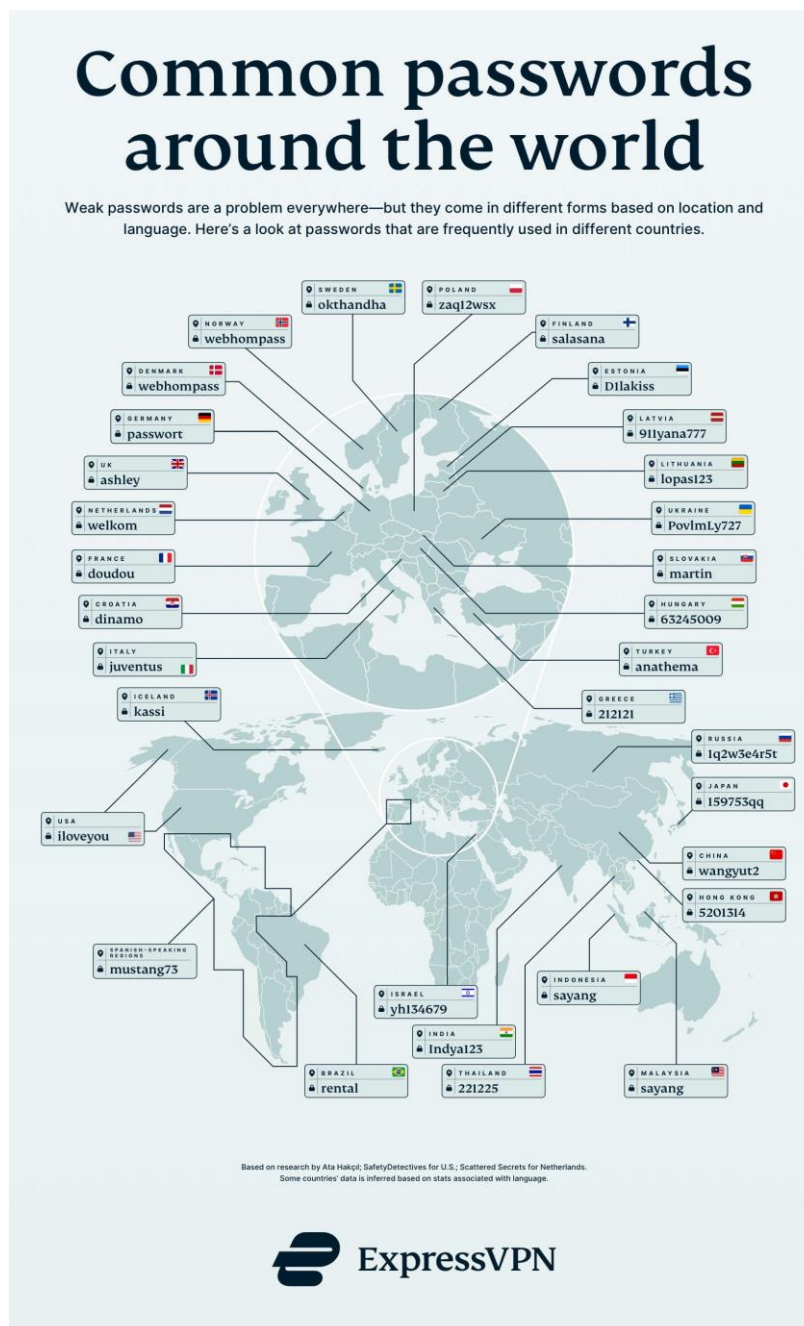
10. ábra. Az internet használatának idővonala.[73]

A Global Web Index 2017-es jelentése szerint a felhasználók internetezéssel töltött ideje korcsoportonként eltérő, és átlagosan naponta 6,5 órát töltenek a felhasználók az interneten. A 16 és 24 év közöttiek 2,5 órával több időt töltenek el az interneten, mint az 55 és 64 év közötti felhasználók a jelentés alapján [74], [75]. A 2023-as jelentés szerint egy átlagos felnőtt 4 óra és 35 percet tölt naponta az okoseszközén vagy a tabletjén [76]. Az Emarketer jelentése szerint 2025-re a tárgyak internete (IoT) eszközeivel, mint például okoshangszórókkal töltött átlagos idő el fogja érni a napi 45 percet [77]. A virtuális tér és annak használata hatalmas piacot és több milliárdnyi felhasználót hozott létre. A virtuális térben az eszközök támadásoknak vannak kitéve. Mint ahogy a fizikai életben is számos eszközzel próbáljuk magunkat megvédeni, például a zár használatával vagy önvédelmi

eszközökkel ugyanígy szükséges lenne a digitális információk védelmére is. „A tudás megszerzésének az alapvető eszköze az internetet felhasználók információbiztonsági tudatosságának kialakítása, és annak folyamatos fejlesztése, valamint a technológiai fejlettség fokának megfelelő szinten tartása” [67]. A digitális eszközök szinte már minden területen jelen vannak a mindennapi életünkben. A biztonságtudatosság nagyon fontos, hiszen „gyakran az emberi tényező bizonyul a leggyengébb láncszemnek” [78]. „Az okoseszközök hétköznapivá válásával, és a különböző funkciókat betöltő alkalmazások elterjedésével olyan információbiztonsági kockázatokkal néz szembe az átlagos felhasználó, amelyeknek talán nincs is tudatában.” Mivel olyan információkhoz juthatnak, mint például a felhasználók mindennapi szokásai, amelyekkel következtetni lehet például az adott személy tartózkodási helyére, valamint fogyasztási szokásaira, és akár a káros szenvedélyeire is [79]. „A mai digitális társadalomban fontos az egyének megfelelő és felelősségteljes bevonása, hogy tudatában legyenek a technológia kockázataival” [62].

2.2. Jelszóhasználat

Az IoT-eszközök teljes védelméhez szükséges, hogy a biztonsági beállításokat elvégezzük. Ami azt jelenti, hogy a telepítendő eszközök kezelőfelületére való bejelentkezéskor az alapértelmezett felhasználónevet és jelszót mindig meg kell változtatnunk. Mivel minden eszköz esetében azok azonosak lehetnek, így nem nehéz kitalálni a támadóknak [49]. Manapság egyre több helyen kell különböző jelszavakat használnunk, ezért a felhasználók gyakran akár több helyen is ugyanazt a jelszót használják. Egyes felhasználók rövid míg mások hosszabb jelszavakat használnak. A rövid és hosszú jelszavak használatának is vannak előnyei és hátrányai. A rövid jelszó előnye, hogy könnyen megjegyezhető, míg a hosszabb jelszót gyakran nehéz megjegyezni. Egy rövid jelszót sokkal könnyebb kitalálni, addig a hosszabb jelszó nagyobb védelmet jelent [80]. A 11. ábrán láthatjuk, hogy mely jelszavakat használták legtöbbször 2024-ben a világon néhány ország bemutatásával, mint például Lengyelország, Norvégia, Németország, Franciaország, Olaszország, Szlovákia, Magyarország, Törökország, Japán, Kína és az Amerikai Egyesült Államok. Láthatjuk, hogy vannak olyan országok, ahol kevesebb mint 8 karaktert használnak jelszónak, illetve értelmes szót tartalmazó jelszót használnak, vagy olyan jelszót használnak, ami csak számokat vagy csak kisbetűket tartalmaz.



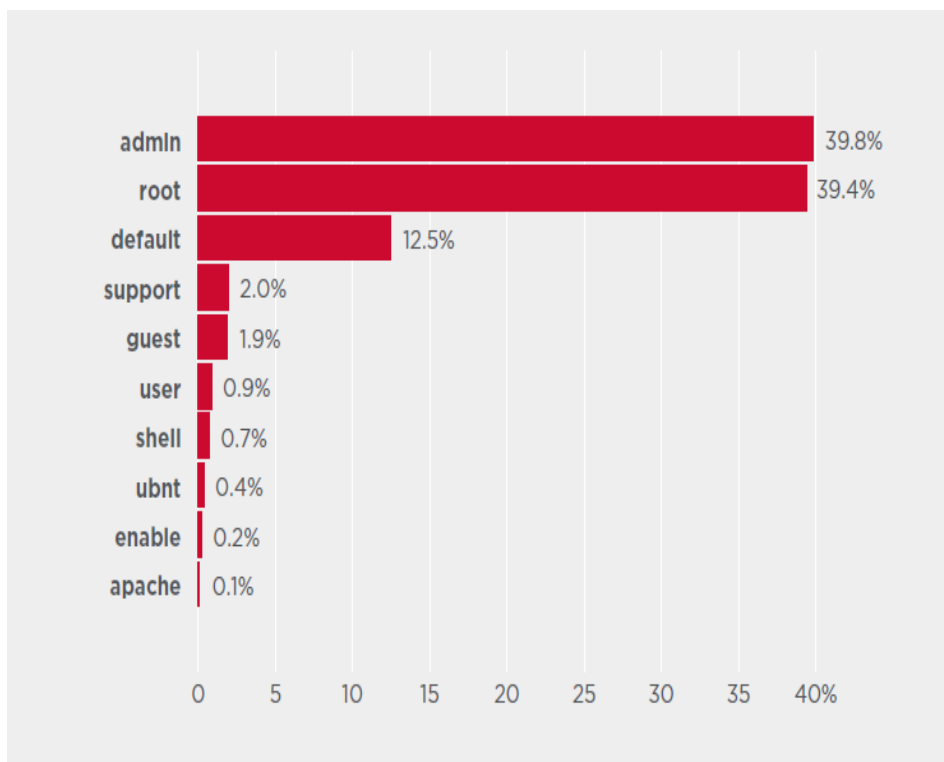
11. ábra. A leggyakrabban használt jelszavak 2024-ben a világon, néhány ország bemutatásával.[81]

A Cybernews 2024-es jelentése szerint világszerte legtöbbször „123456” jelszót használnak. A Cybernews jelentése szerint a következő jelszavakat használták legtöbbször 2024-ben:

- „123456”
- „123456789”
- „qwerty”

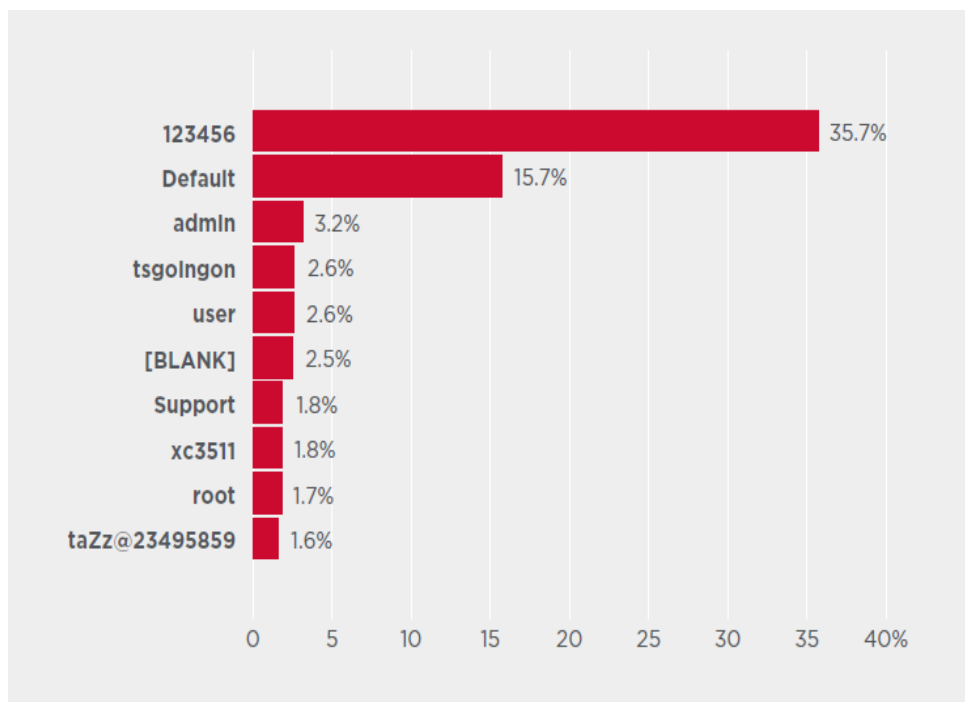
- „password”
- „12345”
- „qwerty123”
- „1q2w3e”
- „12345678”
- „111111”
- „1234567890” [82]

A Cybernews jelentése szerint az olyan jelszavak, mint a „123456”, „123456789”, „qwerty”, „password” és „12345” kerültek az öt leggyakrabban használt jelszó közé világszerte. Annak ellenére, hogy találhatunk már különböző javaslatokat arra vonatkozóan, hogyan és miért fontos az erős és egyedi jelszavak használata, valamint hogy miért ajánlott jelszókezelőt használni, sokan még mindig gyenge és könnyen kitalálható jelszavakat használnak, amelyeket még egy kezdő kiberbűnöző is könnyen feltörhet [74]. A jelentés ezen kívül azt is vizsgálta, hogy hány karakterből állnak a jelszavak, amit legtöbbször használnak. Ami alapján legtöbbször 6 és 8 karakterű jelszavakat használnak a Cybernews 2024-es jelentése szerint [82]. Az IoT-eszközök esetében a gyenge jelszavak súlyos következményekkel járhatnak, mivel a támadók kihasználhatják őket [83]. Ezért fontos, hogy minden eszközön erős jelszót használjunk [84]. A Statista jelentése szerint 2021-ben az IoT-eszközök öt leggyakrabban használt jelszava a következő volt: „admin”, „root”, „nc11”, „user” és „enable” [85]. Vannak olyan okoseszköz felhasználók is, akik még az alapértelmezett jelszót sem változtatják meg, és például „123456”-ot, vagy olyan jelszót használnak, amely értelmes szavakat vagy személyes adatokat tartalmaz, mint például a születési dátum vagy a kedvenc háziállatuk nevét [86]. A NordPass jelentése szerint a leggyakoribb jelszó 2019-ben „12345” volt, majd ezt követte az „123456” 2020-2021-ben, majd pedig a „password” 2022-ben [87]. A Symantec jelentése szerint 2020-ban a 10 leggyakrabban használt felhasználónév az IoT elleni támadásakor a 12. ábrán látható. Láthatjuk, hogy a leggyakrabban használt felhasználónév az „admin” volt.



12. ábra. A Symantec jelentése 2020-ban a 10 legtöbbet használt felhasználónevet tartalmaz , amit használtak az IoT elleni támadások során [88]

A jelentés alapján megfigyelhető, hogy a legnépszerűbb felhasználónév az „admin” volt (39,8%), majd ezt követi a „root” (39,4%), és a „default” (12,5%). A 13.ábrán láthatjuk a Symantec jelentése szerint 2020-ban a 10 legtöbbet használt jelszót. Látható, hogy a legtöbbet használt jelszó az „123456” volt.



13. ábra. A Symantec jelentése 2020-ban a 10 legtöbbet használt jelszó, amit használtak az IoT elleni támadásokor. [88]

A 13. ábrán látható, hogy az IoT-eszközök esetében a legtöbbet használt jelszó az „123456” (35,7%), majd a „default” (15,7%) és az „admin” (3,2%). Az is előfordulhat azonban, hogy több helyen ugyanazt a jelszót használják. Mivel így nem kell több jelszóra emlékezniük, hanem elég megjegyezni a megadott jelszót. Az egyszerű jelszavak használata nem biztonságos, mivel könnyen kitalálhatók, amit a támadók könnyen kihasználhatnak [83]. 2019-ben a feltört jelszavak 80%-a anyagi veszteségeket okozott a vállalatoknak és a felhasználóknak is [89]. A Security.org szerint egy 7 karakterből álló jelszó feltörése 2 másodpercig tart, ha csak kis és nagybetűket, valamint számokat tartalmaz, ha pedig a jelszó nem tartalmaz számokat, akkor még kevesebb idő szükséges, mivel 1 másodperc is elegendő a jelszó feltöréséhez [90].

A jelszó használatakor fontos, hogy figyeljünk a következőkre:

- Az alapértelmezésben megadott jelszavakat ne használjuk, mindig meg kell változtatni.
- Fontos, hogy a jelszavaknak erősnek kell lenniük, és nem szabad, hogy személyes információkat tartsanak.
- Ugyanazt a jelszót ne használjuk fel több helyen.

- Fontos, hogy a jelszavakat rendszeresen változtassuk meg, és ne használjuk ugyanazt a jelszót különböző szolgáltatásokhoz.
- Fontos, hogy a jelszó tartalmazzon számokat, kis és nagybetűket, valamint speciális karaktereket.

A jelszókezelő használata segítségül szolgálhat, hiszen megkönnyíti az összes jelszó megjegyzését, és általában az összes jelszót egy fő jelszóval védi. Mivel a jelszókezelők tárolják az összes jelszót, ezért támadási célponttá válhatnak. Ezért fontos, hogy csak megbízható jelszókezelőt használjunk [62].

A támadók a jelszavakat feltörhetik a „brute force” és a szótáralapú támadással. A „brute force”, vagy magyarul nyers erő támadás esetében a támadók a „lehetséges karakterek kombinációiból próbálják a jelszót összeállítani.” A rövid jelszavak esetében a támadóknak ezt sokszor sikerül is végrehajtaniuk. A szótáralapú támadás esetében pedig a támadók kipróbálják az értelmes szavakat és a gyakran használt jelszavakat. A Nemzeti Kibervédelmi Intézet a jelszavak kezelésére a következő ajánlásokra hívja fel a figyelmet. A jelszavak esetében fontos, hogy csak mi használjuk, és ne adjuk más személyeknek oda. Ezenkívül felhívják a figyelmet arra is, hogy a jelszavakat ne írjuk le, mert lehetséges, hogy így elveszíthetjük, vagy illetéktelen kezébe fog kerülni. A Nemzeti Kibervédelmi Intézet felhívja a figyelmet arra, hogy ugyanazt a jelszót ne használjuk több helyen, mivel ha a támadók feltörik a jelszót, akkor a többi helyen is, ahol ugyanazt a jelszót használtuk, ahhoz is hozzáférhetnek. Ezen kívül nagyon fontos, hogy a jelszavakat rendszeresen változtassuk meg [91].

2.3. Európai Unió szabályozásai

Az Európai Unió Kiberbiztonsági Ügynökség (ENISA) 2004-ben jött létre, és célja, hogy biztosítsa Európa szerte az egységes és magas szintű kiberbiztonságot. Az ENISA „hozzájárul az uniós kiberpolitikához, kiberbiztonsági tanúsítási rendszerek alkalmazásával javítja az IKT termékek, szolgáltatások és folyamatok megbízhatóságát” [92]. Az Európai Bizottság fontosnak tartja, hogy „szilárdabb és ellenállóbb biztonsági kereteket biztosítson az IoT-eszközök és azon hálózatok számára”[93]. Az Európai Unió Tanácsa elfogadta a következtetéseket a csatlakoztatott eszközök kiberbiztonságáról 2020-ban, melyben elismerték, hogy „az internetre csatlakoztatott fogyasztási cikkek, valamint az ipari eszközök a használata megnőtt”, valamint a magánéletben, az információ és kiberbiztonsági téren is új kockázatok jöttek létre [93]. „A kibertámadások

és a kiberbűncselekmények Európa szerte egyre gyakoribbá és egyre kifinomultabbá válnak”[94]. Várhatóan a jövőben ez tovább fog növekedni, mivel 2025-re világszerte 41 milliárd készülék fog majd kapcsolódni a dolgok internetéhez. Úgy gondolják, hogy „amennyiben komoly kiberbiztonsági intézkedéseket hoznak, ezáltal a polgároknak nagyobb fog lenni a bizalma a digitális eszközök iránt, ezért 2020-ban az Európai Bizottság és az Európai Külügyi Szolgálat új uniós kiberbiztonsági stratégiát terjesztett elő” [8]. „A hálózati és információs rendszerek biztonságáról szóló irányelv 2016-ban lépett életbe”, amely az első olyan intézkedés, ami az Európai Unió szerte alkalmazandó [95]. Az Európai Unió Kiberbiztonsági Ügynökség (ENISA) oldalán megtalálható ajánlások az IoT biztonságára az 1. táblázatban láthatók.

1. táblázat. Az ENISA ajánlásai az IoT biztonságára. Forrás: Saját szerkesztés

Megjelenés éve	Ajánlások
2017	Alapvető biztonsági ajánlások az IoT-re - A kritikus információs infrastruktúrák összefüggésében.
2019	Bevált gyakorlatok az IoT biztonságára - Biztonságos szoftverfejlesztési életciklus.
2020	Útmutató a dolgok internete védelméhez- Biztonságos ellátási lánc.

2017-ben megjelent az ENISA tanulmánya az Alapvető biztonsági ajánlások IoT-re. A kritikus információs infrastruktúrák összefüggésében melynek célja, hogy betekintést nyújtson az IoT biztonsági követelményeibe. Az IoT termékek és szolgáltatások biztonságának a biztosítása alapvető prioritás, hiszen az IoT ellen irányuló támadások veszélyeztethetik az emberek, valamint a magánéletük biztonságát. Emellett személyes adatokat gyűjtenek, elemeznek, használnak, ami által adatvédelmi aggályok merülnek fel. Az IoT biztonsági intézkedéseinek meghatározásakor a legnagyobb kihívást az IoT alkalmazási területeinek a sokfélesége okozza [96]. „A személyes adatok megfelelő szintű védelme érdekében az Európai Unió egy mindenre kiterjedő, átfogó szabályozást alkotott meg. Ez az ún. Általános Adatvédelmi Rendelet (General Data Protection Regulation, röviden: GDPR)” [97]. 2019-ben jelent meg az ENISA tanulmánya a Bevált gyakorlatok az IoT biztonságára - Biztonságos szoftverfejlesztési életciklus címmel. Ennek a dokumentumnak a célja az IoT SDLC biztonsági intézkedéseinek a kidolgozása, valamint az, hogy iránymutatásokat és ajánlásokat nyújtson [98]. 2020-ban megjelent az ENISA harmadik tanulmánya, amely az előző kettő tanulmányra épül fel. A tanulmány

az Útmutató a dolgok internete védelméhez Biztonságos ellátási lánc az IoT-re címmel jelent meg, amely iránymutatásokat határoz meg az IoT ellátási lánc biztosítására [99]. „Az Európai Unió 2022-ben fogadta el a 2016-os irányelv helyébe lépő kiberbiztonsági irányelvet a NIS 2 irányelvet” [8]. „Az új uniós kiberbiztonsági szabályok biztonságosabb hardvereket és szoftvereket biztosítanak.” [100] Az okoseszközök a hétköznapi életünk részévé váltak, és a felhasználók számára sokszor nem egyértelmű, hogy milyen biztonsági kockázatot hordoznak magukkal. „A kiberreziliencia-törvény (CRA) célja, hogy megvédje a digitális komponenssel rendelkező termékeket, vagy szoftvereket vásárló vagy használó fogyasztókat és vállalkozásokat. A rendelet minden olyan termékre vonatkozik, amely közvetlenül vagy közvetve kapcsolódik egy másik eszközhöz vagy hálózathoz” [94]. A kiberrezilienciáról szóló jogszabály 2024-ben fog várhatóan hatályba lépni, és 2027-ig kell a gyártóknak az uniós piacra megfelelő termékeket forgalomba hozniuk [101].

3. INFORMATIKAI OKTATÁSI TANANYAG

3.1. Informatikai oktatási tananyag Magyarországon

Az informatikai tanterv követelményei a Művelődési Minisztérium tantervében 1988-ban jelentek meg minden diák számára. A követelmény az általános iskolások számára a 4. és a 8.osztály technikai tantárgyában jelent meg. A gimnáziumok első, valamint második évfolyamai számára szintén a technika tantárgyban jelent meg. A külön tantárgyra való igény a 80-as évek vége felé egyre fontosabbá vált. A Nemzeti alaptantervet 1995-ben fogadták el, és 1998-ban az informatika önálló műveltségterületként jelent meg [102]. Hazánkban 2020 szeptemberében az informatika tantárgyat felváltotta a digitális kultúra tantárgy, amely „a hagyományos informatikaórák helyett tartalmában, és célkitűzéseiben is megújult digitális kultúra vette át” [103]. Magyarországon a „digitális kultúra fejlesztése 3–4. évfolyamon a tevékenysékedtetés módszerével, gyakran digitális eszközök közvetlen használata nélkül történik, addig az 5–6. évfolyamon a tanulók már rendszeresen használják a számítógéptermet, és az iskola számítógépes hálózatát.”[104] A digitális kultúra tantárgy a Nemzeti alaptantervben rögzített kulcskompetenciákat az alábbi módon fejleszti, mint például tanulási, kommunikációs és digitális kompetenciák.

A 2. táblázatban láthatjuk a 2020-ban kiadott Nemzeti alaptantervet és kerettantervet a digitális kultúra tantárgyra. Láthatjuk évfolyamok szerint a heti óraszámot, és hogy összesen hány órából áll az adott évfolyam számára a digitális kultúra tantárgy.

2. táblázat. A Nat a digitális kultúra tantárgy során az óraszámok az évfolyamok szerint a 2020-ban kiadott Nemzeti alaptanterv és kerettantervek alapján.[104]

Évfolyam	Heti óraszám	Összesen
1-2.	Nem jelenik meg önálló tantárgyként.	
3-4.	1+1	68
5-6.	1+1	68
7-8.	1+1	68
9-10.	2+1	102
11.	2	68

Az 5–6. évfolyamon a digitális kultúra tantárgy alapóraszámja 68 órából áll, ahol a diákok olyan témakörökről tanulhatnak, mint például az online kommunikáció, az információs társadalom, e-Világ, digitális eszközök használata. Az online kommunikációs témakörnél

pedig a diákok már arról tanulnak, hogy tisztában legyenek a hálózatot és a személyes információkat érintő fenyegetésekkel, valamint hogy tudják alkalmazni az adatok védelmét biztosító lehetőségeket. Az 5-6 évfolyamnál az online kommunikáció 5 órából áll. Ennek a témakörnek a célja, hogy a diákok tisztában legyenek például a hálózatot és a személyes információkat érintő fenyegetésekkel, és hogy kezelni tudják „az operációs rendszer mappáit, fájljait és a felhőszolgáltatásokat.”[104]

Az információs társadalom, e-Világ a 5-6 évfolyamnak 6 órából áll, melynek célja, hogy a tanuló a következőket sajátítsa el, mint például:

- „Ismerje az információs társadalom múltját, jelenét, valamint a várható jövőjét.”
- „Tudjon védekezni az internetes zaklatás különböző formái ellen, és szükség esetén segítséget kérjen.”

Az 5-6 évfolyamban a digitális eszközök használata témakör 4 órából áll, melyben a diákok a következőkről tanulnak, mint például:

- „Az informatikai eszközöket önállóan tudják használni, és a tipikus felhasználói hibákat el tudják kerülni, valamint az egyszerűbb felhasználói szintű hibákat el tudják hárítani.”
- „Értelmezni tudják az informatikai eszközöket működtető szoftverek hibajelzéseit, és azokról be tudjanak számolni.” [104]

A 7–8. évfolyamon a digitális kultúra tantárgy alapóraszám szintén 68 órából áll. Ennél az évfolyamnál a tananyag kapcsolódik az 5–6. évfolyam tananyagához [105], [24]. A középiskolás tananyagban a diákok a témakör feldolgozása során tanulnak például az „okoseszközök okos használatára, a tudatos felhasználói és vásárlói magatartás alakítására, a biztonsági okokból bevezetett korlátozások megismerésére és elfogadására.” [106] A 9-10 évfolyamban az információs társadalom és e-Világ témakör 3 órából áll, mely által a tanulók megtanulják a következőket:

- Tudják alkalmazni az adatok védelmét biztosító lehetőségeket a gyakorlatban.
- Tisztában legyenek a „digitális személyazonosság és az információhitelesség fogalmával.”

A 9-10. évfolyamban az online kommunikáció témakör 4 órából áll, mely során a tanuló a következőket sajátítsa el:

- „Az online kommunikáció során alkalmazni tudja a kialakult viselkedési kultúrát és szokásokat, valamint a szerepelvárásokat.”
- „Ismerje és alkalmazni tudja az információkeresési stratégiákat és technikákat, a találati listát a problémának megfelelően szűri, ellenőrzi annak hitelességét.”
- „Ismerje és alkalmazza a fogyatékkal élők közötti kommunikáció eszközeit és formáit.”

A 9-10. évfolyamban a digitális eszközök használata témakör 6 órából áll, melyek során a tanuló a következőket sajátítsa el, mint például:

- „Tudatosan alakítja az informatikai környezetet, és ismeri az informatikai környezet jellemzőit, figyelembe veszi a digitális eszközök egészségkárosító hatásait, óvja saját, valamint a környezete egészségét.”
- „Tisztában van a digitális kártevők elleni védekezés lehetőségeivel.”
- „Ezenkívül önállóan tudja használni az informatikai eszközöket, és el tudja kerülni a tipikus felhasználói hibákat, valamint elhárítja az egyszerűbb felhasználói hibákat.”[106]

A középiskolában a 9-10. évfolyam digitális kultúra tantárgy 102 órából áll, a 11. évfolyamon az óraszám 68 órából. A 11.évfolyamban az információs társadalom, e-Világ témakör 4 órából áll, az online kommunikáció és a digitális eszközök használata 2 órából [104], [106].

3.2. Informatikai oktatási tananyag Szerbiában

Szerbiában 1985 és 1986-ban vezették be a 8.évfolyam számára a Műszaki oktatásban első alkalommal az Elektronika és Informatika tantárgyat. Majd 1995-ben vezették be a 7.évfolyam számára az Információs technikát. Majd 2004/2005-ben bevezették az általános iskolások számára első osztálytól az ötödik osztályig választható tantárgyként [107]. A Tanjug hírügynökség 2016-os jelentése szerint az Országos Oktatási Tanács úgy döntött, hogy az Informatika és Számítástechnika az általános iskolások számára választható tantárgy fog maradni, és nem fogják kötelező tantárggyá tenni. Viszont az 5.

évfolyamtól a 8. évfolyamig továbbra is kötelező lesz a heti két óra Műszaki és Informatika tantárgy, valamint a heti egy óra Informatika és Számítástechnika tantárgy. Ezenkívül 2016-ban az Informatika és Számítástechnika tantárgy a középiskolákban kötelező tantárggyá vált [108]. A 3. táblázatban láthatjuk az informatika megjelenését a szerbiai tantervben az évek során.

3. táblázat. Az informatika megjelenése az általános és középiskolák tantervében Szerbiában. Forrás: a szerző szerkesztése

Év	Évfolyam
1985/1986	A 8. évfolyam számára első alkalommal jelenik meg az Elektronika és Informatika tantárgy.
2004/2005	Az általános iskolások számára első osztálytól az ötödik osztályig választható tantárgy az informatika.
2016	Az Informatika és Számítástechnika az általános iskolások számára választható tantárgy, viszont az 5. évfolyamtól a 8. évfolyamig továbbra is kötelező a heti két óra Műszaki és Informatika tantárgy, valamint a heti egy óra Informatika és Számítástechnika tantárgy.
2016	2016-tól az Informatika és Számítástechnika tantárgy kötelező a középiskolákban.
2017/2018	Az innovatív tanterv alkalmazása az általános iskolákban az Informatika és Számítástechnika tantárgy bevezetése.
2020/2021	Az általános iskolások számára az informatikai tantárgy kötelező az 1. évfolyamtól az 5. évfolyamig.

A Szerb Köztársaság Oktatásfejlesztési Stratégiája felismerte a fontosságát annak, hogy új technológiákat vezessen be az oktatási rendszer javítása érdekében, ezért Szerbiában az általános iskolák 2017/2018-as tanévben már az innovatív tanterv alkalmazását kezdték meg, amikor bevezették az Informatika és Számítástechnikát, majd a Technika és technológia alapfokú oktatást, melyet a tanulók 2018/2019-es tanévtől követhetnek [107]. A 2020/2021-es tanévben a diákok alapfokú oktatást kapnak az általános iskolákban. Az 1.évfolyamtól a 4. évfolyamig a Digitális Világ tantárgy során, majd szabadon választhatják választható tantárgyként a Játékoktól a számítógépig tantárgyat, amely nem kötelező tantárgy. Szerbiában a 2020/2021-es tanévtől az informatika tantárgy kötelezővé vált az általános iskolások számára [109]. Az 5. évfolyamban tanulók a Technika és technológia tantárgy mellett a következő kötelező tantárgyakat tanulják: a 6. évfolyamban Műszaki és Informatikai oktatás, majd a 7.évfolyamban a Számítástechnikát. Szerbiában az általános iskolások az 5.évfolyamban az Informatika és Számítástudomány tantárgyból a következő témákat tanulják a 2017-2018-as évfolyamban, ami összesen 36 órából áll:

- Információ és kommunikációtechnológia
- Digitális írástudás
- Számítástechnika
- Projektoktatás

Az információ és kommunikációtechnológia témakörnél a tanulók a következő témákról tanulnak, mint például:

- Az IKT eszközök hardver és szoftveregységei.
- A munkakörnyezet beállítása.
- Az adatok gyűjtése.

A digitális írástudásnál a tanulók a következő témákról tanulnak:

- Az IKT eszközök felelősségteljes és biztonságos használata.
- Előírások a biztonságos internet használatához.
- Internetes keresés, és a keresett tartalom letöltése.
- Személyes adatok védelme.
- A függőség kockázata technológiai eszközök használatától [110].

A 6. évfolyamban a tanulók az internet témaköréről tanulnak 4 órában, a következő témákról, mint például:

- Internet és elektronikus posta.
- Keresés az interneten.
- Biztonsági kód a számítógépen, vírusok [111].

Szerbiában a 7. évfolyamban a tanulók az internet témaköréről összesen 6 órában tanulnak, mely a következő témakörökből áll:

- Az elektronikus kommunikáció biztonsága az interneten.
- Blog, fórum, vita és megjegyzések megfogalmazása az interneten.
- Videókonferencia és elektronikus tanulás, valamint távoktatás.
- Digitális könyvtár, elektronikus posta [112].

Szerbiában a 8. évfolyam Informatika és Számítástudomány tantárgyának a felépítése a következőkből áll, mint például:

- Táblázatkezelés.
- Választható modulok.
- Projekt készítése [113].

Szerbiában a középiskolák, amelyek nem az IT és a digitális ágazatokhoz tartoznak, csak az első évben kötelező számukra a Számítástechnika és Informatika tantárgy. A lakosságnak szóló tanfolyamok, valamint képzések esetében a pénzügyi szempont nagyon fontos szerepet kap, hiszen aki szeretné a digitális kompetenciáit fejleszteni, szüksége van például külön tanfolyamokat elvégeznie, és azokat kifizetnie. Ezért, akiknek nincs rá lehetőségük és nincs pénzük kifizetni a külön tanfolyamokat, sajnos nem tudják úgy fejleszteni magukat, mint azok, akiknek van rá lehetőségük. Ezenkívül nagyon kevés tanfolyam és képzés foglalkozik a lakosság digitális kompetenciáival, mint például az eszközök és az adatok védelmével [114]. Szerbiában a RATEL a köztársasági statisztikai intézet jelentése szerint 2023-ban a legtöbben a 16 és 24 éves korosztály használta az internetet, és legtöbben okostelefonon [115].

3.3. Informatikai oktatási tananyag Szlovákiában

Az Európai Unió a tagállamok számára ajánlásokat fogalmaz meg a tagországok oktatáspolitikájára vonatkozóan, de minden ország saját maga határozhatja meg a döntéseit. „A 245/2008 sz. Köznevelési Törvény értelmében (Zákon č. 245/2008 Z.z. o výchove a vzdelávaní) az állami oktatási program a nevelés és oktatás szabályozására vonatkozó nemzetközi szabványnak megfelelően kidolgozott, hierarchikusan a legmagasabb szintű tantervi dokumentum Szlovákiában. Szlovákiában a nemzeti tanterveket a Szlovák Köztársaság Oktatásügyi, Tudományos, Kutatási és Sportminisztériuma adja ki” [116]. A kerettanterv határozza meg az időbeosztást a tantárgyakra, és az iskola az előírásokat figyelembe véve dönthet arról, hogy az egyes tananyagokat mikor fogja oktatni időbelileg. Szlovákiában a kerettantervben le van írva szintek szerint az informatika órák száma, hogy hány óra szükséges. Ezenkívül az iskoláknak lehetőségük van döntést hozni arról, hogy mely tantárgyakat szeretnék több óraszámban oktatni. „Szlovákiában az informatikai kerettantervhez minden témakörhöz kapcsolódik teljesítménystandard és tartalmi standard [117]. A 4. táblázatban láthatjuk az

informatikai óraszámokat Szlovákiában, melyek száma kötelező a kerettanterv szerint egyes szinteken, mint például az általános iskola (alsó és felső tagozat) és gimnázium számára.

4. táblázat. Informatikai óraszám Szlovákiában.[118] [119]

Általános iskola	1-4 évfolyam	2 óra
	5-8 évfolyam	4 óra
Gimnázium		3 óra

Az informatikai kerettantervben megtudhatjuk, hogy Szlovákiában az általános iskolások a 4. évfolyam végére olyan témakörökről tanulnak, mint például az internet veszélyei, és ezenkívül tudniuk kell alkalmazni a jogosulatlan e-mailek „használatára elleni védelmére vonatkozó szabályokat.” A 6. évfolyam végére pedig a diákoknak tisztában kell lenniük például az internet veszélyeivel, az adatok védelmére vonatkozó szabályokat tudják alkalmazni, tudniuk kell a kiberbűnözésről. A 8. évfolyam végére pedig a diákoknak olyan témakörökkel kell, hogy tisztában legyenek, mint például az internet kockázatai, tudniuk kell értékelni, mely információkat kell védeni a visszaélésektől, tisztában kell lenniük a rosszindulatú szoftverek használatának a veszélyeivel, és tudatában kell lenniük a számítógépes bűnözésnek. „A gimnáziumi oktatás informatikai kerettantervében is megjelenik a biztonság és rizikó témakör”[119]. A tanulóknak a gimnáziumban már tudniuk kell például a rosszindulatú szoftverek kockázatait, fel tudják ismerni a számítógépes bűnözést, fel tudják mérni az interneten található információk megbízhatóságát, valamint tudniuk kell biztosítani az adatokat és a kommunikációt az esetleges visszaélésekkel szemben [117].

3.4. Részkövetkeztetések

Több tanulmány is található, amely foglalkozik Magyarország és Szerbia informatikai oktatási tananyagával. Az eddigi elemzések, melyek vizsgálták a két ország informatikai oktatási tananyagát, azt mutatják, hogy Magyarország előnyben van Szerbiához képest. Magyarországon és Szerbiában az informatikai oktatás területén vizsgált eddigi felmérések eltérést mutatnak a két ország informatikai tananyagában [120], [121], [122]. Magyarország és Szlovákia informatikai oktatási tananyaga között is különbség található [117], [119]. Az informatikai oktatási tananyag Magyarországon, Szerbiában és Szlovákiában is eltérő. Szerbiában a középiskolások, akik nem az IT, valamint a digitális

ágazatokhoz tartoznak, számára csak az első évben kötelező a Számítástechnika és Informatika tantárgy. Szerbiában a lakosságnak szóló tanfolyamok, valamint egyéb képzések esetében a pénzügyi helyzet fontos szerepet játszik, hiszen aki szeretné magát fejleszteni szüksége van külön tanfolyamokon részt venni, és ha nincs rá pénze, akkor nem tudja úgy fejleszteni magát, mint akiknek van lehetőségük különböző tanfolyamokat kifizetni. Ezáltal Szerbiában a lakosság azon része, aki nem tudja a különböző tanfolyamokat kifizetni, nem tudja magát úgy fejleszteni, mint akinek van rá lehetősége. Ezen kívül Szerbiában még mindig kevés tanfolyam és képzés foglalkozik a lakosság digitális kompetenciáival, mint például az eszközök és az adatok védelmével. Magyarországon 2020-ban az informatika tantárgyat felváltotta a digitális kultúra tantárgy, amely a hagyományos informatikaórák helyett tartalmában és célkitűzéseiben is megújult digitális kultúra vette át. Magyarországon a középiskolás tananyagban a diákok a témakör feldolgozása során tanulnak az okoseszközök tudatos felhasználói és vásárlói magatartásának alakítására. Szerbiában azok a középiskolások, akik nem az IT, valamint a digitális ágazatokhoz tartoznak számára csak az első évben kötelező a Számítástechnika és Informatika tantárgy. Szerbia az elmúlt évek során több lépést is tett, hogy próbálja javítani az oktatási rendszert, de további javításokra lenne szükség, ha összehasonlítjuk Szerbia és Magyarország informatikai oktatási tananyagát. Amennyiben összehasonlítjuk Magyarországot és Szlovákia informatikai oktatási tananyagát, láthatjuk, hogy a két ország informatikai oktatási tananyaga között is különbség van. Magyarországon az informatika óraszámok száma alapján több informatikai óraszám van, mint Szlovákiában. Az is látható, hogy a két ország tantervében különbség van még a biztonság és a kockázat témakör esetében, mivel Szlovákiában nagyobb hangsúly van a biztonság és a kockázat témakörre fektetve.

4. KVANTITATIV KUTATÁS AZ OKOSESZKÖZ HASZNÁLÓK KÖRÉBEN FELMÉRÉS EREDMÉNYEINEK ELEMZÉSE

A kutatásom során a kvantitatív módszereket alkalmaztam. A kutatásom célja az volt, hogy részletesen feltárjam leíró statisztikai módszerekkel, hogy az okoseszköz használók mely okoseszközöket használják legtöbbször, mely márkák a legnépszerűbbek, és hogy milyen gyakran, valamint milyen hosszú jelszavakat használnak az okoseszköz használók. Emellett azt is vizsgáltam a felmérésben, hogy a résztvevők közül hányan használnak okoseszközöket, melyek a legnépszerűbb okoseszközök és márkák, melyek a legfontosabb szempontok az okoseszközök vásárlásakor, használnak-e vírusvédelmet, a firmware frissítéseket telepítik-e, valamint az applikációkat frissítik-e rendszeresen. A jelszóhasználatra vonatkozóan használnak-e kis és nagybetűket, számokat, speciális karaktereket, tartalmaz-e személyes információt a jelszó, értelmes szót, ugyanazt a jelszót használják-e több helyen, milyen gyakran változtatják a jelszót, illetve hogy milyen hosszú jelszavakat használnak.

4.1. Kutatási adatok

A felmérésben résztvevők a kérdőívet online tölthették ki. A kérdőív kitöltése névtelenül és önkéntesen történt. A felmérést három országban végeztem: Magyarországon, Szerbiában és Szlovákiában. A kutatás mindhárom országban online történt. Mivel Szerbiában élek, ezért fontosnak gondoltam, hogy a kérdőívet elkészítsem szerb nyelven is. Magyarországon és Szlovákiában a kérdőív kitöltése magyar nyelven történt.

4.2. A kérdőív

A kérdéseket az eddigi szakmai tanulmányaim alapján állítottam össze. A célom ezzel a kérdőívvel az volt, hogy bebizonyítsam a felhasználói oldal információbiztonsági tudatlanságát, hogy nem rendelkeznek megfelelő ismeretekkel ahhoz, hogy az okoseszközöket biztonságosan tudják használni a jelszóhasználat esetében. A kérdéseket úgy próbáltam megfogalmazni, hogy mindenki számára érthető legyen. Fontos volt, hogy a kérdések minél érthetőbbek legyenek a válaszadók számára, és a felmérésben résztvevőknek lehetősége legyen több lehetséges közül is választani, valamint fontosnak tartottam, hogy a saját véleményüket is le tudják írni a felmérésben. A kérdőív összesen

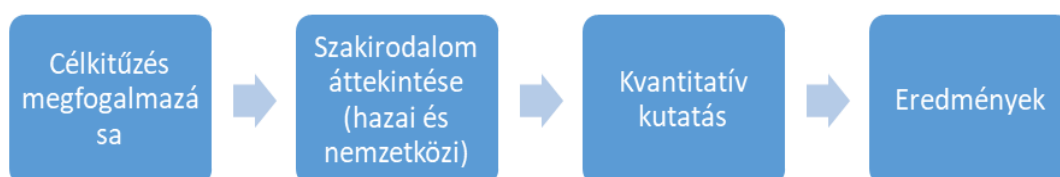
20 kérdést tartalmaz, és a felmérés online történt. A felmérésben összesen 447 résztvevő vett részt Szerbiában, Magyarországon és Szlovákiában.

4.3. A kutatás módszertana

A kutatási módszereknél statisztikai módszereket alkalmaztam. „A kvantitatív kutatások azon alapulnak, hogy a vizsgálat tárgyát képező jelenségek mérhető, megszámlálható, számszerűsíthető, és az így nyert adatok statisztikai módszerekkel elemezhető. A fenti megközelítésből adódóan a kvantitatív eljárást megfelelő elemszámú mintán elvégezve, az eredmények megbízhatósága és pontossága meghatározható” [123]. A kvantitatív kutatás célja, hogy információt gyűjtsön a társadalom vagy egy szervezet meghatározott csoportjáról. „Kvantitatív kutatás objektív, számszerűsíthető, statisztikailag mérhető, értékelhető adatok gyűjtése. Elsősorban az ok-okozati, valószínűségi összefüggéseket vizsgáló kutatások keretein belül alkalmazzák. Jellemzően matematikai-statisztikai elemzési módszerekkel” [124].

4.4. Kutatási lépések

A kutatási lépések során először is megfogalmaztam a célkitűzést, ezután a szakirodalmi áttekintés következett. Majd a kvantitatív kutatás és a kérdőív szerkesztése, a kérdőív megosztása, és ezután az adatok elemzése következett. Első lépésként az online kérdőívben kapott válaszokat az Excel táblázatban dolgoztam fel, majd ezután az SPSS statisztikai szoftvert használtam az adatok pontosítására. A 14. ábrán láthatjuk a kutatás folyamatát.



14. ábra. A kutatás folyamata. Forrás: Saját szerkesztés

A kérdőív összesen 20 kérdésből áll. A kutatás 2023-ban kezdődött és 2024 február 3-án zárult. A kérdőívet online lehetett kitölteni. A kérdőív kitöltése anonim módon, önkéntesen és névtelenül történt. Az online kérdőív mellett azért döntöttem, mert a

válaszadóknak így lehetőségük volt névtelenül anonim módon részt venni a felmérésben, és így lehetőségük volt őszintén válaszolni a kérdésekre, amennyiben szükségesnek gondolták így több idő állt rendelkezésükre kiválasztani a megfelelő választ. Ezenkívül a felmérés három országban történt, így a résztvevők kényelmesen, akár otthonról is anonim módon kitölthették a kérdőívet. A nagy mintaszám miatt úgy gondoltam, hogy az online kérdőív esetében meg fogja könnyíteni az adatelemzést. Valamint napjainkban az online kérdőív igen népszerű, és mivel az okoseszköz használók körében végeztem a felmérést, ezért úgy gondoltam, hogy aki okoseszközt használ számára előnyösebb lesz az online kérdőív kitöltése.

4.5. Kutatási kérdések

A felmérés során az első kérdésnél a résztvevők kiválaszthatták, hogy melyik nemhez tartoznak (férfi/nő). A 6.táblázatban láthatjuk a felmérésben résztvevők válaszait nemek szerint Szerbiában, Magyarországon és Szlovákiában, melyben láthatjuk, hogy a felmérésben legtöbben Szerbiában vettek részt. Ha megnézzük, akkor láthatjuk, hogy országonként Szerbiában nemek szerint legtöbben a nők vettek részt 58,8%, Magyarországon pedig a férfiak 79,3%, Szlovákiában szintén a nők vettek legtöbben részt a felmérésben 57,6%.

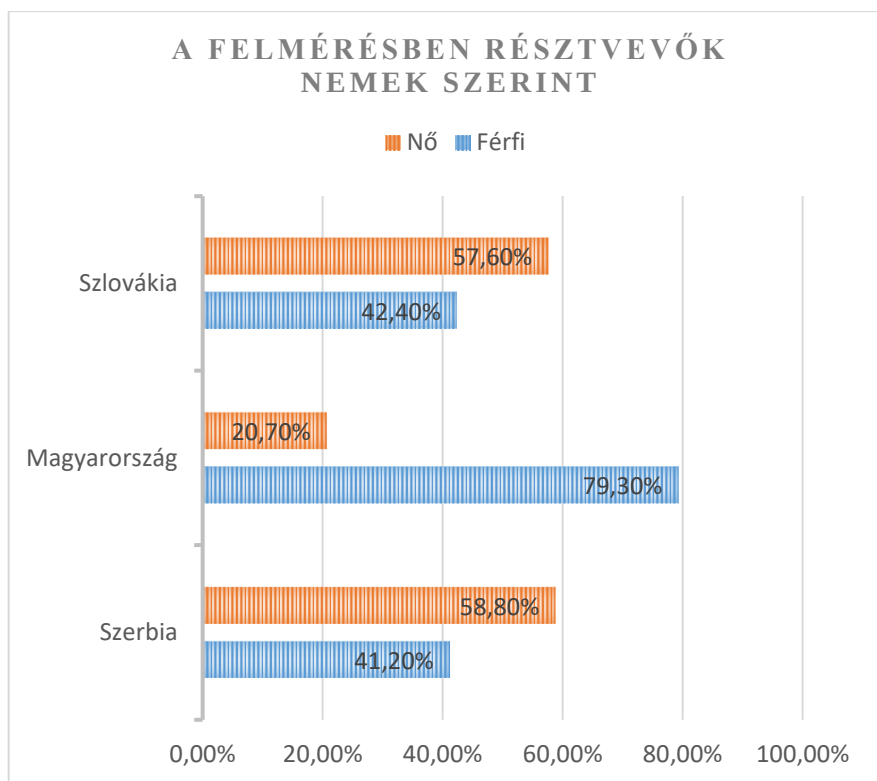
6. táblázat.A felmérésben résztvevők nemek szerint Szerbiában, Magyarországon és Szlovákiában.

Forrás: Saját szerkesztés

Nemek	Szerbia		Magyarország		Szlovákia	
	N	Százalék (%)	N	Százalék (%)	N	Százalék (%)
Férfi	113	41,2%	107	79,3%	25	42,4%
Nő	161	58,8%	28	20,7%	34	57,6%
Összesen	274	100%	135	100%	59	100%

Szerbiában a felmérésben összesen 274-en vettek részt, és ebből 113 férfi (41,2%), és 161 nő (58,8%) vett részt a kérdőív kitöltésében. Magyarországon a felmérésben összesen 135-en vettek részt, és ebből a férfiak közül 107-en vettek részt (79,3%), míg a nők 28-an (20,7%). Szlovákiában a felmérésben összesen 59-en vettek részt, és ebből 25 férfi (42,4%), és 34 nő (57,6%).

A 15. ábrán láthatjuk a felmérésben résztvevőket nemek szerint Szerbiában, Magyarországon és Szlovákiában diagramon ábrázolva. Láthatjuk, hogy Szerbiában és Szlovákiában legtöbben nők vettek részt a felmérésben, Magyarországon pedig a férfiak.



15. ábra. A felmérésben résztvevők nemek szerint. Forrás: Saját szerkesztés

A második kérdésnél a felmérésben résztvevők kiválaszhatták az életkorukat (18-24 éves, 25-34 éves, 35-50 éves, 51-60 éves és 60 felett). A 4.táblázatban láthatjuk a felmérésben résztvevők életkorát Szerbiában, Magyarországon és Szlovákiában a válaszok alapján.

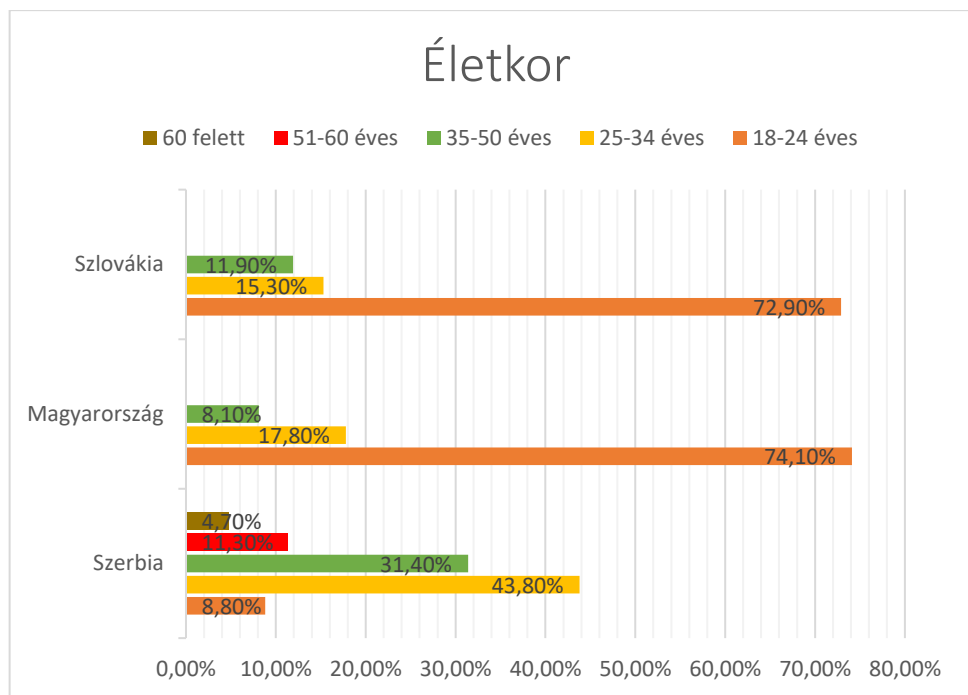
A 6. táblázatban láthatjuk a felmérésben résztvevők életkorát Szerbiában, Magyarországon és Szlovákiában. Szerbiában, akik részt vettek a felmérésben a korcsoport alapján legtöbben 25-34 évesek, Magyarországon legtöbben 18-24 évesek vettek részt, míg Szlovákiában szintén legtöbben a 18-24 évesek vettek részt a felmérésben.

6. táblázat. A felmérésben résztvevők életkora Szerbiában, Magyarországon és Szlovákiában. Forrás: Saját szerkesztés

Életkor	Szerbia		Magyarország		Szlovákia	
	N	Százalék (%)	N	Százalék (%)	N	Százalék (%)
18-24 éves	24	8,8%	100	74,1%	43	72,9%
25-34 éves	120	43,8%	24	17,8%	9	15,3%
35-50 éves	86	31,4%	11	8,1%	7	11,9%
51-60 éves	31	11,3%	0	0%	0	0%
60 felett	13	4,7%	0	0%	0	0%

Láthatjuk, hogy a felmérésben résztvevők életkora alapján Szerbiában a 18-24 éves korosztály közül 24-en (8,8%), 25-34 évesek közül 120-an választották (43,8%), 35-50 évesek közül 86-an (31,4%) vettek részt a felmérésben, az 51-60 éves korosztályból 31-en (11,3%), illetve a 60 feletti korosztályból 13-an (4,7%). Magyarországon a 18-24 éves korosztályból 89-en (78,1%), 25-34 éves korosztályból 19-en (16,7%), 35-50 évesek közül 6-an (5,3%), és az 51-60 éves korosztály, valamint a 60 feletti korosztály nem vett részt a felmérésben. Szlovákiában a 18-24 éves korosztály közül 43-an vettek részt (72,9%), és 25-34 évesek közül 15,3%, a 35-50 éves korosztályból pedig 11,9% vett részt a felmérésben.

A 16. ábrán láthatjuk a felmérésben résztvevők életkorát országonként diagramon is ábrázolva. Láthatjuk, hogy Szerbiában legtöbben a korcsoport szerint a 25-34 évesek vettek részt a felmérésben addig Magyarországon és Szlovákiában a 15-24 éves korcsoport.



16. ábra. A felmérésben résztvevők életkora Szerbiában, Magyarországon és Szlovákiában. Forrás: Saját szerkesztés

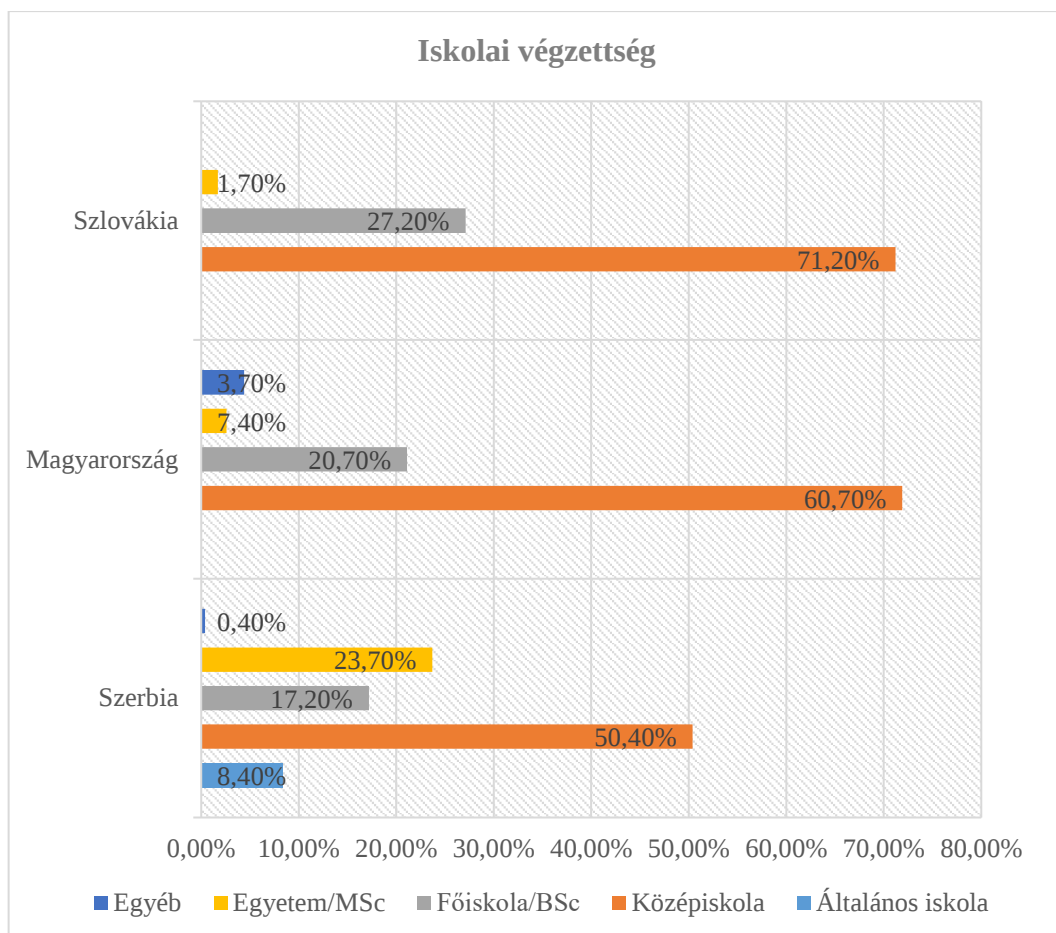
A harmadik kérdésnél a felmérésben résztvevők válaszolni tudtak, hogy mi a legmagasabb iskolai végzettségük. A következő lehetőségek közül tudtak választani: általános iskola, középiskola, főiskola, egyetem, valamint lehetőségük volt egyéb lehetőséget is kiválasztani.

A 7. táblázatban láthatjuk a felmérésben résztvevők iskolai végzettségét országoként. Láthatjuk, hogy mindhárom országban legtöbben középiskolai végzettséggel rendelkeznek, Szerbiában 50,4%, Magyarországon 60,7%, és Szlovákiában 71,2%.

7. táblázat. A felmérésben résztvevők iskolai végzettsége Szerbiában, Magyarországon és Szlovákiában. Forrás: Saját szerkesztés

Iskolai végzettség	Szerbia		Magyarország		Szlovákia	
	N	Százalék (%)	N	Százalék (%)	N	Százalék (%)
Általános iskola	23	8,4%	10	7,4%	0	0%
Középiskola	138	50,4%	82	60,7%	42	71,2%
Főiskola/BSc	47	17,2%	28	20,7%	16	27,1%
Egyetem/MSc	65	23,7%	10	7,4%	1	1,7%
Egyéb	1	0,4%	5	3,7%	0	0%

A 17. ábrán láthatjuk a felmérésben résztvevők iskolai végzettségét országonként diagramon is ábrázolva. Ami alapján megfigyelhető, hogy a felmérésben Szerbiában, Magyarországon és Szlovákiában is legtöbben középiskolai végzettséggel rendelkeznek.



17. ábra. A felmérésben résztvevők iskolai végzettségét országonként. Forrás: Saját szerkesztés

Láthatjuk, hogy a felmérésben résztvevők iskolai végzettsége Szerbiában 23-an választák (8,4%), hogy általános iskolával rendelkeznek, 138-an választák, hogy középiskolával rendelkeznek (50,4%), főiskolával 47-en (17,2%), egyetemmel 65-en (23,7%), valamint egyéb végzettséggel 1-en választak (0,4%). Magyarországon a felmérésben résztvevők közül 82-en választák (71,9%), hogy középiskolai végzettséggel rendelkeznek, 24-en (21,1%) választák, hogy főiskolai végzettséggel rendelkeznek, és 3-an (2,6%) választák, hogy egyetemi végzettséggel rendelkeznek, és 5-en (4,4%) választák, hogy egyéb végzettséggel rendelkeznek. Szlovákiában a felmérésben résztvevők közül 42-en (71,2%) választák, hogy általános iskolával rendelkeznek, 16-an (27,1%) választák, hogy főiskolai végzettséggel rendelkeznek, és 1 válaszadó (1,7%) válaszolta, hogy egyetemi végzettséggel rendelkezik. A 8. táblázatban látható, hogy a felmérésben résztvevők közül hányan választák országonként, hogy

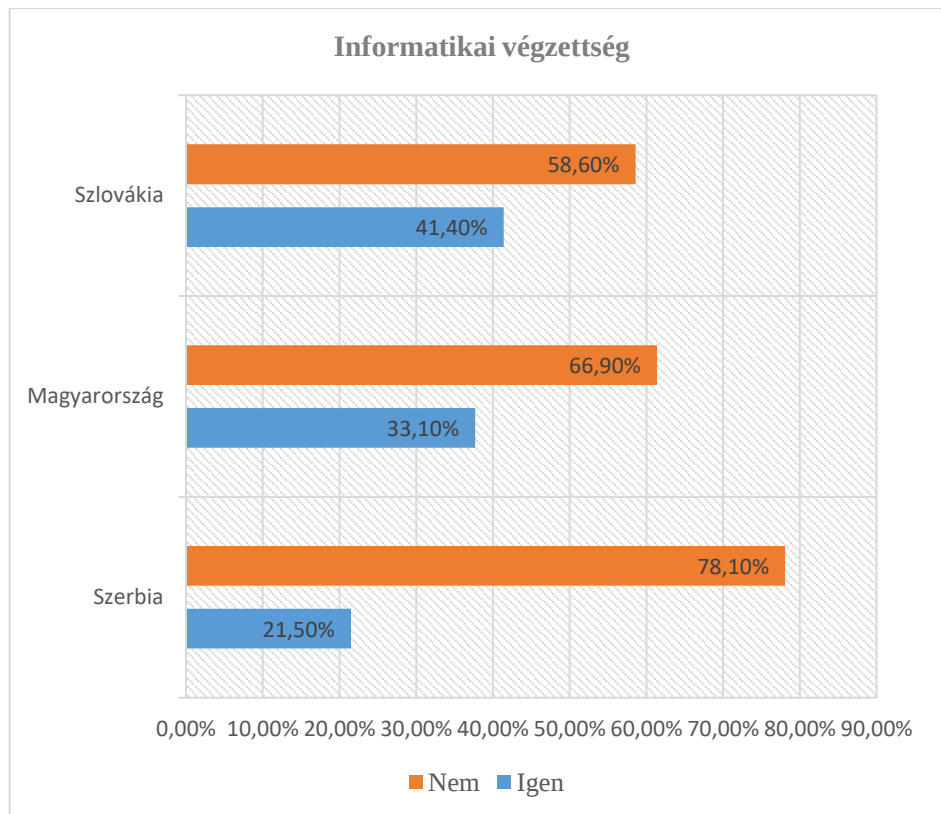
rendelkeznek informatikai végzettséggel. Láthatjuk, hogy legtöbben Szerbiában válaszolták, hogy nem rendelkeznek informatikai végzettséggel 78,1%, majd ezután Magyarországon 66,9%, és Szlovákiában 58,6%. Láthatjuk, hogy mind a három országban a résztvevők több mint fele nem rendelkezik informatikai végzettséggel.

8. táblázat. A felmérésben résztvevők informatikai végzettsége Szerbiában, Magyarországon és Szlovákiában. Forrás: Saját szerkesztés

Informatikai végzettség	Szerbia		Magyarország		Szlovákia	
	N	Százalék (%)	N	Százalék (%)	N	Százalék (%)
Igen	59	21,5%	44	33,1%	24	41,4%
Nem	214	78,1%	89	66,9%	34	58,6%

A 7. táblázatban láthatjuk, hogy Szerbiában a felmérésben résztvevők közül 59-en válaszolták (21,5%), hogy rendelkeznek informatikai végzettséggel, és 214-en (78,1%) válaszolták, hogy nem rendelkeznek. Magyarországon a felmérésben résztvevők közül 44-en válaszolták, hogy rendelkeznek informatikai végzettséggel (33,1%), és 89-en (66,9%) válaszolták, hogy nem rendelkeznek. Szlovákiában a felmérésben résztvevők közül 24-en (41,4%) válaszolták, hogy rendelkeznek informatikai végzettséggel, és 34-en (58,6%) válaszoltak nemmel.

A 18. ábrán látható, hogy a felmérésben résztvevők hányan válaszolták, hogy rendelkeznek informatikai végzettséggel diagramon ábrázolva. Megfigyelhetjük, hogy legtöbben Szerbiában válaszolták, hogy nem rendelkeznek informatikai végzettséggel, és legtöbben Szlovákiában válaszolták, hogy informatikai végzettséggel rendelkeznek.



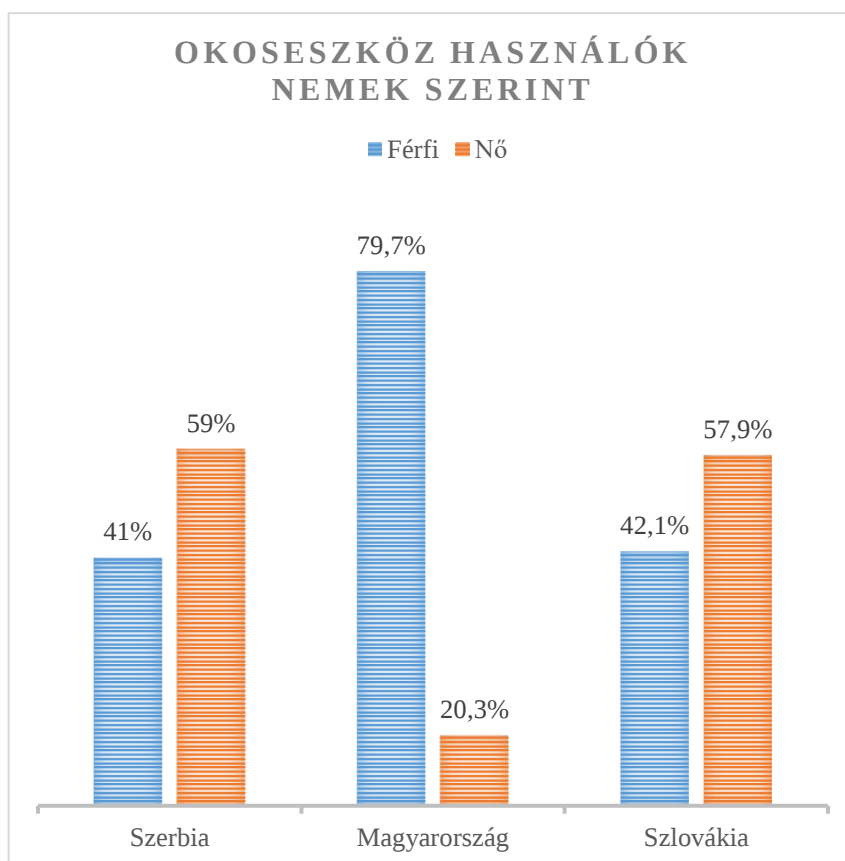
18. ábra. A felmérésben résztvevők informatikai végzettsége országoként. Forrás: Saját szerkesztés

A felmérésben fontos volt, hogy a résztvevők használnak-e okoseszközt, mivel a felmérés célja az okoseszköz használók körében történt. Ezért abban az esetben, ha valaki azt válaszolta, hogy mégsem használ okoseszközt, akkor a felmérés során felhívtam a figyelmet arra, hogy a következő kérdésekre ne válaszoljon, és lépjen tovább a kérdőívben, valamint, hogy válassza ki, hogy nem használ okoseszközt. Ennél a kérdésnél vizsgáltam, hogy hányan használnak okoseszközöket a felmérésben résztvevők közül. Valamint azt is vizsgáltam, hogy külön nemek szerint (férfi és nő) hányan használnak okoseszközöket. A 9. táblázatban látható, hogy a felmérésben résztvevők közül hányan használnak okoseszközöket nemek szerint Szerbiában, Magyarországon és Szlovákiában. Láthatjuk a válaszok alapján, hogy legtöbben Szerbiában a nők választották, hogy okoseszközöket használnak 59%-a, míg Magyarországon a férfiak 79,7%-a, és Szlovákiában szintén a nők választották legtöbben, hogy okoseszközöket használnak 57,9%.

9. táblázat. Az okoseszköz használók nemek szerint Szerbiában, Magyarországon és Szlovákiában a felmérés alapján. Forrás: Saját szerkesztés

Nemek	Szerbia		Magyarország		Szlovákia	
	N	Százalék (%)	N	Százalék (%)	N	Százalék (%)
Férfi	110	41%	106	79,7%	24	42,1%
Nő	158	59%	27	20,3%	33	57,9%
Összesen	268	100%	133	100%	57	100%

A 19. ábrán láthatjuk a felmérés alapján az okoseszköz használókat nemek szerint országonként. Láthatjuk, hogy Szerbiában és Szlovákiában legtöbben a nők választották, hogy okoseszközöket használnak, míg Magyarországon legtöbben a férfiak választották, hogy használnak okoseszközöket a felmérésben résztvevők közül.



19. ábra. Az okoseszköz használók nemek szerint Szerbiában, Magyarországon és Szlovákiában a felmérés alapján. Forrás: Saját szerkesztés

A válaszadók Szerbiában 97,8%-a válaszolta, hogy használ legalább egy okoseszközt, és mindössze 2,2%-a nem használ. Magyarországon a felmérésben résztvevők 98,5%-a válaszolta, hogy használnak okoseszközt, és 1,5%-a nem válaszolt erre a kérdésre.

Szlovákiában a válaszadók 96,6%-a válaszolta, hogy használnak okoseszközt, 1,7%-a válaszolta, hogy nem használ, míg 1,7% nem válaszolt erre a kérdésre. Láthatjuk, hogy Szerbiában, Magyarországon és Szlovákiában is a felmérésben résztvevők között az okoseszközhasználat igen magas. Szerbiában a férfiak közül 110-en (41%) válaszoltak, hogy használnak okoseszközt, míg a nők 158-an (59%). Magyarországon a férfiak közül 99-en (88,4%) válaszoltak, hogy használnak okoseszközt, míg a nők 13-an (11,6%). Szlovákiában a válaszadók közül a férfiak 24-en (42,1%), és a nők 33-an (57,9%) válaszoltak, hogy használnak okoseszközt.

A 10. táblázatban látható az okoseszközhasználók életkora Szerbiában, Magyarországon és Szlovákiában. Láthatjuk, hogy a válaszok alapján Szerbiában a legtöbben a 25-34 éves korcsoportból válaszolták, hogy okoseszközöket használnak 44%, míg Magyarországon a legtöbben a 18-24 éves korcsoportból 74,4%, és Szlovákiában szintén a 18-24 éves korcsoportból 73,7%.

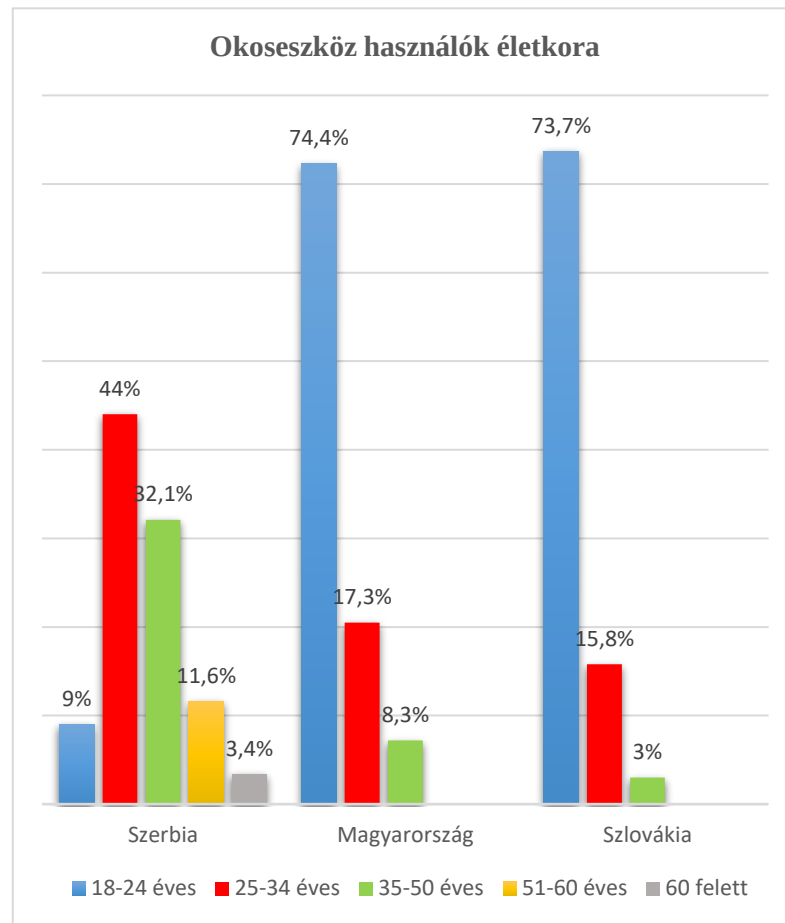
10. táblázat. Az okoseszköz használók életkora Szerbiában, Magyarországon és Szlovákiában a felmérés alapján. Forrás: Saját szerkesztés

Életkor	Szerbia		Magyarország		Szlovákia	
	N	Százalék (%)	N	Százalék (%)	N	Százalék (%)
18-24 éves	24	9%	99	74,4%	42	73,7%
25-34 éves	118	44%	23	17,3%	9	15,8%
35-50 éves	86	32%	11	8,3%	6	10,5%
51-60 éves	31	11,6%	0	0%	0	0%
60 felett	9	3,4%	0	0%	0	0%

A 10. táblázatban látható a felmérésben résztvevők közül hányan használnak okoseszközöket életkor szerint Szerbiában, Magyarországon és Szlovákiában. Szerbiában a felmérésben résztvevők válaszai alapján, akik azt válaszolták, hogy használnak okoseszközöket, ha megnézzük az életkor szerinti felosztást, akkor láthatjuk, hogy legtöbben a 25-34 éves korosztályból válaszoltak, hogy használnak okoseszközt, míg Magyarországon a felmérésben résztvevők válaszai alapján a 18-24 éves korosztályból. Szlovákiában szintén legtöbben a 18-24 éves korosztályból válaszoltak, hogy használnak okoseszközt.

A 20. ábrán láthatjuk az okoseszköz használók életkorát diagramon ábrázolva Szerbiában, Magyarországon és Szlovákiában. Láthatjuk, hogy Szerbiában legtöbben a 25-34 éves

korcsoportból használnak okoseszközöket, addig a felmérésben résztvevők válasza alapján Magyarországon és Szlovákiában a 15-24 éves korcsoportból.



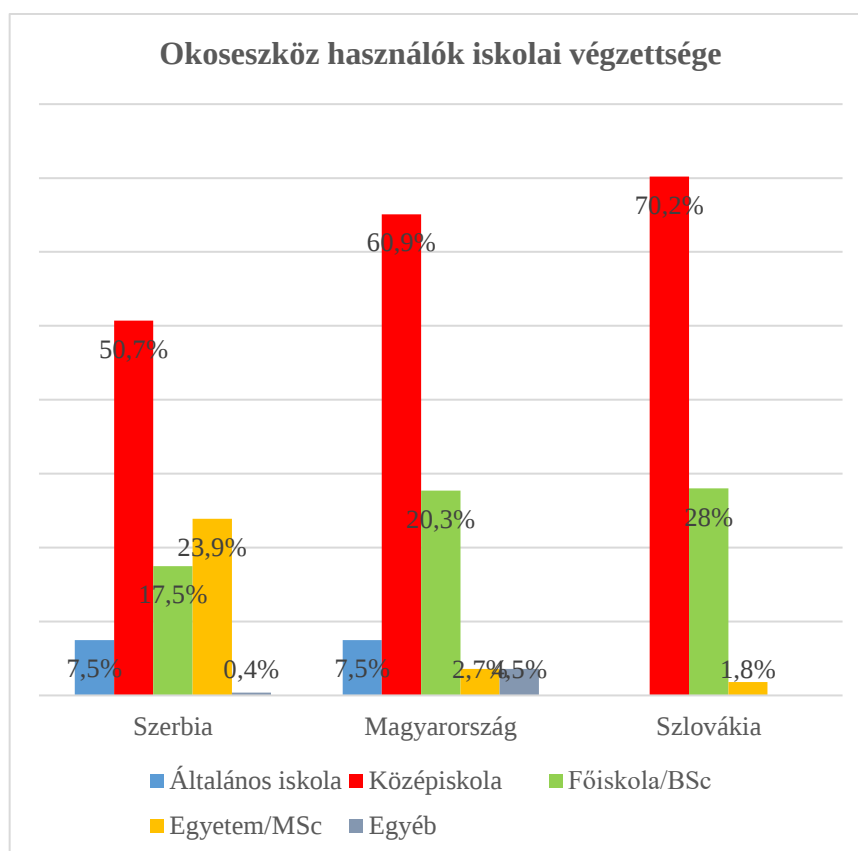
20. ábra. Az okoseszköz használók életkora Szerbiában, Magyarországon és Szlovákiában. Forrás: Saját szerkesztés

A 11. táblázatban láthatjuk az okoseszköz használók iskolai végzettségét a felmérés alapján Szerbiában, Magyarországon és Szlovákiában. Láthatjuk, hogy legtöbben az okoseszköz használók közül Szerbiában középiskolai végzettséggel rendelkeznek 50,7%, Magyarországon szintén a legtöbben középiskolai végzettséggel rendelkeznek 72,3%, és Szlovákiában 70,2%. Ami alapján elmondható, hogy mind a három országban legtöbben középiskolai végzettséggel rendelkeznek.

11. táblázat. Az okoseszköz használók iskolai végzettsége a felmérés alapján Szerbiában, Magyarországon és Szlovákiában. Forrás: Saját szerkesztés

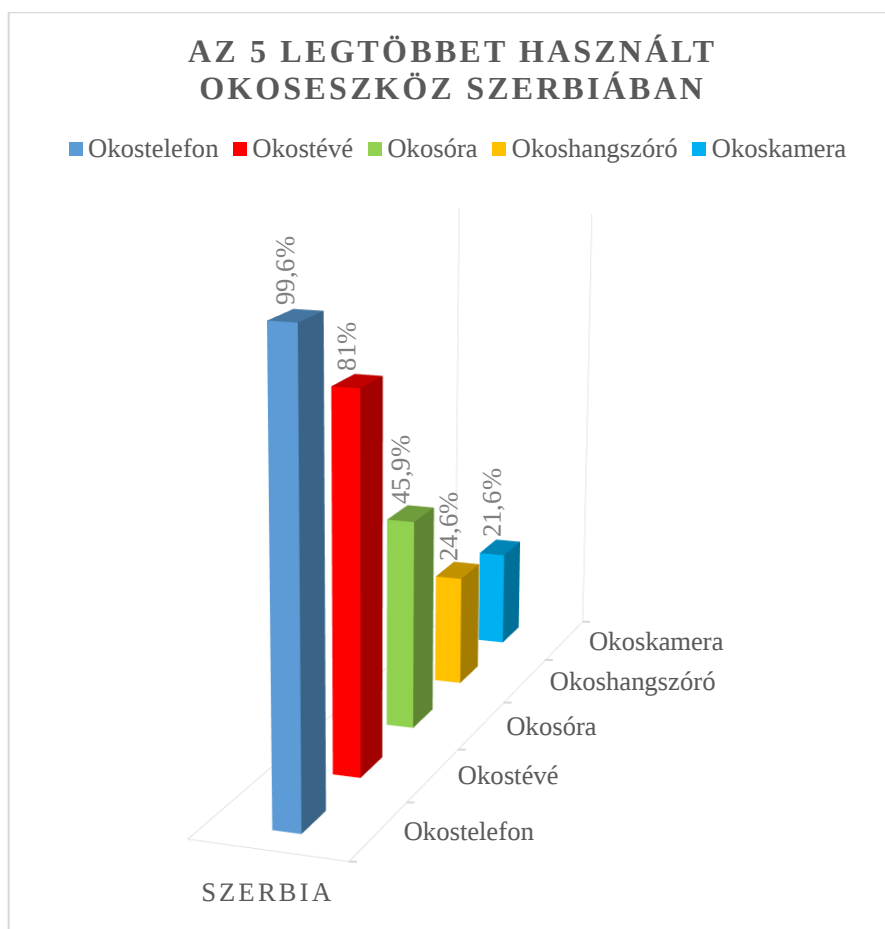
Iskolai végzettség	Szerbia		Magyarország		Szlovákia	
	N	Százalék (%)	N	Százalék (%)	N	Százalék (%)
Általános iskola	20	7,5%	10	7,5%	0	0%
Középiskola	136	50,7%	81	60,9%	40	70,2%
Főiskola/BSc	47	17,5%	27	20,3%	16	28%
Egyetem/MSc	64	23,9%	10	7,5%	1	1,8%
Egyéb	1	0,4%	5	3,8%	0	0%

A felmérésben résztvevők válaszai alapján, akik azt választották, hogy használnak okoseszközöket elmondhatjuk, hogy a többség középiskolai végzettséggel rendelkezik Szerbiában, Magyarországon és Szlovákiában. A 21. ábrán láthatjuk az okoseszköz használók iskolai végzettségét diagramon ábrázolva Szerbiában, Magyarországon és Szlovákiában. Láthatjuk, hogy mind a három országban legtöbben középiskolai végzettséggel rendelkeznek, akik okoseszközöket használnak.



21. ábra. Az okoseszköz használók iskolai végzettsége Szerbiában, Magyarországon és Szlovákiában. Forrás: Saját szerkesztés

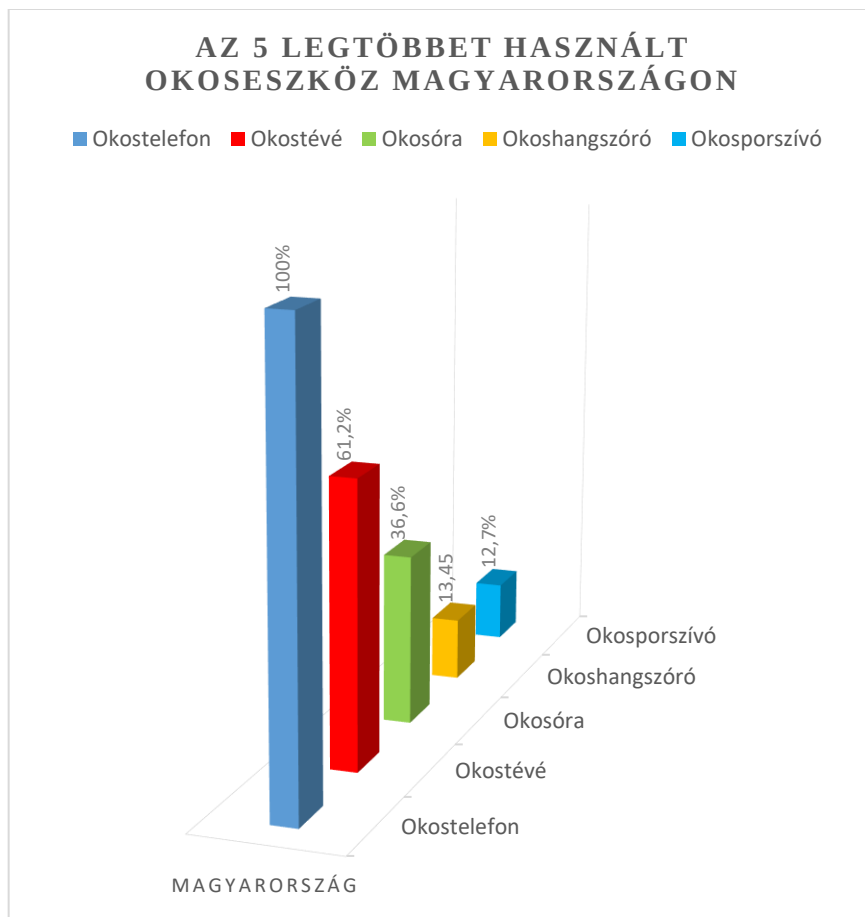
Úgy gondoltam, hogy fontos lenne a felmérésben azt is vizsgálni, hogy az okoseszköz használók milyen okoseszközökkel rendelkeznek. Ezért ennél a kérdésnél a felmérésben résztvevőknek lehetőségük volt több lehetőség közül választani, mint például az okostelefon, okosóra, okostévé, okosmérleg, okoshangszóró, okoscsengő, okoskamera, okosporszívó. De fontos volt, hogy lehetőség legyen egyénileg is leírni, hogy milyen okoseszközöket használnak abban az esetben, ha a felsoroltak közül esetleg nem használnak egyik okoseszközt sem. Ennél a kérdésnél a felmérésben résztvevők válaszai alapján az 5 legtöbbet használt okoseszközt fogom bemutatni országonként. A 22. ábrán láthatjuk az 5 legtöbbet használt okoseszközt a felmérés alapján Szerbiában. Láthatjuk, hogy Szerbiában a legtöbbet használt okoseszköz az okostelefon.



22. ábra. Az 5 legtöbbet használt okoseszköz a felmérés alapján Szerbiában.
Forrás: Saját szerkesztés

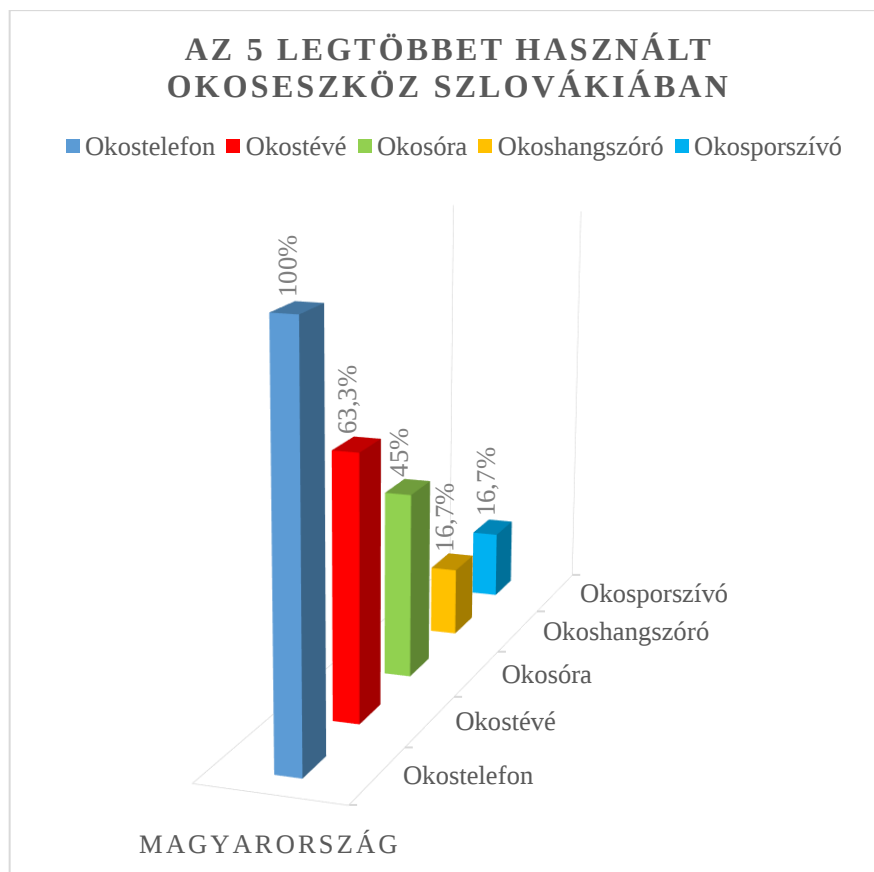
Szerbiában a válaszadók közül legtöbben azt választották, hogy okostelefont használnak (99,6%), így az okostelefon került az első helyre, majd ezt követi második helyen az okostévé (81%), a harmadik helyre az okosóra (45,9%), a negyedik helyre az okoshangszóró (24,6%), és az ötödik helyre pedig az okoskamera (21,6%).

A 23. ábrán látható az 5 legtöbbet használt okoseszközt a felmérés alapján Magyarországon. Láthatjuk, hogy Magyarországon a legtöbbet használt okoseszköz az okostelefon.



23. ábra. Az 5 legtöbbet használt okoseszköz a felmérés alapján Magyarországon. Forrás: Saját szerkesztés

Magyarországon a felmérésben résztvevők válaszai alapján szintén az okostelefon került az első helyre (100%), majd ezt követi az okostévé második helyen (61,4%), az okosóra a harmadik helyre került (39,5%), az okoshangszóró (14,9%) a negyedik helyre került, és az okosporszívó (12,3%) az ötödik helyre. A 24. ábrán láthatjuk az 5 legtöbbet használt okoseszközt a felmérés alapján Szlovákiában. Láthatjuk, hogy Szlovákiában a legtöbbet használt okoseszköz az okostelefon.



24. ábra. Az 5 legtöbbet használt okoseszköz a felmérés alapján Szlovákiában. Forrás: Saját szerkesztés

Láthatjuk, hogy a felmérésben résztvevők legtöbbször azt választották, hogy okostelefont használnak (100%) ezzel került az első helyre, majd ezt követi az okostévé második helyen (63,3%), és (45%) az okosóra harmadik helyen, (16,7%) az okoshangszóró a negyedik helyre került az okosporszívóval (16,7%). Láthatjuk, hogy a legtöbbet használt okoseszköz a felmérés alapján Szlovákiában az okostelefon.

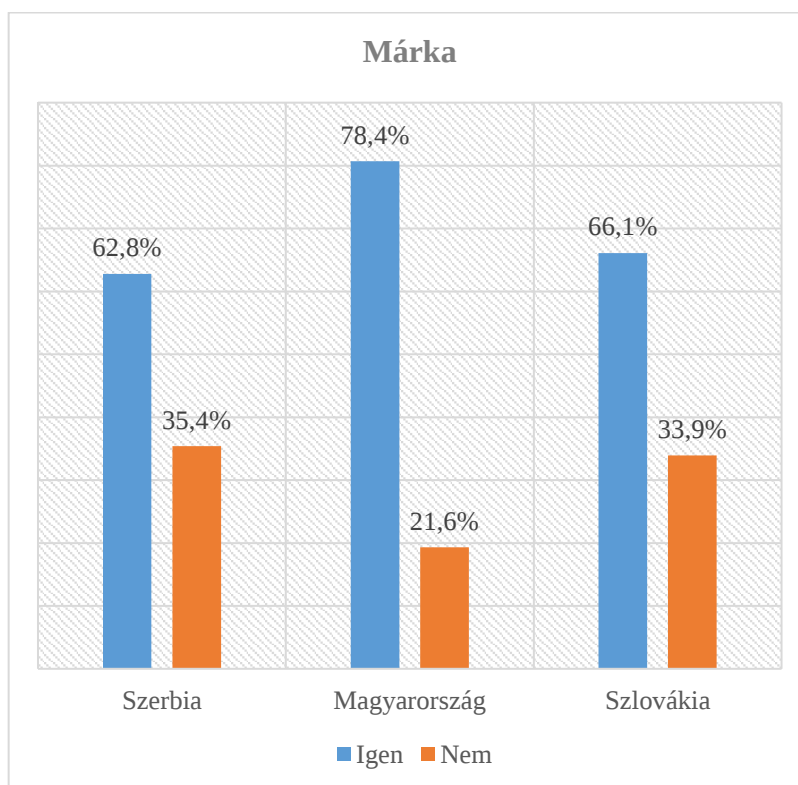
A környezetemben tapasztaltak alapján az okoseszköz használók közül vannak olyanok, akik számára fontos, hogy ismert márkát vásároljanak meg, ami megbízható, de vannak olyan okoseszköz használók, akik számára fontosabb, hogy a megvásárolt okoseszköz minél olcsóbb legyen és nem számít, hogy a márka ismert vagy sem lényeg, hogy minél olcsóbb legyen.

A 12. táblázatban láthatjuk, hogy a felmérésben résztvevők közül hányan választották, hogy fontos számukra az okoseszköz márkája Szerbiában, Magyarországon és Szlovákiában. Láthatjuk, hogy legtöbbször Magyarországon választották, hogy fontos számukra az okoseszköz márkája 78,4%, majd Szlovákiában 66,1%, és Szerbiában 62,8%.

12. táblázat Az okoseszköz márka fontossága Szerbiában, Magyarországon és Szlovákiában. Forrás: Saját szerkesztés

Márka	Szerbia		Magyarország		Szlovákia	
	N	Százalék (%)	N	Százalék (%)	N	Százalék (%)
Igen	172	62,8%	105	78,4%	39	66,1%
Nem	97	35,4%	29	21,6%	20	33,9%

A 25. ábrán látható, hogy a felmérésben résztvevők számára mennyire fontos az okoseszköz márkája Szerbiában, Magyarországon és Szlovákiában. Láthatjuk, hogy Magyarországon válaszolták a legtöbben 78,4%-kal, hogy fontos az okoseszköz márkája, és legkevesebben pedig Szerbiában 62,8%-kal válaszolták ezt.



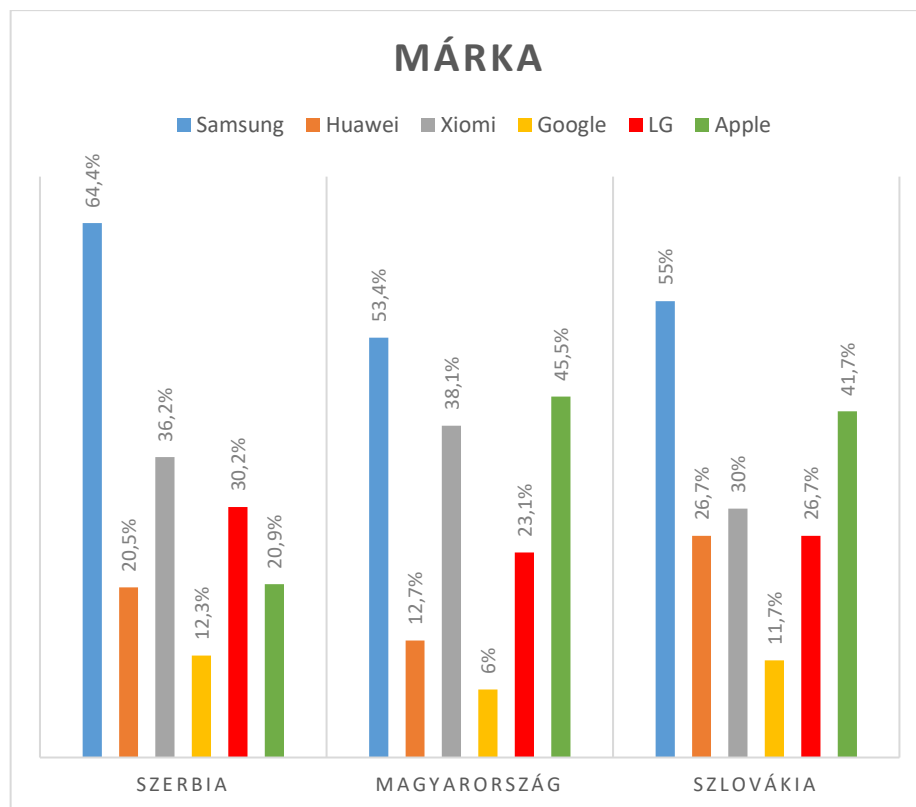
25. ábra. Az okoseszköz márka fontossága Szerbiában, Magyarországon és Szlovákiában. Forrás: Saját szerkesztés

Láthatjuk ezek alapján, hogy a márka fontossága Szerbiában 172-en (62,8%) válaszolták, hogy fontos számukra az okoseszköz márka, és 97-en (35,4%) válaszolták, hogy nem 5-en nem válaszoltak erre a kérdésre, ami (1,8%). Magyarországon 105-en (78,4%)

választották, hogy fontos számukra az okoseszköz márka, és 29-en (21,6%) választottak nemmel.

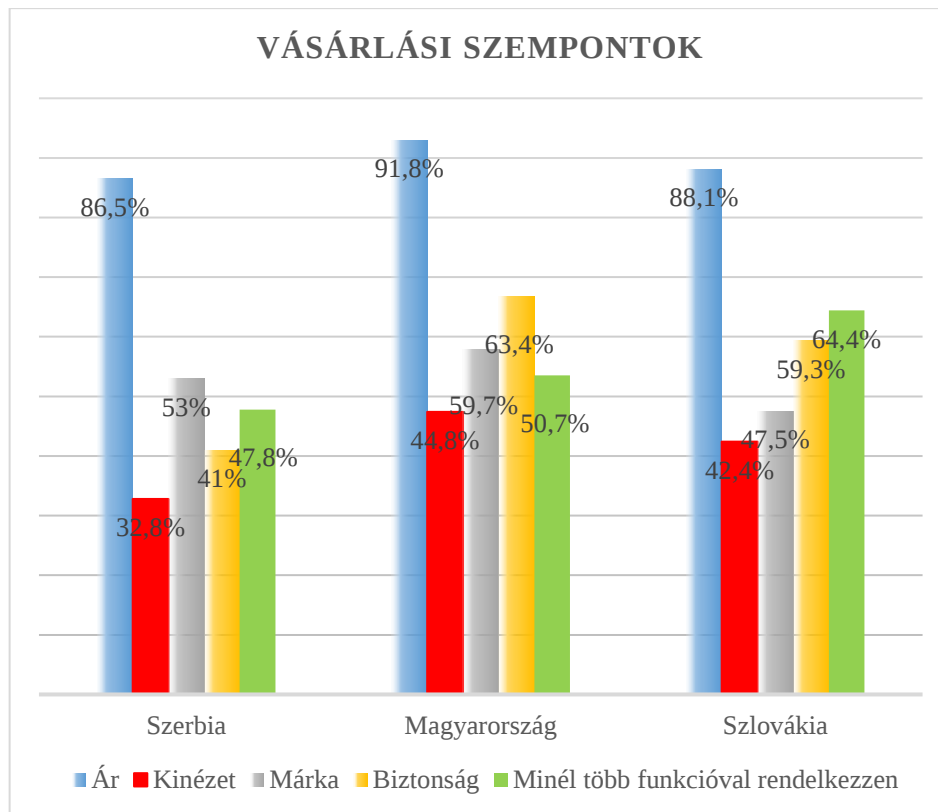
A felmérésben résztvevőknek lehetőségük volt több megadott márka közül választani. Mivel több okoseszköz márka nevét soroltam fel, amelyek közül a felmérésben résztvevők választani tudtak ezenkívül lehetőség volt egyéb márkát is megjelölni, és a saját véleményüket leírni a kérdésnél. Ezt a kérdést azért láttam fontosnak feltenni a kérdőívben, mert ezáltal láthatjuk azt is, hogy az okoseszköz márkák közül melyek azok a márkák, amelyeket a felhasználók legtöbbször használnak. A kérdőívben olyan okoseszköz márkákat jelöltem meg, melyek a napjainkban ismertebb márkák. Mivel több márkát is meg lehet adni, ezért úgy gondoltam, hogy a 6 legnépszerűbb márkát fogom bemutatni a felmérésben résztvevők válaszai alapján Szerbiában, Magyarországon és Szlovákiában.

A felmérés alapján Szerbiában az okoseszköz márkák közül legtöbbször azt választották, hogy az okoseszköz márkák közül a Samsungot (63,4%) használják, majd ezt követi a Xiaomi (36,2%), és az LG (30,2%), az Apple (20,9%), és a Google (12,3%). Magyarországon a megkérdezettek közül szintén legtöbbször azt választották, hogy a Samsung márkát használják legtöbbször (53,4%), majd ezt követi az Apple (45,5%), és a Xiaomi (38,1%), az LG (23,1%), és a Huawei (12,7%), végül a Google (6%). Szlovákiában a válaszadók legtöbbször a Samsung márkát használják (55%), majd ezt követi az Apple (41,7%), ezután az LG (26,7%), a Huawei (26,7%), majd pedig a Google (11,7%). A 26. ábrán láthatjuk a 6 legtöbbször használt márkát Szerbiában, Magyarországon és Szlovákiában a felmérés alapján. Láthatjuk, hogy Szerbiában legtöbbször a Samsung márkát használják 64,4%. Magyarországon 53,4%, és Szlovákiában szintén a legtöbbször azt választották, hogy a Samsung márkát használják 55%. A felmérés alapján elmondható, hogy mind a három országban a Samsung márkát használják legtöbbször.



26. ábra. A 6 legtöbbet használt okoseszköz márkája Szerbiában, Magyarországon és Szlovákiában a felmérés alapján. Forrás: Saját szerkesztés

Úgy gondoltam, hogy a kérdőívben fontos lenne feltenni egy olyan kérdést is, hogy milyen szempontok alapján döntenek el a felhasználók, hogy melyik okoseszközt vásárolják meg, mint például az ár, a kinézet, a márkák, a biztonság, és hogy minél több funkcióval rendelkezzen. Ezáltal betekintést kaphatunk az okoseszközhasználat vásárláskor, hogy milyen szempontokat vesznek figyelembe. A kérdésben több lehetséges szempontot adtam meg, amelyek közül tudtak választani, mint például az ár, kinézet, márkák, biztonság, minél több funkcióval rendelkezzen, és egyéb lehetőség. Ennél a kérdésnél is lehetőség volt a válaszadóknak saját véleményét írni. A 28. ábrán látható a legfontosabb vásárlási szempontok Szerbiában, Magyarországon és Szlovákiában a felmérés alapján diagramon ábrázolva. Megfigyelhetjük, hogy mind a három országban a legfontosabb szempont vásárláskor az ár. A felmérésben résztvevők közül Szerbiában 86,5%-a válaszolta az árat, Magyarországon 91,8%-a, és Szlovákiában 88,1%-a szintén az árat választotta.

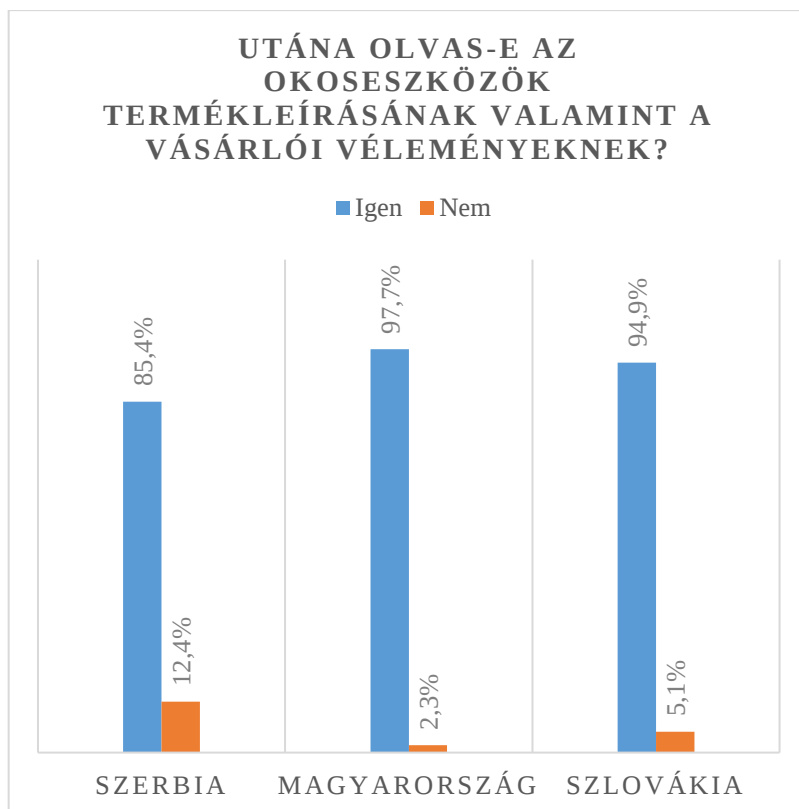


27. ábra. A legfontosabb vásárlási szempontok Szerbiában, Magyarországon és Szlovákiában a felmérés alapján. Forrás: Saját szerkesztés

A vásárlási szempontoknál a felmérésben résztvevőknek lehetőségük volt kiválasztani, hogy számukra, melyek a legfontosabb szempontok az okoseszköz vásárlásakor. A következő szempontok közül tudtak válaszolni: ár, kinézet, márka, biztonság, minél több funkcióval rendelkezzen az okoseszköz, de lehetőség volt több választ is megjelölni, illetve lehetőség volt egyéni választ is megadni. Szerbiában ez alapján a legfontosabb vásárlási szempont közé sorolták az árat, amely első helyre került 86,2%, majd ezt követi a márka második helyen 53%, és hogy minél több funkcióval rendelkezzen az okoseszköz harmadik helyre 47,8%. Majd a biztonság követi negyedik helyen 41%, és az ötödik helyre pedig a kinézet 32% került. A válaszadók emellett megemlítették, hogy számukra még fontos, hogy az okoseszköz használata egyszerű legyen és megbízható. Magyarországon a legfontosabb szempont vásárláskor szintén az ár került első helyre 91,8%, majd a biztonság a második helyre került 63,4%, a márka harmadik helyre 59,7%. Magyarországon a felmérésben résztvevők 50,7%-a szerint fontos, hogy minél több funkcióval rendelkezzen az okoseszköz a negyedik helyre került, majd a kinézet ötödik helyre 44,8%. A felmérésben résztvevők ezeken kívül megemlítették, hogy számukra fontos még a minőség, valamint a párosítási lehetőség. Szlovákiában a válaszadók 88,1%-

a azt válaszolta, hogy vásárláskor a legfontosabb szempont az ár, így első helyre került. Második helyre a minél több funkcióval rendelkező eszköz 64,4%-a, a harmadik helyre pedig a biztonság 59,3%-a, negyedik helyre a márka 47,5%-a, és az ötödik helyre a kinézet 42,4%-a került. Emellett megemlítették, hogy fontos számukra még a teljesítmény, illetve a szervíz lehetőség az országban. A felmérésben lehetőség volt a válaszadóknak több okoseszköz közül választani, hogy kiválasztják azokat az okoseszközöket, amelyeket használnak. A következő okoseszközök közül tudtak választani: okostelefon, okosóra, okostévé, okosmérleg, okoshangszóró, okoscsengő, okoskamera, okosporszívó vagy egyéb okoseszköz. Ez alapján Szerbiában a válaszadók közül legtöbben azt választották, hogy okostelefont használnak 99,6%-a, így az okostelefon került az első helyre, majd ezt követi második helyen az okostévé 81%-kal, és a harmadik helyre az okosóra került 45,9%-kal, a negyedik helyre az okoshangszóró 24,6%-kal, és az ötödik helyre pedig az okoskamera 21,6%-kal.

A felmérésben úgy gondoltam, hogy fontos lenne feltenni egy olyan kérdést is amire a felhasználók válaszolhatnak, hogy a megvásárolni kívánt okoseszköz termékleírásának, vagy a vásárlói véleményeknek utána szoktak-e olvasni. Ezt a kérdést azért gondoltam fontosnak, mert az eddigi irodalomkutatásaim alapján, és saját tapasztalataim szerint vannak olyan okoseszköz használók, akik nem szokták elolvasni az okoseszköz termékleírását, valamint a vásárlói véleményeket. Ennél a kérdésnél igen és nem válasszal lehetett válaszolni. A 28. ábrán látható a felmérésben résztvevők válaszai arról, hogy utána szoktak-e olvasni a megvásárolni kívánt okoseszköz termékleírásának, valamint a vásárlói véleményeknek Szerbiában, Magyarországon és Szlovákiában. Megfigyelhetjük, hogy mind a három országban a válaszadók magas számban választották, hogy utána olvasnak az okoseszközök termékleírásának és a vásárlói véleményeknek. Szerbiában a válaszadók 85,4%-a válaszolt igennel, Magyarországon 97,7%-a, és Szlovákiában 94,9%-a.



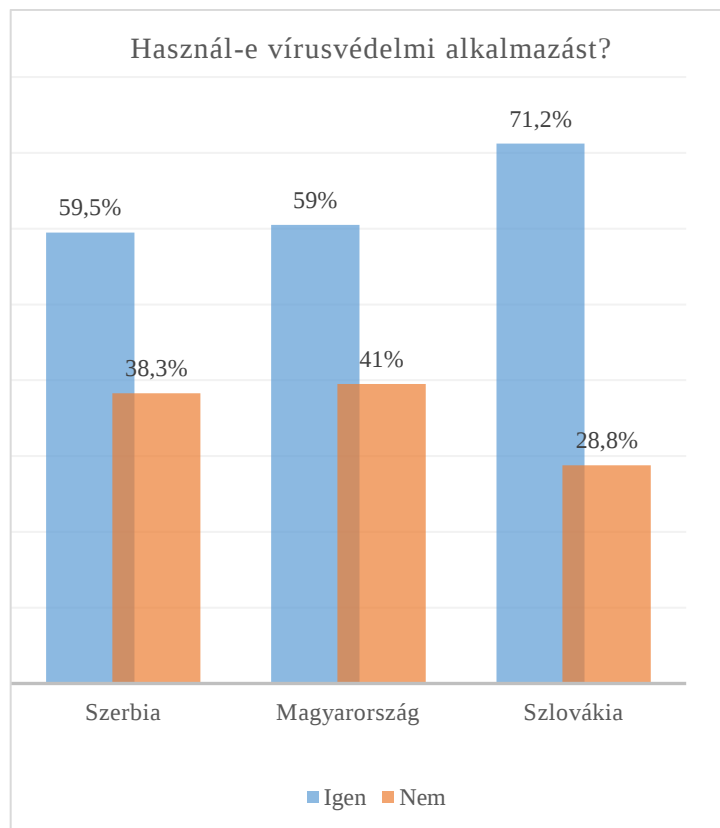
28. ábra. A felmérésben résztvevők válaszai arra vonatkoznak, hogy utána szoktak-e olvasni a megvásárolni kívánt okoseszköz termékleírásának és vásárlói véleményeknek Szerbiában, Magyarországon és Szlovákiában. Forrás: Saját szerkesztés

Láthatjuk, hogy Szerbiában a felmérésben résztvevők közül 234-en (85,4%) válaszoltak, hogy utána olvasnak a termékleírásnak, valamint a vásárlói véleményeknek amikor okoseszközt szeretnének vásárolni, és 34-en (12,4%) válaszoltak nemmel. Magyarországon a felmérésben résztvevők közül 130-an (97,7%) válaszoltak igennel, és mindössze csak 3-an (2,3%) válaszoltak nemmel. Ha megnézzük Szlovákiát, akkor láthatjuk, hogy 56-an (94,9%) igennel válaszoltak, és mindössze csak 3-an (5,1%) válaszoltak nemmel.

A felmérésben úgy gondoltam, hogy fontos lenne feltenni egy kérdést, hogy az okoseszközhasználók használnak-e vírusvédelmet. Az eddigi irodalomkutatás alapján, valamint a környezetemben tapasztaltak alapján, vannak olyan okoseszközhasználók, akik nem használnak vírusvédelmet.

A 29. ábrán látható a vírusvédelem használata Szerbiában, Magyarországon és Szlovákiában a felmérés alapján. Láthatjuk, hogy mindhárom országban a válaszadók több mint fele válaszolta, hogy használ vírusvédelmet. Szerbiában 59,5%-a,

Magyarországon 59%-a, és Szlovákiában 71,2%-a válaszolta, hogy használnak vírusvédelmet.

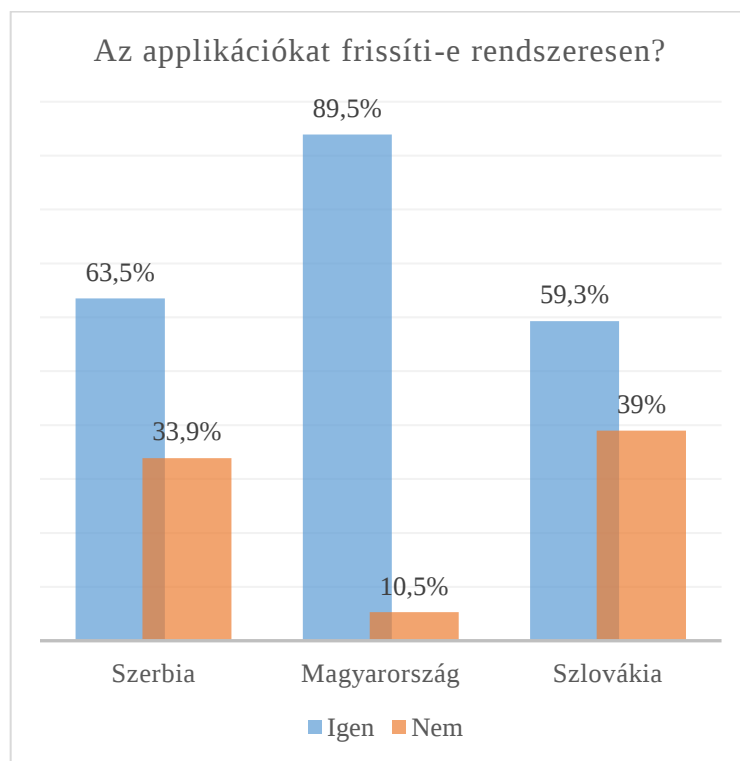


A 29. ábra láthatjuk a vírusvédelem használatát Szerbiában, Magyarországon és Szlovákiában a felmérés alapján. Forrás: Saját szerkesztés

A felmérésben résztvevők arra a kérdésre, hogy használnak-e vírusvédelmi alkalmazást Szerbiában, a válaszadók közül 163-an (59,5%) válaszolták, hogy használnak vírusvédelmi alkalmazást, és 105 válaszadó (38,3%) válaszolta, hogy nem használ. Magyarországon a válaszadók közül 79-en válaszolták, hogy használnak vírusvédelmet (59%), és 55-en nemmel válaszoltak (41%). Szlovákiában a válaszadók közül 42-en (71,2%) válaszolták, hogy használnak vírusvédelmet, és 17-en (28,8%) válaszolták, hogy nem használnak.

A felmérésben résztvevők válaszolhattak arra a kérdésre is, hogy az applikációkat frissítik-e rendszeresen. Ennél a kérdésnél a felmérésben résztvevők igen és nem válasszal tudtak válaszolni. Azért gondoltam fontosnak ezt a kérdést, mert a környezetemben tapasztaltak alapján, valamint az eddigi szakirodalmi áttekintések alapján nem minden felhasználó frissíti rendszeresen az applikációkat.

A 30. ábrán látható, hogy a felmérésben résztvevők közül hányan frissítik rendszeresen az applikációkat országoként. Láthatjuk, hogy Magyarországon válaszolták legtöbben, hogy az applikációkat rendszeresen frissítik 89,5%, majd Szerbiában 63,5%, és legkevesebben Szlovákiában válaszolták 59,3%, hogy rendszeresen frissítik az applikációkat.

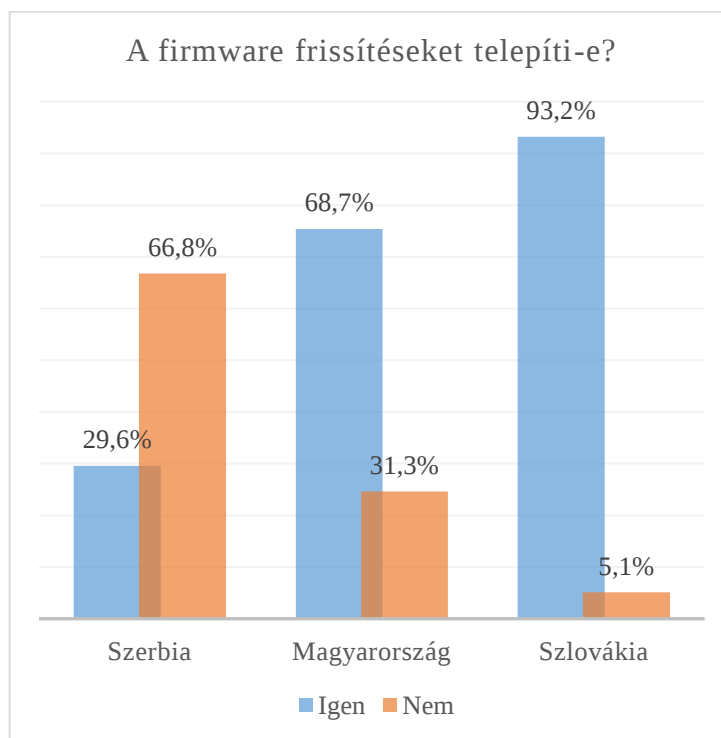


30. ábra. Az applikációk rendszeres frissítése Szerbiában, Magyarországon és Szlovákiában a felmérés alapján. Forrás: Saját szerkesztés

Arra a kérdésre, hogy az applikációkat frissítik-e rendszeresen a válaszadók közül Szerbiában 174-en (64,6%) válaszolták, hogy az applikációkat rendszeresen frissítik, és 93-an (33,9%) válaszoltak nemmel. Magyarországon a felmérésben résztvevők közül 119-en (89,5%) válaszolták, hogy az applikációkat rendszeresen frissítik, és 14-en (10,5%) válaszolták, hogy nem frissítik az applikációkat rendszeresen. Szlovákiában a felmérésben résztvevők közül 35-en (59,3%) válaszolták, hogy az applikációkat rendszeresen frissítik, és 23-an (39%) válaszoltak nemmel.

A felmérésnél a válaszadók válaszolhattak arra a kérdésre, hogy a firmware frissítéseket telepítik-e. Azért tettem fel ezt a kérdést, mert a környezetemben tapasztaltak alapján, valamint az irodalomkutatás során több helyen is találkoztam azzal, hogy az okoseszköz használók a firmware frissítéseket nem telepítik.

A 31. ábrán látható a felmérés alapján hányan választották, hogy a firmware frissítéseket telepítik Szerbiában, Magyarországon és Szlovákiában. Láthatjuk, hogy legtöbben Szlovákiában választották, hogy a firmware frissítéseket telepítik, Magyarországon pedig 68,7%-a választotta. Legkevesebben Szerbiában választották, hogy telepítik a firmware frissítéseket 29,6%.



31.ábra. A firmware frissítések telepítése a felmérés alapján Szerbiában, Magyarországon és Szlovákiában. Forrás: Saját szerkesztés

Szerbiában 81-en (29,9%) igennel választottak, és 183-an (66,8%) azt választották, hogy a firmware frissítéseket nem telepítik. Magyarországon a válaszadók közül 92-en (68,7%) választották, hogy telepítik a firmware frissítéseket, és 42-en (31,3%) választották, hogy nem telepítik. Szlovákiában a válaszadók 55-en (93,2%) választották, hogy a firmware frissítéseket telepítik, és 3-an (5,1%) választottak nemmel.

Az elkövetkező néhány kérdésnél a jelszóra vonatkozó kérdéseket tettem fel, mert a környezetemben tapasztaltak alapján, valamint a szakirodalmi áttekintések szerint a felhasználók sokszor nem használnak a jelszó esetében kis és nagybetűket, számokat, speciális karaktereket. Sokszor a jelszó személyes információkat tartalmaz például születési dátumot, értelmes szót, és sokszor a jelszót nem változtatják, illetve ugyanazt a jelszót több helyen is használják.

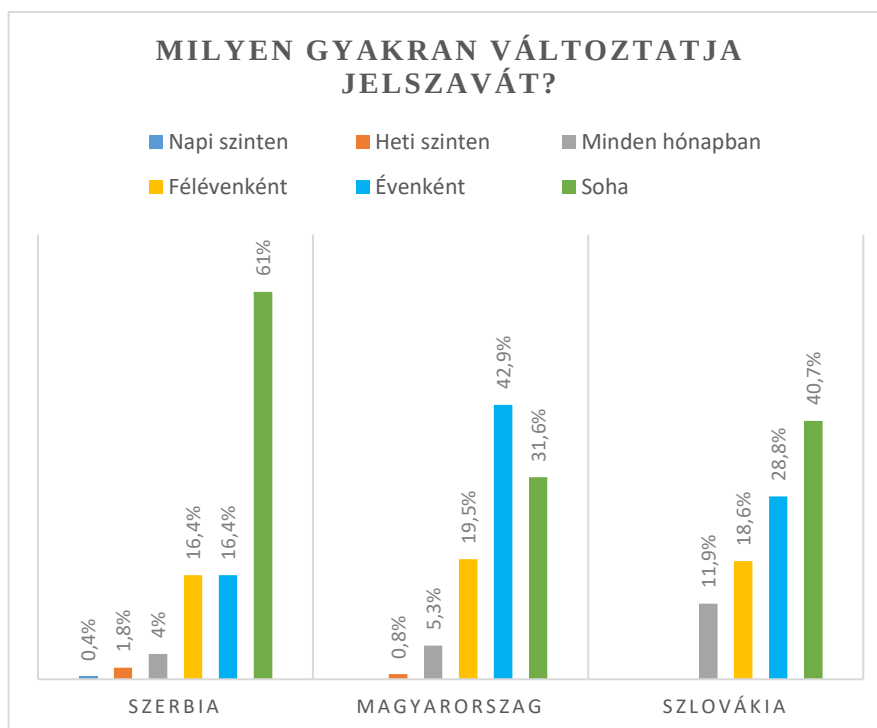
A 13. táblázatban látható, hogy a jelszót milyen gyakran változtatják a felmérés szerint Szerbiában, Magyarországon és Szlovákiában. Megfigyelhetjük, hogy Szerbiában a válaszadók 61%-a válaszolta, hogy a jelszót, amit használnak soha nem változtatják meg, míg Magyarországon a válaszadók 31,8%-a, addig Szlovákiában a válaszadók 40,7%-a. Láthatjuk, hogy Magyarországon a legkevesebben válaszolták azt, hogy a jelszót, amit használnak soha nem változtatják meg Szerbiához és Szlovákiához képest. Ezenkívül Magyarországon válaszolták legtöbben, hogy legalább félévenként 18,9%-a változtatja a jelszót, és 43,2%-a válaszolta, hogy legalább évente változtatja a jelszavát. A végső választ a statisztikai elemzés fogja megadni a következtetések helyességére vagy helytelenségére.

13. táblázat. A jelszóváltoztatás gyakorisága Szerbiában, Magyarországon és Szlovákiában a felmérés alapján. Forrás: Saját szerkesztés

Jelszó változtatás	Szerbia	Magyarország	Szlovákia
	Százalék (%)	Százalék (%)	Százalék (%)
Napi szinten	0,4%	0%	0%
Heti szinten	1,8%	0,8%	0%
Minden hónapban	4%	5,3%	11,9%
Félévenként	16,4%	18,9%	18,6%
Évenként	16,4%	43,2%	28,8%
Soha	61%	31,8%	40,7%

A 32. ábrán látható, hogy a felmérésben résztvevők milyen gyakran változtatják a jelszót, amit használnak országonként diagramon is ábrázolva. Láthatjuk, hogy Magyarországon válaszolták legkevesebben, hogy soha nem változtatják a jelszót Szerbiához és Szlovákiához képest. Ezenkívül, ha megnézzük a jelszó gyakoriságának a változtatását az országok között (Magyarország, Szerbia, Szlovákia). Elmondható, hogy Magyarország előnyben van Szerbiához és Szlovákiához képest, hiszen Magyarországon válaszolták a két országhoz képest a legkevesebben, hogy soha nem változtatják meg a jelszót. Ha megnézzük Magyarországon a legtöbben válaszolták, hogy félévenként (19,5%) és évenként (42,9%) változtatják a jelszót, addig Szerbiában félévenként (16,4%) és évenként (14,6%), ami kevesebb mint Magyarországon. Ha megnézzük Magyarországot és Szlovákiát, akkor láthatjuk, hogy Magyarország Szlovákiával szemben is előnyben van a jelszóváltoztatás gyakoriságánál, amikor a jelszót félévenként és évenként változtatják, mivel Szlovákiában 18,6% válaszolta, hogy a jelszót amit használnak félévenként változtatják illetve 28,8% válaszolta, hogy évenként változtatja,

ami kevesebb Magyarországhoz képest. A végső választ a statisztikai elemzés fogja megadni a következtetések helyességére vagy helytelenségére.

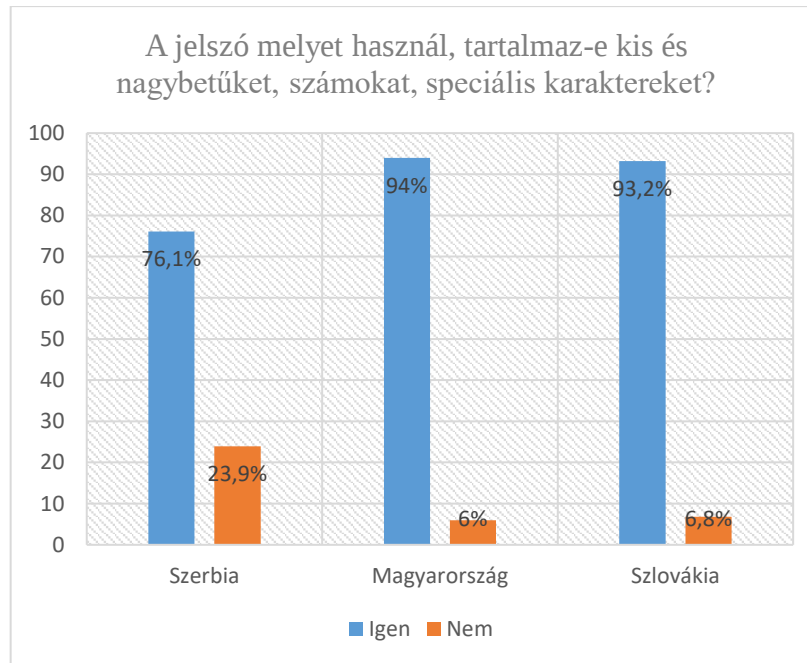


32. ábra. A jelszóváltoztatás gyakorisága Szerbiában, Magyarországon és Szlovákiában a felmérés alapján. Forrás: Saját szerkesztés

A felmérésben azt is vizsgáltam, hogy az okoseszközhaználóok milyen gyakran változtatják a jelszavakat. Ez azért volt fontos, mert az eddigi tapasztalataim alapján az okoseszközhaználóok közül sokan soha nem változtatják meg a jelszót, amit használnak. A felmérésben résztvevők válasza alapján Szerbiában a válaszadók 61%-a soha nem változtatja meg a jelszót, 16,4% évenként, 16,4% félévenként változtatja, 4% minden hónapban, 1,8% heti szinten, és 0,4% napi szinten. Magyarországon a válaszadók 31,6%-a soha nem változtatja a jelszót, 42,9% évenként változtatja, 19,5% félévenként, 5,3% minden hónapban, és 0,8% heti szinten. Szlovákiában a felmérésben résztvevők 11,9%-a minden hónapban változtatja a jelszót, 18,6% félévenként, 28,8% évenként, és 40,7% soha.

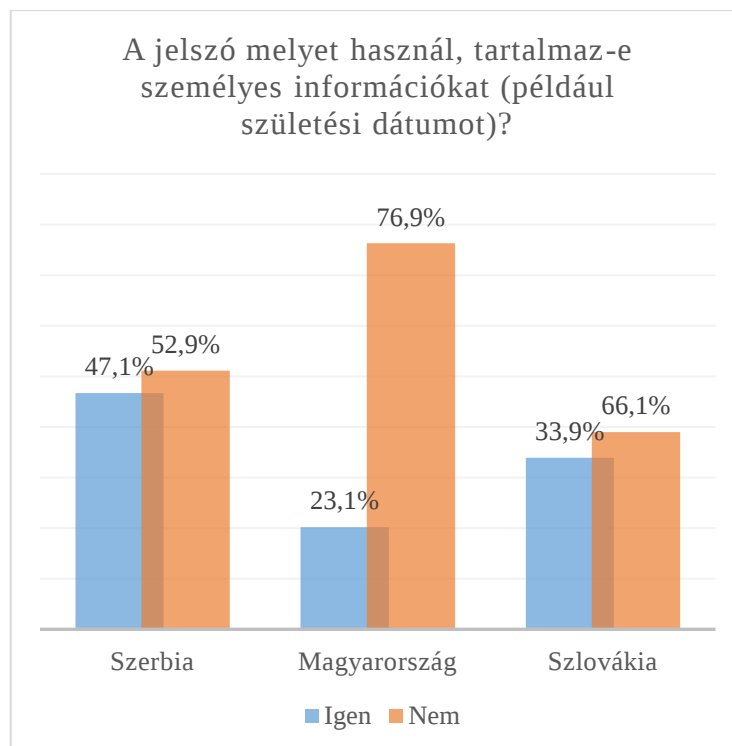
A 33. ábrán látható a felmérés alapján hányan válaszolták a jelszóhasználat esetében, hogy a jelszó tartalmaz kis és nagybetűket, számokat, speciális karaktereket Szerbiában, Magyarországon és Szlovákiában. Láthatjuk, hogy a jelszó, amely kis és nagybetűket, számokat és speciális karaktereket tartalmaz, legtöbbször Magyarországon használják 94%, Szerbiában 76,1%, és Szlovákiában 93,2%. Ami alapján elmondható, hogy

Magyarországon használnak Szerbiához és Szlovákiához képest legtöbben olyan jelszót, ami tartalmaz kis és nagybetűket, számokat és speciális karaktereket. A végső választ a statisztikai elemzés fogja megadni a következtetések helyességére vagy helytelenségére.



33. ábra. A felmérés alapján hányan használnak jelszót, ami tartalmaz kis és nagybetűket, számokat, speciális karaktereket Szerbiában, Magyarországon és Szlovákiában. Forrás: Saját szerkesztés

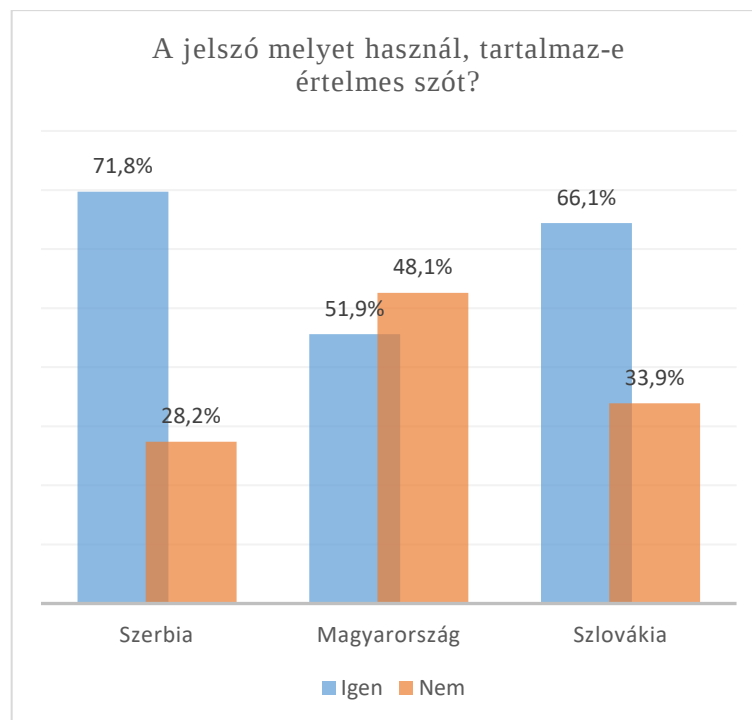
A 35. ábrán láthatjuk, hogy a felmérésben résztvevők a jelszóhasználat esetében használnak-e jelszónak személyes információkat, mint például a születési dátumot. Láthatjuk, hogy Magyarországon válaszolták legtöbben, hogy nem használnak személyes információkat tartalmazó jelszót 76,9%, addig Szerbiában 52,9% válaszolt igennel még Szlovákiában 66,1%. A végső választ a statisztikai elemzés fogja megadni a következtetések helyességére vagy helytelenségére.



34. ábra. A felmérés alapján a jelszóhasználat esetében, hogy a jelszó tartalmaz-e személyes információkat Szerbiában, Magyarországon és Szlovákiában. Forrás: Saját szerkesztés

Láthatjuk a felmérés alapján, hogy Szerbiában a felmérésben résztvevők közül 46,7% válaszolta, hogy a jelszó, amit használnak tartalmaz személyes információt, és csak 51,1% válaszolta, hogy nem tartalmaz. Magyarországon 22,9% válaszolta, hogy a jelszó, amit használnak tartalmaz értelmes szót, és 74,8% válaszolt nemmel. Szlovákiában 33,9% válaszolt igennel és 39% nemmel. A felhasználók általában olyan jelszavakat használnak, amelyeket könnyen meg tudnak jegyezni, ezért sokan használnak olyan jelszót, ami értelmes szót tartalmaz.

A 35. ábrán látható, hogy a felmérésben résztvevők közül hányan választották országonként, hogy a jelszó, amit használnak értelmes szót tartalmaz. Láthatjuk, hogy legtöbben Szerbiában használnak olyan jelszót, ami értelmes szót tartalmaz 71,8%, majd ezután Szlovákia 66,1%, és legkevesebben Magyarországon használnak olyan jelszót, ami értelmes szót tartalmaz. A végső választ a statisztikai elemzés fogja megadni a következtetések helyességére vagy helytelenségére.



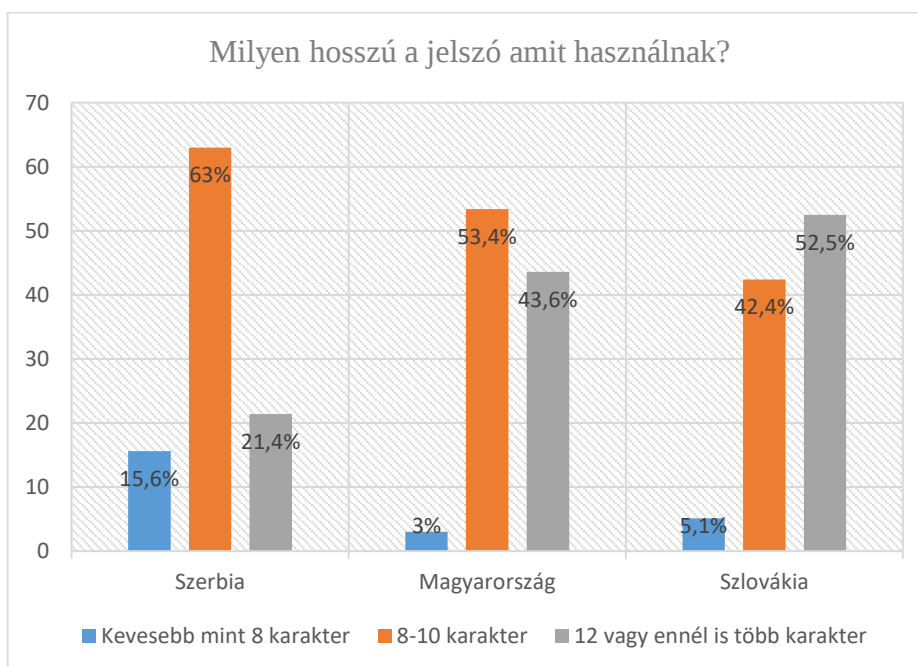
35. ábra. A felmérésben résztvevők a jelszóhasználatra vonatkozóan használnak-e értelmes szót. Forrás: Saját szerkesztés

Megfigyelhetjük, hogy a felmérésben résztvevők közül Szerbiában 71,8%-a válaszolta, hogy a jelszó, amit használtak értelmes szót tartalmaz, és 28,2% válaszolt nemmel. Magyarországon a felmérésben résztvevők 51,9%-a válaszolta, hogy a jelszó, amit használnak tartalmaz értelmes szót, és 48,1% válaszolt nemmel. Szlovákiában a felmérésben résztvevők 66,1%-a válaszolt igennel, hogy a jelszó, amit használnak értelmes szót tartalmaz, és 33,9% nemmel válaszoltak. A jelszóhasználat esetében a jelszó hossza vonatkozó kérdést azért gondoltam fontosnak, mert a felhasználók közül sokan kevesebb mint 8 karaktert használnak jelszónak a szakirodalmi áttekintések alapján, illetve a környezetemben tapasztaltak alapján. A 14. táblázatban látható a jelszó hosszának a használata a felmérés alapján Szerbiában, Magyarországon és Szlovákiában. Láthatjuk, hogy Szlovákiában használják legtöbbször a 12 vagy ennél is több karakterből álló jelszót 52,5%, majd Magyarországon 43,6%, és legkevesebben pedig Szerbiában 20,4%. A végső választ a statisztikai elemzés fogja megadni a következtetések helyességére vagy helytelenségére.

14. táblázat. A jelszó hossza a felmérés alapján Szerbiában, Magyarországon és Szlovákiában. Forrás: Saját szerkesztés

Jelszó hossza	Szerbia	Magyarország	Szlovákia
	Százalék (%)	Százalék (%)	Százalék (%)
Kevesebb mint 8 karakter.	15,6%	3%	5,1%
8-10 karakter.	63%	53,4%	42,4%
12 vagy ennél is több karakter.	21,4%	43,6%	52,5%

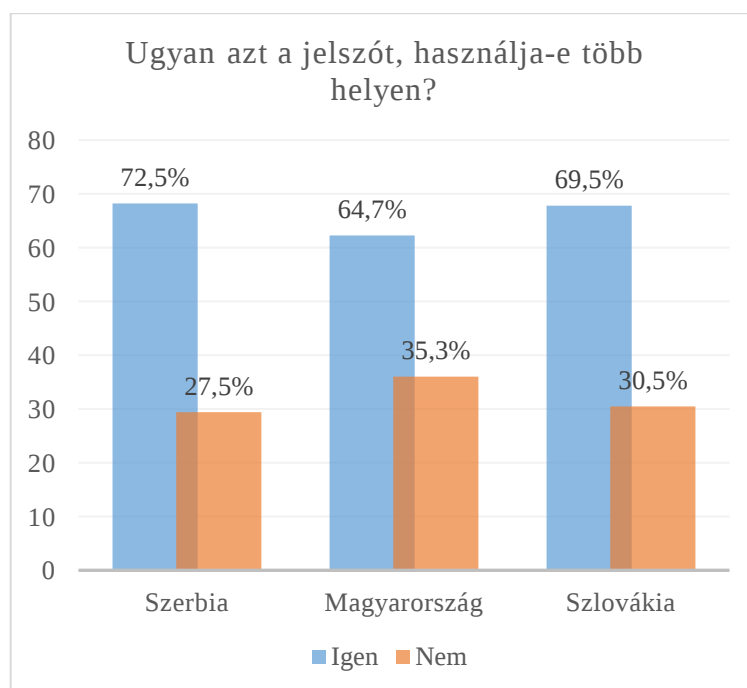
36. ábrán láthatjuk a jelszó hosszának a használatát a felmérés alapján Szerbiában, Magyarországon és Szlovákiában diagramon ábrázolva. Láthatjuk, hogy Szlovákiában használják legtöbbször 52,5%-a 12 vagy ennél is hosszabb jelszót, míg Magyarországon 43,6%-a, és Szerbiában 21,4%-a válaszolta, hogy 12 vagy ennél is hosszabb jelszót használnak. A végső választ a statisztikai elemzés fogja megadni a következtetések helyességére vagy helytelenségére.



36. ábra. A jelszó hosszának használata Szerbiában, Magyarországon és Szlovákiában a felmérés alapján. Forrás: Saját szerkesztés

A jelszóhasználat esetében vizsgáltam azt is, hogy milyen hosszú jelszavakat szoktak leggyakrabban használni. Ami alapján elmondhatjuk, hogy a felmérésben résztvevők Szerbiában 15,7%-a válaszolta, hogy kevesebb mint 8 karaktert használnak jelszónak, 62,1%-a válaszolta, hogy a jelszó, amit használnak 8-10 karakter, és 20,4%-a válaszolta,

hogy 12, vagy ennél is több karaktert tartalmazó jelszót használ. Magyarországon a felmérésben résztvevők 3%-a válaszolta, hogy kevesebb mint 8 karaktert tartalmaz a jelszó, amit használnak, 53,4%-a azt válaszolta, hogy 8-10 karaktert tartalmaz, és szintén 43,6%-a válaszolta, hogy a jelszó, amit használnak 12, vagy ennél is több karaktert tartalmaz. Szlovákiában a felmérésben résztvevők 45,8%-a válaszolta azt, hogy kevesebb mint 8 karaktert használnak jelszónak, és 52,2%-a válaszolta, hogy a jelszó, amit használnak 12 vagy ennél is több karaktert tartalmaz. A felhasználók közül vannak olyanok, akik ugyanazt a jelszót akár több helyen is használják. A 37. ábrán láthatjuk, hogy a felmérésben résztvevők közül hányan választák, hogy ugyanazt a jelszót használják több helyen. Láthatjuk, hogy Magyarországon választották legkevesebben, hogy ugyanazt a jelszót használják több helyen 64,7%, még legtöbben Szerbiában választották, hogy ugyanazt a jelszót több helyen használják 72,5%, majd Szlovákiában 67,8% választotta. A végső választ a statisztikai elemzés fogja megadni a következtetések helyességére vagy helytelenségére.

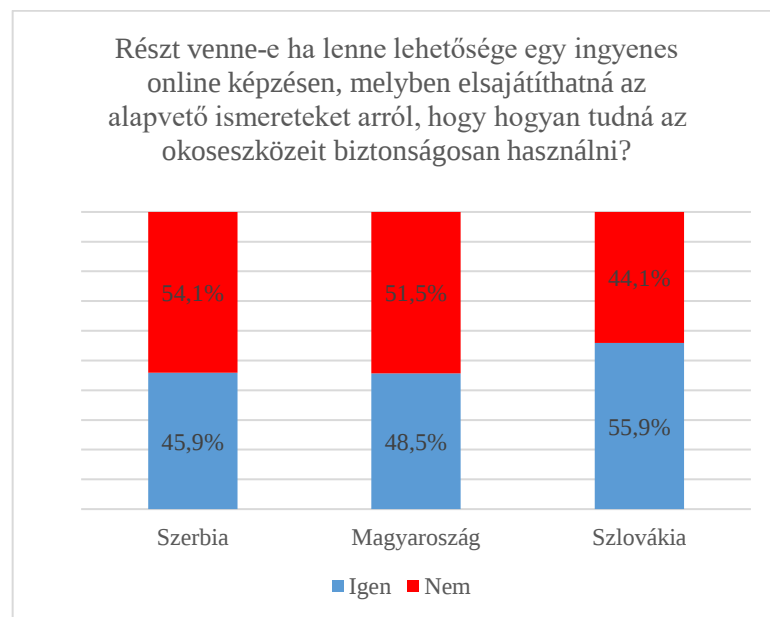


37. ábra. Ugyanaz a jelszó használata a felmérés szerint Szerbiában, Magyarországon és Szlovákiában.

Forrás: Saját szerkesztés

A felmérésben résztvevők közül Szerbiában 72,5%-a válaszolta, hogy ugyanazt a jelszót használja több helyen, míg 27,5% válaszolt nemmel. Magyarországon a felmérésben résztvevők 64,7%-a válaszolta, hogy ugyanazt a jelszót több helyen használja, míg 35,3% nemmel válaszolt. Szlovákiában a felmérésben résztvevők 69,5%-a válaszolt igennel, és

30,5% nemmel. A 38. ábrán láthatjuk, hogy a felmérésben résztvevők közül hányan vennének részt egy ingyenes online képzésen, melyben elsajátíthatnák az alapvető ismereteket arról, hogy hogyan tudnák az okoseszközeiket biztonságosan használni. Láthatjuk, hogy Magyarországon 48,5%, és Szerbiában 45,9% a felmérésben résztvevők közel fele válaszolta, hogy lenne igény egy ingyenes online képzésre, addig Szlovákiában a résztvevők több mint fele 55,9% igényt tartana egy ilyen képzésre.



A 38. ábra. A felmérés alapján a képzésen való részvétel szándéka Szerbiában, Magyarországon és Szlovákiában. Forrás: Saját szerkesztés

Szerbiában a felmérésben résztvevők válaszai alapján 45,9%-a azt válaszolta, hogy szeretnének részt venni egy ingyenes online képzésen, melyben elsajátíthatnák az alapvető ismereteket arról, hogy hogyan tudnák az okoseszközeiket biztonságosan használni, míg 54,1%-a azt válaszolta, hogy nem szeretnének részt venni egy ilyen képzésen. Magyarországon a válaszadók 48,5%-a azt válaszolta, hogy szeretnének részt venni, ha lenne rá lehetőség egy ilyen képzésen, addig 51,5%-a azt válaszolta, hogy nem vennének részt. Szlovákiában a felmérésben résztvevők 55,9%-a azt válaszolta, hogy részt vennének egy ilyen képzésen, addig 44,1%-a nemmel válaszolt.

4.6. Mann-Whitney U Teszt

A Mann-Whitney U-teszt egy statisztikai teszt, amelynek a meghatározására használják, hogy összehasonlítsunk két csoportot, hogy szignifikánsan különböznek-e egymástól. A Mann-Whitney U-teszt két csoport összehasonlítására használható. A Mann-Whitney U

teszt szignifikáns különbséget mutat, ha ($p < 0,05$) [125]. A 15. táblázatban láthatjuk a felmérésben résztvevők jelszóhasználati szokásait országonként.

15. táblázat. Jelszóhasználati szokások Magyarországon, Szerbiában és Szlovákiában. Forrás: Saját szerkesztés

Jelszóhasználati szokások	Magyarország	Szerbia	Szlovákia
	Százalék (%)	Százalék (%)	Százalék (%)
Jelszó tartalmaz kis és nagybetűket, számokat, speciális karaktereket.			
Igen	94%	76,1%	93,2%
Nem	6%	23,9%	6,8%
Jelszó személyes információkat tartalmaz.			
Igen	23,1%	47,1%	33,9%
Nem	76,9%	52,9%	66,1%
Jelszó értelmes szót tartalmaz.			
Igen	51,9%	71,8%	66,1%
Nem	48,1%	28,2%	33,9%
Ugyan azt a jelszót több helyen használja.			
Igen	64,7%	72,5%	69,5%
Nem	35,3%	27,5%	30,5%
A jelszó változtatás.			
Napi szinten.	0%	0,4%	0%
Heti szinten.	0,8%	1,8%	0%
Minden hónapban.	5,3%	4%	11,9%
Félévenként.	18,9%	16,4%	18,6%
Évenként.	43,2%	16,4%	28,8%
Soha.	31,8%	61%	40,7%
A jelszó hossza.			
Kevesebb mint 8 karakter.	3%	15,6%	5,1%
8-10 karakter.	53,4%	63%	42,4%
12 vagy ennél is több karakter.	43,6%	21,4%	52,5%

1. A jelszó amelyet használ, tartalmaz-e kis és nagybetűket, számokat, speciális karaktereket?

Magyarországon a felmérésben résztvevők 94%-a válaszolta azt, hogy az általuk használt jelszó kis és nagybetűket, számokat, speciális karaktereket tartalmaz, és mindössze 6% válaszolt nemmel. Addig Szerbiában a felmérésben résztvevők közül 76,1%-a válaszolta, hogy az általuk használt jelszó kis és nagybetűket, számokat, speciális karaktereket tartalmaz, és 23,9% nemmel válaszolt. Szlovákiában 93,2%-a válaszolta, hogy nagy és kisbetűket, számokat és speciális karaktereket tartalmazó jelszót használ, és 6,8% válaszolt nemmel.

2. A jelszó amelyet használ, tartalmaz-e személyes információkat (például születési dátumot)?

Magyarországon a válaszadók közül 23,1%-a válaszolta, hogy az általuk használt jelszó személyes információkat tartalmaz, míg 76,9% nemmel válaszolt. Szerbiában a válaszadók közül 47,1%-a válaszolta azt, hogy az általuk használt jelszó személyes információkat tartalmaz 52,9% pedig nemmel válaszolt. Szlovákiában 33,9%-a válaszolt igennel, és 66,1% nemmel válaszolt.

3. A jelszó amelyet használ, tartalmaz-e értelmes szót?

Magyarországon arra a kérdésre, hogy a jelszó tartalmaz-e értelmes szót a résztvevők 51,9%-a azt válaszolta, hogy az általuk használt jelszó értelmes szót tartalmaz, és 48,1% válaszolt nemmel. Szerbiában a válaszadók 71,8%-a azt válaszolta, hogy az általuk használt jelszó értelmes szót tartalmaz, és 28,2% válaszolta, hogy az általuk használt jelszó nem tartalmaz értelmes szót. Szlovákiában a válaszadók 66,1%-a válaszolt úgy, hogy értelmes szót tartalmazó jelszót használnak, és 33,9% nemmel válaszolt.

4. Ugyanazt a jelszót használja-e több helyen?

Magyarországon a válaszadók 64,7%-a ugyanazt a jelszót használja több helyen, míg 35,3% azt válaszolta, hogy nem használja ugyanazt a jelszót több helyen. Szerbiában a válaszadók 72,5%-a válaszolta, hogy ugyanazt a jelszót több helyen használják, és 27,5%-a válaszolt nemmel. Szlovákiában a felmérésben a válaszadók 69,5%-a válaszolt

igennel arra a kérdésre, hogy használják-e több helyen ugyanazt a jelszót, és 30,5% pedig azt válaszolta, hogy nem használják ugyanazt a jelszót több helyen.

5. Milyen gyakran változtatja jelszavát?

Magyarországon a válaszadók 31,8%-a válaszolta, hogy soha nem változtatják meg a jelszót, 43,2% évente, 18,9% félévenként, 5,3%, havonta, 0,8% pedig hetente változtatja a jelszót. Szerbiában a felmérésben résztvevők válaszai alapján a válaszadók 61%-a soha nem változtatja meg a jelszót, 16,4% évente, 16,4% félévenként, 4% havonta, 1,8% válaszolta, hogy heti rendszerességgel, és 0,4% válaszolta, hogy naponta változtatja a jelszavát. Szlovákiában a felmérésben résztvevők 11,9%-a válaszolta, hogy havonta változtatja meg a jelszót, 18,6% félévenként, 28,8% évente, 40,7% pedig azt válaszolta, hogy soha nem változtatja meg az általuk használt jelszót.

6. Milyen hosszú a jelszó, amit használ?

Magyarországon a felmérésben résztvevők 3%-a azt válaszolta, hogy az általuk használt jelszó 8 karakternél rövidebb, 53,4% válaszolta, hogy 8-10 karakterből áll, és 43,6% válaszolta, hogy az általuk használt jelszó 12, vagy ennél is több karakterből áll. Szerbiában a résztvevők 15,6%-a válaszolta, hogy 8 karakternél kevesebb karaktert használnak jelszónak, 63% válaszolta, hogy az általuk használt jelszó 8-10 karakterből áll, és 21,4% válaszolta, hogy az általuk használt jelszó 12, vagy több karaktert tartalmaz. Szlovákiában 5,1%-a válaszolta, hogy a jelszó 8 karakternél kevesebb karaktert tartalmaz, és 42,4% válaszolta, hogy 8-10 karaktert tartalmazó jelszót használnak, és 52,5% válaszolt, hogy az általuk használt jelszó 12, vagy ennél is több karakterből áll. A 16. táblázatban láthatjuk az okoseszköz használók jelszóhasználati szokásait Magyarországon leíró statisztikával.

16. táblázat. Az okoseszköz használók jelszóhasználati szokásai Magyarországon leíró statisztikával.

Forrás: Saját szerkesztés

Jelszóhasználati szokások leíró statisztikával	N	Sum	Átlag	Std. Szórás
Jelszó tartalmaz kis és nagybetűket, számokat, speciális karaktert.	133	141	1,06	0,239
Jelszó személyes információkat tartalmaz.	131	232	1,77	0,422
Jelszó értelmes szót tartalmaz.	133	197	1,48	0,502
Ugyan azt a jelszót több helyen használja.	133	180	1,35	0,480
A jelszó változtatás.	133	664	4,99	0,892
A jelszó hossza.	133	320	2,41	0,551

A 17. táblázatban láthatjuk az okoseszköz használók jelszóhasználati szokásait Szerbiában leíró statisztikával.

17. Az okoseszköz használók jelszóhasználati szokásai Szerbiában leíró statisztikával. Forrás: Saját szerkesztés

Jelszóhasználati szokások leíró statisztikával	N	Sum	Átlag	Std. Szórás
Jelszó tartalmaz kis és nagybetűket, számokat, speciális karaktert.	267	333	1,25	0,432
Jelszó személyes információkat tartalmaz.	268	408	1,52	0,500
Jelszó értelmes szót tartalmaz.	264	338	1,28	0,450
Ugyan azt a jelszót több helyen használja.	267	345	1,29	0,456
A jelszó változtatás.	269	1489	5,54	1,220
A jelszó hossza.	267	548	2,05	0,605

A 18. táblázatban láthatjuk az okoseszköz használók jelszóhasználati szokásait Szlovákiában leíró statisztikával.

18. táblázat. Az okoseszköz használók jelszóhasználati szokásai Szlovákiában leíró statisztikával. Forrás:

Saját szerkesztés

Jelszóhasználati szokások leíró statisztikával	N	Sum	Átlag	Std. Szórás
Jelszó tartalmaz kis és nagybetűket, számokat, speciális karaktert.	58	81	1,40	0,493
Jelszó személyes információkat tartalmaz.	58	96	1,66	0,479
Jelszó értelmes szót tartalmaz.	58	78	1,34	0,479
Ugyan azt a jelszót több helyen használja.	58	76	1,31	0,467
A jelszó változtatás.	58	288	4,97	1,042
A jelszó hossza.	58	120	2,07	1,006

A 19. táblázatban láthatjuk Magyarországon és Szerbiában van-e különbség a jelszóhasználat esetében.

19. táblázat: Jelszóhasználat Magyarországon és Szerbiában Mann-Whitney U teszt. Forrás: Saját szerkesztés

Mann-Whitney U teszt	p
A jelszó tartalmaz kis és nagybetűket, számokat, speciális karaktereket.	0,003
A jelszó személyes információkat tartalmaz.	0,545
A jelszó értelmes szót tartalmaz.	0,002
Ugyan azt a jelszót több helyen használja.	0,963
A jelszó változtatás.	0,837
A jelszó hossza.	0,910

A jelszóhasználat esetében, amikor a jelszó tartalmát nézzük, hogy a jelszó kis és nagybetűket, számokat és speciális karaktereket használnak, valamint értelmes szót tartalmaz szignifikáns különbség van. Láthatjuk, hogy a jelszóhasználat esetében, amikor a jelszó tartalmát nézzük meg, hogy a válaszadók Magyarországon szignifikánsan összetettebb jelszavakat használnak a jelszó tartalmát illetően, mely így biztonságosabb azonos hosszúság esetén a brute force támadáskor. Az értelmes szót tartalmazó jelszó esetében pedig elmondható, hogy Szerbiában szignifikánsan többen használnak olyan jelszót, ami értelmes szót tartalmaz. Láthatjuk, hogy nincs szignifikáns különbség a személyes információkat tartalmazó jelszó, a jelszó hossza és a jelszóváltoztatás gyakorisága között, valamint ugyanaz a jelszó használata esetében amikor több helyen

használják. A személyes információkat tartalmazó jelszó esetében az okoseszköz használók Magyarországon és Szerbiában is ugyanúgy sok helyen használnak személyes információkat tartalmazó jelszavakat. Láthatjuk, hogy ugyanaz a jelszó használata több helyen esetében az okoseszköz használók Magyarországon és Szerbiában ugyanúgy több helyen használják ugyanazt a jelszót. A jelszóváltoztatás esetében Magyarországon és Szerbiában is az okoseszköz használók ugyanolyan ritkán változtatják meg a jelszót. A jelszó hossza esetében pedig látható, hogy mindkét országban ugyanúgy kevesen használnak 12 vagy ennél is több karaktert tartalmazó jelszót.

A 20. táblázatban láthatjuk Magyarországon és Szlovákiában van-e különbség a jelszóhasználati szokások között.

20. táblázat: Jelszóhasználat Magyarországon és Szlovákiában Mann-Whitney U teszt. Forrás: Saját szerkesztés

Mann-Whitney U teszt	p
A jelszó tartalmaz kis és nagybetűket, számokat, speciális karaktereket.	0,003
A jelszó személyes információkat tartalmaz.	0,002
A jelszó értelmes szót tartalmaz.	0,002
Ugyan azt a jelszót több helyen használja.	0,963
A jelszó változtatás.	0,837
A jelszó hossza.	0,910

A jelszóhasználat esetében, amikor a jelszó tartalmát nézzük, hogy a jelszó kis és nagybetűket, számokat és speciális karaktereket használnak, valamint személyes információt és értelmes szót jelszónak szignifikáns különbség van. Láthatjuk a jelszóhasználat esetében, amikor a jelszó tartalmát nézzük meg, hogy az okoseszköz használók Magyarországon szignifikánsan összetettebb jelszavakat használnak a jelszó tartalmát illetően, mely így biztonságosabb azonos hosszúság esetén a brute force támadáskor. Láthatjuk, hogy Szlovákiában szignifikánsan többen használnak olyan jelszót, ami személyes információkat és értelmes szót tartalmaz. Láthatjuk, hogy nincs szignifikáns különbség a jelszó hossza és a jelszóváltoztatás gyakorisága között, valamint ugyanaz a jelszó használata esetében, amikor több helyen használják ugyanazt a jelszót. Láthatjuk, hogy ugyanaz a jelszó használata esetében több helyen az okoseszköz használók Magyarországon és Szlovákiában is ugyanúgy több helyen használják

ugyanazt a jelszót. A jelszóváltoztatás esetében pedig Magyarországon és Szlovákiában is az okoseszköz használók ugyanúgy ritkán változtatják meg a jelszót, amit használnak. A jelszó hossza esetében pedig látható, hogy mindkét országban ugyanannyian kevesen használnak 12 vagy ennél is több karaktert tartalmazó jelszót.

A 21. táblázatban láthatjuk, hogy Szerbia és Szlovákia jelszóhasználati szokásai között van-e különbség.

21. táblázat: Jelszóhasználat Szerbiában és Szlovákiában Mann-Whitney U teszt. Forrás: Saját szerkesztés

Mann-Whitney U teszt	p
A jelszó tartalmaz kis és nagybetűket, számokat, speciális karaktereket.	0,008
A jelszó személyes információkat tartalmaz.	0,002
A jelszó értelmes szót tartalmaz.	0,338
Ugyan azt a jelszót több helyen használja.	0,161
A jelszó változtatás.	0,315
A jelszó hossza.	0,610

A jelszóhasználat esetében amikor a jelszó tartalmát nézzük, hogy a jelszó kis és nagybetűket, számokat és speciális karaktereket tartalmaz, valamint személyes információkat szignifikáns különbség van. Láthatjuk, hogy a jelszóhasználat esetében, amikor a jelszó tartalmát nézzük meg, hogy a válaszadók Szlovákiában szignifikánsan összetettebb jelszavakat használnak a jelszó tartalmát illetően, mely így biztonságosabb azonos hosszúság esetén a brute force támadáskor. A személyes információt tartalmazó jelszó esetében elmondható, hogy Szerbiában szignifikánsan többen használnak olyan jelszót, ami értelmes szót tartalmaz. Láthatjuk, hogy nincs szignifikáns különbség az értelmes szót tartalmazó jelszó, a jelszó hossza és a jelszóváltoztatás gyakorisága között, valamint ugyanaz a jelszó használata több helyen esetében. Az értelmes szót tartalmazó jelszó esetében látható, hogy Szerbiában és Szlovákiában is ugyanúgy sokan használnak értelmes szót tartalmazó jelszót. Láthatjuk, hogy ugyanaz a jelszó használata esetében több helyen az okoseszköz használók ugyanúgy több helyen használják ugyanazt a jelszót Szerbiában és Szlovákiában is. A jelszó változtatás esetében Szerbiában és Szlovákiában is az okoseszköz használók ugyanúgy ritkán változtatják meg a jelszót. A jelszó hossza esetében pedig látható, hogy mindkét országban ugyanannyian kevesen használnak 12 vagy ennél is több karaktert tartalmazó jelszót.

4.7. Részkövetkeztetések

A felmérés alapján láthatjuk, hogy Szerbiában, Magyarországon és Szlovákiában a felmérésben résztvevők között az okoseszközök használata népszerű. Szerbiában, Magyarországon és Szlovákiában is a legnépszerűbb okoseszközök a felhasználók körében az okostelefon, az okosóra és az okostévé. Ha megnézzük, akkor láthatjuk, hogy mindhárom országban a legnépszerűbb okoseszköz az okostelefon. Ami az okoseszköz márkákra vonatkozik Szerbiában, Magyarországon és Szlovákiában is a legnépszerűbb okoseszköz márka a Samsung. A felmérésben résztvevő okoseszközhasználók többsége középiskolai végzettséggel rendelkezik Szerbiában, Magyarországon és Szlovákiában is. Az okoseszközök megvásárlásakor a legfontosabb szempont a felmérésben résztvevők válasza alapján Szerbiában, Magyarországon és Szlovákiában is az ár. Ami a biztonságot illeti láthatjuk, hogy Szerbiában, Magyarországon és Szlovákiában is a felmérésben résztvevők között vannak olyan okoseszköz használók, akik azt válaszolták, hogy nem használnak vírusvédelmet, vagy nem telepítik a firmware frissítéseket, és az applikációkat sem frissítik rendszeresen. Ha megnézzük mindhárom országot a válaszadók válasza alapján, akkor láthatjuk, hogy Szerbiában az okoseszközhasználók kevesebben telepítik a firmware frissítéseket, és az applikációkat is sokkal kevesebben frissítik rendszeresen, mint akik Magyarországon vettek részt a felmérésben. Ha megnézzük Magyarországot és Szlovákiát akkor láthatjuk, hogy Szlovákiában a felmérésben résztvevők válasza alapján sokkal többen használnak vírusvédelmet, és a firmware frissítések telepítése esetében is többen válaszoltak igennel, mint akik Magyarországon vettek részt a felmérésben. Magyarországon, Szerbiában és Szlovákiában is a felmérés alapján van olyan okoseszközhasználó, aki a jelszóhasználat esetében olyan jelszót használ, ami nem tartalmaz kis és nagybetűket, számokat, speciális karaktereket. A jelszó személyes információkat is tartalmaz, és értelmes szót. A felmérésben résztvevők Magyarországon, Szerbiában és Szlovákiában is több mint 60%-a válaszolta, hogy ugyanazt a jelszót több helyen használja. A jelszóhasználat megváltoztatásának gyakorisága esetében láthattuk, hogy Szerbiában a felmérésben résztvevők 61%-a válaszolta, hogy soha nem változtatja meg a jelszót, addig Magyarországon a 31,8%-a, míg Szlovákiában 40,7%-a. A jelszó hosszának esetében Magyarországon és Szerbiában is a felmérés alapján legtöbben 8-10 karaktert használnak, míg Szlovákiában legtöbben a felmérés alapján 12, vagy annál is több karaktert. Magyarországon a felmérésben résztvevők válasza alapján sokkal többen használnak 12, vagy annál is több karaktert jelszónak, mint Szerbiában. Ha megnézzük

Magyarországot és Szlovákiát akkor láthatjuk, hogy Szlovákiában a felmérés alapján többen használnak 12, vagy annál is több karaktert jelszónak, mint Magyarországon. A felmérésben arra is kerestem a választ, hogy hányan vennének részt egy ingyenes online képzésen, amely alapján Magyarországon és Szerbiában is a felmérésben résztvevők kevesebb mint fele válaszolta, hogy részt venne egy ingyenes online képzésen, melyben elsajátíthatná az alapvető ismereteket arról, hogy hogyan tudnák az okoseszközeiket biztonságosan használni. Szlovákiában a felmérésben résztvevők válaszai alapján több, mint fele válaszolta, hogy részt venne egy ilyen képzésen 55,9%-a. A felmérés által azt szerettem volna bebizonyítani, hogy az okoseszközök használata egyre népszerűbb, és hogy egyre többen használnak már különféle okoseszközöket napjainkban, valamint hogy az okoseszköz használók közül vannak olyan felhasználók, akik nem használnak vírusvédelmet, a firmware frissítéseket nem telepítik, és az applikációkat sem frissítik rendszeresen. A jelszóhasználat esetében pedig olyan jelszót használnak, ami nem tartalmaz kis és nagybetűket, számokat, speciális karaktereket. A jelszó esetében, amit használnak személyes információkat és értelmes szót tartalmaz, valamint ugyanazt a jelszót több helyen is használják, vagy nem változtatják meg soha. A jelszó hossza esetében pedig vannak olyan okoseszköz használók, akik kevesebb mint 8 karaktert használnak jelszónak.

5. ÖSSZEGZETT KÖVETKEZTETÉSEK

A kutatásom célja az okoseszközök biztonsági kihívásainak megismerése volt, valamint hogy feltérképezzem a hétköznapi életben használt okoseszközök mennyire elterjedtek a felhasználók körében, és hogy a felhasználók rendelkeznek-e az alapvető ismeretekkel ahhoz, hogy az okoseszközeiket biztonságosan tudják használni. Ezenkívül a kutatásom célja még, hogy feltérképezzem az okoseszközök jelszóhasználatának szokásait Magyarországon, Szerbiában és Szlovákiában különösen akkor, amikor értelmes szót használnak jelszónak. Valamint az informatikai oktatási tananyag összehasonlítása Magyarországon, Szerbiában és Szlovákiában, hogy van-e eltérés az országok informatikai oktatási tananyaga között. Ezért öt hipotézist fogalmaztam meg.

5.1. Új tudományos eredmények

Az értekezésem egyik része az okoseszközök biztonsági kihívásaival és megismerésével foglalkozik, a másik része az informatikai oktatási tananyaggal és a felhasználók tudatlanságával, valamint a jelszóhasználati szokásaival. A kutatásom első részében irodalomkutatást végeztem, addig a második részében kvantitatív kutatást az okoseszköz használók körében Magyarországon, Szerbiában és Szlovákiában. Az értekezésem során öt hipotézist vizsgáltam, és ezekkel kapcsolatban a következő megállapításokat teszem:

T1: Bebizonyítottam, hogy a hétköznapi életben megnőtt az okoseszközök használatára az igény, és hogy a hétköznapiakban használt okoseszközök iránt egyre több támadás irányul napjainkban.

T2: Bebizonyítottam a felmérés eredményével, valamint az irodalomkutatás során, hogy az okoseszköz használók többsége nem rendelkezik még csak az alapvető ismeretekkel sem, hogy az okoseszközeit biztonságosan tudja használni.

T3: A felmérés eredményével igazoltam, hogy a Magyarországon élők információbiztonsági tudatossága magasabb, mint a Szerbiában élőknek a jelszóhasználat esetében, amikor olyan jelszót használnak, ami értelmes szót tartalmaz. Ezt a Mann Whitney U teszt által megállapítottam a szignifikáns különbséget.

T4: A felmérés eredményével igazoltam, hogy a Magyarországon élők információbiztonsági tudatossága magasabb, mint a Szlovákiában élőknek a

jelszóhasználat esetében, amikor olyan jelszót használnak, ami értelmes szót tartalmaz. Ezt a Mann Whitney U teszt által megállapítottam a szignifikáns különbséget.

T5: Bebizonyítottam összehasonlító elemzéssel, hogy Magyarországon, Szerbiában és Szlovákiában különbség van az információbiztonság tudatossága terén a jelszóhasználatban lévő szignifikáns eltérések felfedésével a három ország esetében.

5.2. A kutatás jelentősége

Mivel napjainkban az okoseszközök használata megnőtt a hétköznapi életben, és egyre többen használnak különféle okoseszközöket a felhasználók közül sokan nem rendelkeznek alapvető ismeretekkel sem arról, hogyan tudnák az okoseszközeiket biztonságosan használni. Az értekezés által betekintést kaphatunk az okoseszközhasználók szokásaiba, hogy az okoseszközök használatának előnyei mellett számos biztonsági kihívást is rejtenek. A felmérés alapján láthattuk az okoseszközhasználók szokásait, ami alapján lehetne számukra egy képzést kidolgozni, amivel javítani lehetne a felhasználók információbiztonsági tudatosságát. Ezzel növelhető, hogy a felhasználók minél tudatosabban és biztonságosabban használják az okoseszközeiket, és ezáltal csökkenteni lehetne a sikeres támadásokat az okoseszközök ellen. Az informatikai oktatási tananyagot is bővíteni lehetne a középiskolások számára, hogy minél biztonságosabban tudják a diákok az okoseszközöket használni és megismerjék, hogy az okoseszközök használata veszélyes is lehet. A jövőbeli kutatásaim számára előnyös lenne még több okoseszközhasználó bevonása a felmérésbe, és más országokban is végezni a felmérést.

IRODALOMJEGYZÉK

- [1] Mandić Dorottya: Az okoseszközök veszélyei, Biztonságtudományi Szemle 5 : 3 pp. 37-45. , 9 p. (2023) [Online]. Elérhető: <https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/369/289> (Letöltve: 2024.02.03)
- [2] Mandić Dorottya, Kiss Gábor: Az okoseszközök és vírusvédelem használata Magyarországon és Szerbiában. 64–75(12) 30th Anniversary conference of the safety and security engineering education: A biztonságtechnikai mérnök képzés 30évi jubileumi konferenciája, Budapest, Magyarország, ISBN: 9789634493297
- [3] State of IoT 2023: Number of connected IoT devices growing 16% to 16.7 billion globally”. [Online]. Elérhető: <https://iot-analytics.com/number-connected-iot-devices/> (Letöltve: 2024.02.11)
- [4] Haig Zsolt: Információs műveletek a kibertérben, Dialóg Campus Kiadó. Budapest, 2018. ISBN: 978-615-5945-05-2
- [5] Mandić Dorottya, Simon János: Biztonságosak-e az okosotthonokban használt okoseszközök, Biztonságtudományi Szemle 4:4 pp. 59-67., 9p. (2022) [Online]. Elérhető: <https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/272/226> (Letöltve: 2024.02.13)
- [6] Mezei Kitti, „A modern technológiák kihívásai a büntetőjogban, különös tekintettel a kiberbűnözésre.”, köt. Állam és Jogtudomány LXI. évfolyam, sz. 4. szám, 2020. [Online]. Elérhető: https://real.mtak.hu/118627/1/2020-04_MEZEI-tan.pdf (Letöltve: 2024.02.17)
- [7] Anand Mohan: SURVEY PAPER ON IOT ATTACKS AND ITS PREVENTION MECHANISMS, Inf. Manag. Comput. Sci., köt. 3, sz. 2, o. 38–41, dec. 2020, doi: 10.26480/imcs.02.2020.38.41.
- [8] „Kiberbiztonság: hogyan kezeli az EU a kiberfenyegetéseket?” [Online]. Elérhető: <https://www.consilium.europa.eu/hu/policies/cybersecurity/> (Letöltve: 2024.03.16) (Letöltve: 2024.02.20)
- [9] „Mit jelent a COVID-19 az intelligens otthoni technológiához?” [Online]. Elérhető: <https://hu.denizatm.com/pages/48116-what-covid-19-has-meant-for-smart-home-technology> (Letöltve: 2024.02.22)
- [10] „A tárgyak internete-IoT”. [Online]. Elérhető: <https://hu.rs-online.com/web/generalDisplay.html?id=i/iot-internet-of-things> (Letöltve: 2024.02.22)
- [11] Kovács László: A kibertér védelme. Budapest, Hungary: Dialóg Campus Kiadó, 2018. ISBN: 978-615-5889-64-6
- [12] Bocskor Viktor, Loós Csaba, Major Tamás, Boldizs Péter Ferenc: A dolgok internete-Technológiai háttér, információbiztonsági és adatvédelmi aspektusok”, Infokommunikációs És Jog, sz. 12, o. 62-63 57-66, 2015. [Online]. Elérhető: <https://fornax.hu/wp-content/uploads/2016/09/Informa%CC%81cio%CC%81biztons%CC%81g-e%CC%81s-adatve%CC%81delem-az-IoT-vila%CC%81ga%CC%81banv02jav.pdf> (Letöltve: 2024.02.26)

- [13] Kevin ASHTON: That ‘Internet of Things’ Thing [Online]. Elérhető: <https://www.rfidjournal.com/that-internet-of-things-thing> (Letöltve:2024.03.02)
- [14] Albert Ágota és Üveges András József: „Az IoT eszközök biztonsága a személyes adatok tükrében szakmai szemle”, Katonai Nemzetbiztonsági Szolg. Tudományos Szakmai Folyóirata, sz. 20:2.138-187, 2022. [Online]. Elérhető: https://www.knbsz.gov.hu/hu/letoltes/szsz/2022_2_szam.pdf (Letöltve:2024.03.02)
- [15] Maros Dóra: Internet of Things, azaz a Dolgok Internete. Elektrotechnika”. [Online]. Elérhető: <https://www.mee.hu/files/files/et2019-7-8.pdf> (Letöltve:2024.03.05)
- [16] D. Evans: „The Internet of Things: How the next evolution of the internet is changing everything”. [Online]. Elérhető: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (Letöltve:2024.03.07)
- [17] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, B. Sikdar: „A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures”, IEEE Access, köt. 7, o. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.
- [18] „Digital around the world”. [Online]. Elérhető: <https://datareportal.com/global-digital-overview> (Letöltve:2024.03.08)
- [19] „Number of internet and social media users worldwide as of April 2024”. [Online]. Elérhető: <https://www.statista.com/statistics/617136/digital-population-worldwide/> (Letöltve:2024.05.03)
- [20] „Connected products”. [Online]. Elérhető: <https://prod.ucwe.capgemini.com/wp-content/uploads/2023/11/Final-Web-Version-Report-Connected-Products.pdf> (Letöltve:2024.05.04)
- [21] Peter Skalfist, Daniel Mikelsten, Vasil Teigens: Mesterséges intelligencia: A negyedik ipari forradalom. [Online]. Elérhető: https://books.google.rs/books?id=tx3NDwAAQBAJ&printsec=frontcover&rdir_es%20c=y#v=onepage&q&f=false (Letöltve:2024.05.07)
- [22] S. A. Goswami, B. P. Padhya, K. D. Patel: „Internet of Things: Applications, Challenges and Research Issues”, in 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India: IEEE, dec. 2019, o. 47–50. doi: 10.1109/I-SMAC47947.2019.9032474.
- [23] Tokody Dániel, Mezei János Imre: Okos, fenntartható és biztonságos városok., KÖZTES EURÓPA: TÁRSADALOM TUDOMÁNYI FOLYÓIRAT: A VIKEK KÖZLEMÉNYEI 9:1-2(21-22) pp. 73-81. , 9 p. (2017), [Online]. Elérhető: <https://www.americanaejournal.hu/index.php/vikekke/article/view/12742/12598> (Letöltve:2024.05.09)
- [24] „Smart Farming – avagy mit is jelent az “okos” mezőgazdaság?” [Online]. Elérhető: <http://www.robotekt.hu/smart-farming-robotekt/> (Letöltve:2024.05.09)
- [25] „Okos eszközök az egészség szolgálatában”. [Online]. Elérhető: <https://www.longevity-project.org/post/okos-eszkozok-az-egeszseg-szolgalataban> (Letöltve:2024.05.10)

- [26] „Hogy működik, mennyibe kerül és egyáltalán mi az az okosotthon?” [Online]. Elérhető: <https://www.xiaomishop.hu/hogy-mukodik-mennyibe-kerul-es-egyaltalan-mi-az-okosotthon> (Letöltve:2024.05.11)
- [27] Ahmad Bilal Zia és CGC TECHNICAL CAMAPUS, JHANERI, „A Research Paper on Internet of Things based upon Smart Homes with Security Risk Assessment using OCTAVE Allegro”, Int. J. Eng. Res., köt. V9, sz. 06, o. IJERTV9IS060692, jún. 2020, doi: 10.17577/IJERTV9IS060692.
- [28] „Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030”. [Online]. Elérhető: <https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/> (Letöltve:2024.05.13)
- [29] H. Touqeer, S. Zaman, R. Amin, M. Hussain, F. Al-Turjman, M. Bilal, „Smart home security: challenges, issues and solutions at different IoT layers”, J. Supercomput., köt. 77, sz. 12, o. 14053–14089, dec. 2021, doi: 10.1007/s11227-021-03825-1.
- [30] „Number of Internet of Things (IoT) connected devices from 2020 to 2030 (in millions), by region”. [Online]. Elérhető: <https://www.statista.com/statistics/1194677/iot-connected-devices-regionally/> (Letöltve:2024.05.13)
- [31] „Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2033, by vertical”. [Online]. Elérhető: <https://www.statista.com/statistics/1194682/iot-connected-devices-vertically/#statisticContainer> (Letöltve:2024.05.15)
- [32] „Kutatás: Már a magyarok kétharmada visel okoseszközt a csuklóján”. [Online]. Elérhető: <https://consumer.huawei.com/hu/press/news/2021/news-210304/> (Letöltve:2024.05.15)
- [33] „Az okoseszközök előnye a folyamatos egészségmonitoring”. [Online]. Elérhető: http://medicalonline.hu/informatika/cikk/az_okoseszkozok_elonye_a_folyamatos_egeszseg-monitoring (Letöltve:2024.05.16)
- [34] „Egészségtudatosabbak az okosórák, és okoskarkötők hazai használói”. [Online]. Elérhető: <https://enet.hu/egeszsegtudatosabbak-az-okosorak-es-okoskarkotok-hazai-hasz-naloi/> (Letöltve:2024.05.17)
- [35] „Egyre többen használnak okoseszközöket otthonukban -INNObytekutatás [Online]. Elérhető”. [Online]. Elérhető: <https://innobyte.hu/egyre-tobben-hasznalnak-okoseszkozokat-otthonukban-innobyte-kutatas/> (Letöltve:2024.05.18)
- [36] „A plafont súrolja a hazai okostelefon használat”. [Online]. Elérhető: <https://enet.hu/a-plafont-surolja-a-hazai-okostelefon-hasznalat/> (Letöltve:2024.05.20)
- [37] „Okoseszközök térhódítása”. [Online]. Elérhető: https://www.smartos.hu/blog/okoses_zkozok-terhoditasa-64 (Letöltve:2024.05.22)
- [38] „Consumer IoT”. [Online]. Elérhető: <https://www.jtsec.es/iot-cybersecurity> (Letöltve:2024.05.23)
- [39] „Sok az új okoseszköz a magyar háztartásokban, de a bevásárlólista még nem üres”. [Online]. Elérhető: <https://www.samsung.com/hu/news/local/sok-az-uj->

okoseszkoz-a-ma-gyar-haztartasokban-de-a-bevasarlolista-meg-nem-ures/
(Letöltve:2024.05.24)

[40] „Digitális Fogyasztói Trendek”. [Online]. Elérhető: https://www2.deloitte.com/content/dam/Deloitte/hu/Documents/technology/Digitalis_Fogyasztoi_Trendek_Felmeres_Magyarország_2022.pdf (Letöltve:2024.05.24)

[41] „Az elektronikus hírközlési piac fogyasztóinak vizsgálata Háztartási felmérés-2022”. [Online]. Elérhető: https://nmhh.hu/dokumentum/236962/haztartasi_felmeres_2022_az_elektronikus_hirkozlesi_piaci_fogyasztoknak_vizsgalata.pdf (Letöltve:2024.05.25)

[42] „The most popular Smart Home Devices 2022”. [Online]. Elérhető: <https://www.reviews.org/home-security/most-popular-smart-home-device-statistics/> (Letöltve:2024.05.27)

[43] „The best smart home devices”. [Online]. Elérhető: <https://www.digitaltrends.com/home/best-smart-home-devices/> (Letöltve:2024.05.27)

[44] „New Xiaomi survey explores how Covid-19 is driving the new smart home, and what it means for 2021 and beyond”. [Online]. Elérhető: <https://techcrunch.com/sponsor/xiaomi/new-xiaomi-survey-explores-how-covid-19-is-driving-the-new-smart-home-and-what-it-means-for-2021-and-beyond/> (Letöltve:2024.05.28)

[45] „Smart Home Spending Increased since Start of Pandemic”. [Online]. Elérhető: <https://www.safewise.com/blog/smart-home-tech-spending/> (Letöltve:2024.05.29)

[46] X. Cao, L. Liu: „Use of Smart Devices: A Survey, Some Research Issues, and Challenges”, in 2020 International Conference on Culture-oriented Science & Technology (ICCST), Beijing, China: IEEE, okt. 2020, o. 378–382. doi: 10.1109/ICCST50977.2020.00079.

[47] Mandic Dorottya: „A mesterséges intelligencia alkalmazása az okosotthonokban”, 4 : 1 pp. 33-41. , 9 p., 2022. [Online]. Elérhető: <https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/196/177> (Letöltve:2024.06.01)

[48] „Az IoT eszközök veszélyei”. [Online]. Elérhető: <https://mernoknok.hu/az-iot-eszkozok-veszelyei/> (Letöltve:2024.06.03)

[49] Tóth András: Új típusú kihívások az infokommunikációban, Ludovika Egyetemi Kiadó, Budapest 2023, ISBN: 978-615-6598-51-6

[50] Mandic Dorottya: „Az okoseszközök veszélyei, Biztonságtudományi Szemle 5(3)37–45.” [Online]. Elérhető: <https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/369/289> (Letöltve:2024.06.04)

[51] Eszter Dániel: „Az új technológiák megjelenésének hatása a személyes adatok védelmére: gépi tanulás, blokklánc, internet-of-things, agyhullám-olvasás”. [Online]. Elérhető: <http://real.mtak.hu/133906/1/eszter.daniel.uj.technologiak.adatvedelem.pdf> (Letöltve:2024.06.05)

[52] „Mit tudnak rólunk okoseszközeink?” [Online]. Elérhető: <https://ikron.hu/okoseszkozok-veszelyei/> (Letöltve:2024.06.05)

- [53] „The OWASP IoT top 10 vulnerabilities and how to mitigate them”. [Online]. Elérhető: <https://www.sisainfosec.com/blogs/the-owasp-iot-top-10-vulnerabilities-and-how-to-mitigate-them/> (Letöltve:2024.06.07)
- [54] Kanizsai Viktor, „Tárgyak Interneté-tárgyak bizonytalansága”, [Online]. Elérhető: http://www.vmtt.org.rs/mtn2016/503_513_Kanizsai.pdf (Letöltve:2024.06.09)
- [55] S. Sanaullah, B. Liu: Information Security Challenges in the Internet of Things (IoT) Ecosystem”, in 2022 International Symposium on Electrical, Electronics and Information Engineering (ISEEIE), Chiang Mai, Thailand: IEEE, febr. 2022, o. 124–129. doi: 10.1109/ISEEIE55684.2022.00029.
- [56] X. Su, B. Wang, C. Choi, D. Choi: Case study on password complexity enhancement for smart devices”, in 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV: IEEE, jan. 2017, o. 1–5. doi: 10.1109/CCNC.2017.8013419.
- [57] „Milyen tévéje van otthon? Figyelmeztetést adott ki az FBI”. [Online]. Elérhető: https://hvg.hu/tudomany/20191203_okos_tevekeszulek_lehallgatas_megfigyeles_fbi (Letöltve:2024.06.12)
- [58] „Kémkedő eszközök”. [Online]. Elérhető: <https://itlawpro.com/hu/adatvedelem/kemkedo-eszkozok> (Letöltve:2024.06.12)
- [59] „Az okoseszközök veszélyei a porszívó is kémkedik?” [Online]. Elérhető: <https://zeroitlab.com/hu/blog/az-okos-eszkozok-veszelyei-porszivo-kemkedik> (Letöltve:2024.06.12)
- [60] „Kényelmesek az okoskütyük - de elég biztonságosak is?” [Online]. Elérhető: <https://www.eset.com/hu/hirek/az-okos-eszkozok-kenyelmesek-de-vajon-biztonsagosak-is-2020/> (Letöltve:2024.06.14)
- [61] K. Győrffyné Holló: Az információbiztonság jelentősége és története”, Gradus, köt. 8, sz. 2, o. 102–112, 2021, doi: 10.47833/2021.2.CSV.001, [Online]. Elérhető: https://gradus.kefo.hu/archive/2021-2/2021_2_CSV_001_Gyorffyne.pdf (Letöltve:2024.06.16)
- [62] A Digitális biztonságról. PROMPT-H Számítástechnikai, Oktatási, Kereskedelmi és Szolgáltató Kft. [Online]. Elérhető: <https://mek.oszk.hu/23600/23634/23634.pdf> (Letöltve:2024.06.19)
- [63] Erdősi Péter Máté és Solymos Ákos, IT biztonság közérthetően. 1054 Budapest, Báthory u. 16., 2018. [Online]. Elérhető: https://nki.gov.hu/wp-content/uploads/2019/03/NJSZT_IT_Biztonsag_kozerthetoen_v3.pdf (Letöltve:2024.06.22)
- [64] „Az információbiztonság lélektana”. [Online]. Elérhető: <https://nki.gov.hu/wp-content/uploads/2019/07/01-Az-inform%C3%A1ci%C3%B3biztons%C3%A1g-l%C3%A9lektana.pdf> (Letöltve:2024.06.23)
- [65] „1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról”. [Online]. Elérhető: https://2010-2014.kormany.hu/download/b/b6/21000/Magyarország_Nemzeti_Kiberbiztonsagi_Strategiaja.pdf (Letöltve:2024.06.23)

- [66] Busa Attila József: A digitális információbiztonság alapja: A megfelelő kibertudatosság”, HÍRVILLÁM SIGNAL BADGE Nemzeti Közzolgálati Egy. H. Tansz. Tudományos Idősz. Kiadványa Prof. J. Signal Departement Univ. Public Serv., sz. pp. 25-43. , 18 p., 2023.
- [67] Mádi-Nátor Anett, Kardos Zoltán: Információbiztonság-tudatosság gyakorlat. [Online]. Elérhető: <https://kti.uni-nke.hu/document/vtkk-uni-nke-hu/informaciobiztonsag-tudatossag-gyakorlat.original.pdf> (Letöltve:2024.06.25)
- [68] Kollár Csaba: Társadalom és információbiztonság: A humán információbiztonság a digitális korban, Társadalom, kulturális háttér, gazdaság : IV. IRI Társadalomtudományi Konferencia, Komárno, Szlovákia : International Research Institute (2016) 488 p. pp. 189-194. , 6 p. [Online]. Elérhető: <https://www.irisro.org/tarstud2016aprilis/42KollarCsaba.pdf> (Letöltve:2024.06.26)
- [69] Bak Gerda, Kelemen-Erdős Anna: Információbiztonság-tudatosság az Y generáció szemszögéből, kvalitatív megközelítés alapján, Hadmérnök, köt. 17, sz. 3, o. 81–95, nov. 2022, doi: 10.32567/hm.2022.3.6. [Online]. Elérhető: <https://folyoirat.ludovika.hu/index.php/hadmernok/article/view/6064/5158> (Letöltve:2024.06.27)
- [70] „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”. [Online]. Elérhető: <https://net.jogtar.hu/jogszabaly?docid=A15H2012.KOR&txtreferer=0000> (Letöltve:2024.06.28)
- [71] „Az internet-hozzáférés aránya a háztartásokban”. [Online]. Elérhető: <https://ksh.hu/s/kiadvanyok/fenntarthato-fejlodes-indikatorai-2023/1-10> (Letöltve:2024.07.02)
- [72] „Internethasználati szokások, digitális média- és tartalomfogyasztás”. [Online]. Elérhető: https://nmhh.hu/cikk/235951/Internethasznalati_szokasok_digitalis_media_es_tartalomfogyasztas (Letöltve:2024.07.04)
- [73] „Digital 2024: Global overview report ”. [Online]. Elérhető: datareportal.com/reports/digital-2024-global-overview-report (Letöltve:2024.08.11)
- [74] „Analyzing time devoted to online and traditional forms of media at a global level, as well as by age and across countries”. [Online]. Elérhető: https://www.gwi.com/hubfs/Digital_vs_Traditional_Media_Consumption.pdf (Letöltve:2024.08.15)
- [75] „Internet Usage Statistics In 2024”. [Online]. Elérhető: <https://www.forbes.com/home-improvement/internet/internet-statistics/> (Letöltve:2024.08.21)
- [76] „US time spent with media 2022 update—pivotal moments for TV, subscription OTT, digital audio, and social media”. [Online]. Elérhető: <https://www.emarketer.com/insights/us-time-spent-with-media/> (Letöltve:2024.08.24)
- [77] „Guide to IoT and connected devices: Growth, trends, and advertising”. [Online]. Elérhető: <https://www.emarketer.com/insights/internet-of-things-devices-examples/> (Letöltve:2024.08.25)

- [78] Bak Gerda, Kiss Sándor: A biztonságtudatosság szisztematikus szakirodalmi áttekintése”, *Hadmérnök*, köt. 16, sz. 4, o. 85–99, 2021, doi: 10.32567/hm.2021.4.7. [Online]. Elérhető: <https://folyoirat.ludovika.hu/index.php/hadmernok/article/view/5549/4828> (Letöltve:2024.09.20)
- [79] Koller Marco, Kerti András: Az okoseszközök applikációi által gyűjtött metaadatokkal való visszaélések kockázati szemléletmód általi, felhasználói szintű lehetséges visszaszorítása”, *Hadmérnök*, köt. 16, sz. 4, o. 145–156, 2021, doi: 10.32567/hm.2021.4.11. [Online]. Elérhető: <https://folyoirat.ludovika.hu/index.php/hadmernok/article/view/5591/4832> (Letöltve:2024.09.21)
- [80] I. Mannuela, J. Putri, Michael, M. S. Anggreainy: Level of Password Vulnerability, in 2021 1st International Conference on Computer Science and Artificial Intelligence (ICCSAI), Jakarta, Indonesia: IEEE, okt. 2021, o. 351–354. doi: 10.1109/ICCSAI53272.2021.9609778.
- [81] „Most common passwords around the world 2024”. [Online]. Elérhető: <https://www.expressvpn.com/blog/infographic-common-passwords-by-country/> (Letöltve:2024.09.24)
- [82] „Most common passwords: latest 2024 statistics”. [Online]. Elérhető: <https://cybernews.com/best-password-managers/most-common-passwords/> (Letöltve:2024.09.26)
- [83] D. K. Davis, M. M. Chowdhury, N. Rifat, „Password Security: What Are We Doing Wrong?”, in 2022 IEEE International Conference on Electro Information Technology (eIT), Mankato, MN, USA: IEEE, máj. 2022, o. 562–567. doi: 10.1109/eIT53891.2022.9814059.
- [84] L. Ayavaca-Vallejo, D. Avila-Pesantez: Smart Home IoT Cybersecurity Survey: A Systematic Mapping”, in 2023 Conference on Information Communications Technology and Society (ICTAS), Durban, South Africa: IEEE, márc. 2023, o. 1–6. doi: 10.1109/ICTAS56421.2023.10082751.
- [85] „Most common passwords used in Internet of Things (IoT) devices over a 45 day period worldwide in 2021”. [Online]. Elérhető: <https://www.statista.com/statistics/1298495/frequently-seen-passwords-in-iot-devices/> (Letöltve:2024.09.27)
- [86] Keszthelyi András: Life is Short. Have another Affair - Password Security, o. 121–130, 2015. [Online]. Elérhető: <https://old2.kgk.uni-obuda.hu/sites/default/files/Keszthelyi.pdf> (Letöltve:2024.09.30)
- [87] „Top 200 most common passwords of the year 2019-2022”. [Online]. Elérhető: <https://s1.nordcdn.com/nord/misc/0.78.0/nordpass/top-200-2023/200-most-common-passwords-en.pdf> (Letöltve:2024.10.01)
- [88] „Threat Landscape Trends – Q2 2020”. [Online]. Elérhető: <https://symantec-enterprise-blogs.security.com/threat-intelligence/threat-landscape-trends-q2-2020> (Letöltve:2024.10.02)
- [89] „How Secure Is My Password?” [Online]. Elérhető: <https://www.security.org/how-secure-is-my-password/> (Letöltve:2024.10.05)

- [90] „How Long Does It Take for a Hacker to Crack a Password?” [Online]. Elérhető: <https://tech.co/password-managers/how-long-hacker-crack-password> (Letöltve:2024.10.11)
- [91] „Jelszóhasználat”. [Online]. Elérhető: <https://nki.gov.hu/it-biztonsag/tartalom/eszkoztar/jelszohasznalat/> (Letöltve:2024.10.11)
- [92] „Az ENISA – Európai Unió Kiberbiztonsági Ügynökség”. [Online]. Elérhető: <https://www.enisa.europa.eu/about-enisa/about/hu> (Letöltve:2024.10.14)
- [93] „Biztonságos megoldások a dolgok internetére”. [Online]. Elérhető: <https://digital-strategy.ec.europa.eu/hu/policies/secure-internet-things> (Letöltve:2024.10.14)
- [94] „A szervezett bűnözés elleni küzdelem az Unióban”. [Online]. Elérhető: <https://www.consilium.europa.eu/hu/policies/eu-fight-against-crime/> (Letöltve:2024.10.14)
- [95] „Az Európai parlament és a tanács (EU) 2016/1148 irányelve: A hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről”. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.HUN&toc=OJ:L:2016:194:TOC (Letöltve:2024.10.15)
- [96] „Baseline Security Recommendations for IoT”. [Online]. Elérhető: <https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot> (Letöltve:2024.10.17)
- [97] Horváth Regina: Az okoseszközök világának kockázatai a GDPR tükrében, avagy mennyire vagyunk biztonságban?”, [Online]. Elérhető: https://acta.bibl.u-szeged.hu/70864/1/forum_discipulorum_2019_131-160.pdf (Letöltve:2024.10.19)
- [98] „Good Practices for Security of IoT - Secure Software Development Lifecycle”. [Online]. Elérhető: <https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1> (Letöltve:2024.10.20)
- [99] „Guidelines for Securing the Internet of Things”. [Online]. Elérhető: <https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things> (Letöltve:2024.10.20)
- [100] „A kiberrezilienciáról szóló jogszabály: az új uniós kiberbiztonsági szabályok biztonságosabb hardvert és szoftvert biztosítanak”. [Online]. Elérhető: <https://digital-strategy.ec.europa.eu/hu/events/cyber-resilience-act-new-eu-cybersecurity-rules-ensure-safer-hardware-and-software> (Letöltve:2024.10.20)
- [101] „A kiberrezilienciáról szóló uniós jogszabály”. [Online]. Elérhető: <https://digital-strategy.ec.europa.eu/hu/policies/cyber-resilience-act> (Letöltve:2024.10.21)
- [102] „Az Informatika helyzete és fejlesztési feladatai”. [Online]. Elérhető: <https://ofi.oh.gov.hu/tudastar/tantargyak-helyzete/informatika-helyzete> (Letöltve:2024.10.21)
- [103] „Informatika helyett jön a digitális kultúra óra - a diákok már ötödikben robotokat programozhatnak”. [Online]. Elérhető: https://eduline.hu/kozoktatas/20200716_digitalis_kultura_ora (Letöltve:2024.10.23)

- [104] „Útmutató a digitális kultúra tantárgy tanításához a 2020-ban kiadott Nemzeti alaptanterv és kerettantervek alapján”. [Online]. Elérhető: <https://www.oktatas2030.hu/wp-content/uploads/2020/10/utmutato-a-digitalis-kultura-tantargy-tanitasahoz.pdf> (Letöltve:2024.10.23)
- [105] „Kerettanterv az általános iskola 5–8. évfolyama számára”. [Online]. Elérhető: https://www.oktatas.hu/kozneveles/kerettantervek/2020_nat/kerettanterv_alt_isk_5_8/ (Letöltve:2024.10.25)
- [106] „Kerettanterv a gimnáziumok 9–12. évfolyama számára”. [Online]. Elérhető: https://www.oktatas.hu/kozneveles/kerettantervek/2020_nat/kerettanterv_gimn_9_12_evf (Letöltve:2024.10.27)
- [107] Silvia Ilić: Upotreba informacionih tehnologija u nastavi – stavovi i mišljenja nastavnika i učenika. [Online]. Elérhető: <https://nardus.mpn.gov.rs/bitstream/id/68509/Disertacija.pdf> (Letöltve:2024.11.03)
- [108] „Zakon o osnovama sistema obrazovanja i vaspitanja”. [Online]. Elérhető: <https://paragraflex.rs/dnevne-vesti/290616/290616-vest7.html> (Letöltve:2024.11.08)
- [109] „Informatika postaje obavezan predmet od prvog razreda osnovnih škola u Srbiji”. [Online]. Elérhető: <https://startit.rs/informatika-postaje-obavezan-predmet-od-prvog-razreda-osnovnih-skola-u-srbiji/> (Letöltve:2024.11.09)
- [110] „Годишњи програм информатика и рачунарство – 5. разред”. [Online]. Elérhető: <https://osstanojemiljkovic.nasaskola.rs/files/Vladimir%20Kne%C5%BEEvi%C4%87/Plan%20Informatika%20i%20Ra%C4%8Dunarstvo%20-%20Kne%C5%BEEvi%C4%87%20Vladimir%20V%20razred.pdf> (Letöltve:2024.11.12)
- [111] „Годишњи програм информатика и рачунарство – 6. разред”. [Online]. Elérhető: <https://osstanojemiljkovic.nasaskola.rs/files/Vladimir%20Kne%C5%BEEvi%C4%87/Plan%20Informatika%20i%20Ra%C4%8Dunarstvo%20-%20Kne%C5%BEEvi%C4%87%20Vladimir%20VI%20razred.pdf> (Letöltve:2024.11.15)
- [112] „Информатика и Рачунарство – 7. разред”. [Online]. Elérhető: <https://osstanojemiljkovic.nasaskola.rs/files/Vladimir%20Kne%C5%BEEvi%C4%87/Plan%20Informatika%20i%20Ra%C4%8Dunarstvo%20-%20Kne%C5%BEEvi%C4%87%20Vladimir%20VII%20razred.pdf> (Letöltve:2024.11.17)
- [113] „Годишњи програм информатика и рачунарство – 8. разред”. [Online]. Elérhető: <https://osstanojemiljkovic.nasaskola.rs/files/Vladimir%20Kne%C5%BEEvi%C4%87/Plan%20Informatika%20i%20Ra%C4%8Dunarstvo%20-%20Kne%C5%BEEvi%C4%87%20Vladimir%20VIII%20razred.pdf> (Letöltve:2024.11.18)
- [114] Marijana Matović: Programi digitalnih kompetencija u Republici Srbiji, Fakultet političkih nauka, Univerzitet u Beogradu. [Online]. Elérhető: <https://www.osce.org/files/f/documents/d/7/495181.pdf> (Letöltve:2024.11.19)

- [115] „Pregled tržišta elektronskih komunikacija i poštanskih usluga u republici Srbiji u 2023. godini”. [Online]. Elérhető: https://www.ratel.rs/uploads/documents/empire_plugin/USLUGE%20%C5%A0IROKO POJASNOG%20PRISTUPA%20INTERNETU.pdf (Letöltve:2024.11.20)
- [116] Zentai Gabriella, Borbélyová Diana, Bencéné Fekete Andrea, Nagyová Alexandra, Horváth Kinga, Orsovics Yvette, Józsa Krisztián: A szlovákiai és a magyar általános iskolai tantervek összehasonlító vizsgálata a DIFER-készségek fejlesztése szempontjából, A comparative study of the Slovak and Hungarian primary school curricula from the point of view of the development of DIFER skills”, *Erud.-Educ.*, köt. 18., sz. 3, o. 78–94, 2023, doi: 10.36007/eruedu.2023.3.078-094. [Online]. Elérhető: https://e-eruditio.ujs.sk/wp-content/uploads/2023/11/Eru-Edu_2023_3_06_Study_078-094.pdf (Letöltve:2024.11.27)
- [117] Pásztor Bence: Az Információbiztonság oktatásának összehasonlítása Szlovákiában és Magyarországon, in *Conference Proceedings, J. Selye University*, 2023, o. 181–186. doi: 10.36007/4782.2023.181. [Online]. Elérhető: <http://uk.ujs.sk/dl/4782/PASZTOR.pdf> (Letöltve:2024.11.29)
- [118] „RÁMCOVÝ UČEBNÝ PLÁN pre ZŠ s vyučovacím jazykom slovenským”. [Online]. Elérhető: https://www.minedu.sk/data/files/6948_priloha_2_rup.pdf (Letöltve:2024.12.01)
- [119] Pásztor Bence: Az információbiztonság megjelenése a Csehországi és a Szlovákiai tantervben, *Gradus*, köt. 11, sz. 1, 2024, doi: 10.47833/2024.1.CSC.009. [Online]. Elérhető: https://gradus.kefo.hu/archive/2024-1/2024_1_CSC_009_Pasztor.pdf (Letöltve:2024.12.03)
- [120] D. Karuovic, D. Glusac, I. Tasic, R. Pap: Comparative presentation of the application of IT in teaching in the Republic of Serbia and Hungary”, in *2015 IEEE 13th International Symposium on Applied Machine Intelligence and Informatics (SAMI)*, Herl’any, Slovakia: IEEE, jan. 2015, o. 249–254. doi: 10.1109/SAMI.2015.7061884.
- [121] D. Mandic, G. Kiss, Z. Rajnai: Password Usage among Users of Smart Devices in Hungary and Serbia”, in *2024 IEEE 18th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, Timisoara, Romania: IEEE, máj. 2024, o. 000309–000314. doi: 10.1109/SACI60582.2024.10619863.
- [122] G. Kiss, A. Szasz: Analysing of the information security awareness of the economic information technology students”, in *2016 IEEE 17th International Symposium on Computational Intelligence and Informatics (CINTI)*, Budapest, Hungary: IEEE, nov. 2016, o. 000213–000218. doi: 10.1109/CINTI.2016.7846406.
- [123] Hunkár Márta: Kutatás módszertana. Debreceni Egyetem 2013, ISBN: 978-615-5183-54-6 [Online]. Elérhető: https://dtk.tankonyvtar.hu/xmlui/bitstream/handle/123456789/3424/kutatas_modszertan_gyakorlati_jegyzet.pdf (Letöltve:2024.06.12)
- [124] Géring Zsuzsanna, Király Gábor, Fűzi Beatrix: Kutatásmódszertani segédletek”, *Budapesti Gazdasági Egyetem*. Budapest, 2019. [Online]. Elérhető: https://publikaciotar.uni-bge.hu/id/eprint/1621/1/Kutat%C3%A1sm%C3%B3dszertani%20sed%C3%A9gletek_e_gybe.pdf (Letöltve:2024.06.14)

[125] „Interpret the key results for Mann-Whitney Test”. [Online]. Elérhető:
<https://support.minitab.com/en-us/minitab/help-and-how-to/statistics/nonparametrics/how-to/mann-whitney-test/interpret-the-results/key-results/>
(Letöltve:2024.06.28)

TÁBLÁZATJEGYZÉK

1.táblázat: Az Enisa ajánlásai az IoT biztonságára.....	34
2.táblázat: A Nat a digitális kultúra tantárgy során az óraszámok az évfolyamok szerint a 2020-ban kiadott Nemzeti alaptanterv és kerettantervek alapján.....	37
3.táblázat. Az informatika megjelenése az általános és középiskolák tantervében Szerbiában.....	40
4.táblázat: Informatikai óraszám Szlovákiában.....	42
5.táblázat: A felmérésben résztvevők nemek szerint Szerbiában, Magyarországon és Szlovákiában.....	46
6.táblázat: A felmérésben résztvevők nemek szerint Szerbiában, Magyarországon és Szlovákiában.....	48
7.táblázat: A felmérésben résztvevők életkora Szerbiában, Magyarországon és Szlovákiában.....	49
8.táblázat: A felmérésben résztvevők iskolai végzettsége Szerbiában, Magyarországon és Szlovákiában.....	51
9.táblázat: A felmérésben résztvevők informatikai végzettsége Szerbiában, Magyarországon és Szlovákiában.....	53
10.táblázat: Az okoseszköz használók nemek szerint Szerbiában, Magyarországon és Szlovákiában a felmérés alapján.....	54
11.táblázat: Az okoseszköz használók életkora Szerbiában, Magyarországon és Szlovákiában a felmérés alapján.....	56
12.táblázat: Az okoseszköz használók iskolai végzettsége a felmérés alapján Szerbiában, Magyarországon és Szlovákiában.....	60
13.táblázat: Az okoseszköz márka fontossága Szerbiában, Magyarországon és Szlovákiában.....	69
14.táblázat: A jelszó változtatás gyakorisága Szerbiában, Magyarországon és Szlovákiában a felmérésben alapján.....	74

15.táblázat: A jelszó hossza a felmérés alapján Szerbiában, Magyarországon és Szlovákiában.....	77
16.táblázat: Az okoseszköz használók jelszóhasználati szokásai Magyarországon leíró statisztikával.....	80
17.táblázat: Az okoseszköz használók jelszóhasználati szokásai Szerbiában leíró statisztikával.....	80
18.táblázat: Az okoseszköz használók jelszóhasználati szokásai Szlovákiában leíró statisztikával.....	81
19.táblázat: Jelszóhasználati szokások Magyarországon, Szerbiában és Szlovákiában..	81
20.táblázat: Jelszóhasználat Magyarországon és Szlovákiában Mann-Whitney U teszt..	82
21.táblázat: Jelszóhasználat Szerbiában és Szlovákiában Mann-Whitney U teszt.....	83

ÁBRAJEGYZÉK

1.ábra: IoT architektúra.....	10
2.ábra: Az IoT alkalmazási területei.....	11
3.ábra: Az IoT használata az okosotthonban.....	13
4.ábra. A világ népessége és a csatlakoztatott eszközök.....	14
5.ábra: Az IoT-eszközök száma 2019-től 2030-ig.....	15
6.ábra: Az IoT-eszközök száma 2020-tól 2030-ig országonként.....	16
7.ábra: Az IoT-eszközök számát világszerte 2019 és 2033 között területenként.....	17
8.ábra: Okoseszközök.....	18
9.ábra: A háztartások internetellátottsága 2020-ban az Európa Unióban és Magyarországon	26
10.ábra: Az internet használat idővonala.....	27
11.ábra: A leggyakrabban használt jelszavak 2024-ben a világon néhány ország bemutatásával.....	29
12.ábra: A Symantec jelentése 2020-ban a 10 legtöbbet használt felhasználónév amit használtak az IoT elleni támadásokor.....	31
13.ábra: A Symantec jelentése 2020-ban a 10 legtöbbet használt jelszó, amit használtak az IoT elleni támadásokor.....	32
14.ábra: A kutatás folyamata.....	45
15.ábra: A felmérésben résztvevők nemek szerint.....	47
16.ábra: A felmérésben résztvevők életkora Szerbiában, Magyarországon és Szlovákiában.....	49
17.ábra: A felmérésben résztvevők iskolai végzettségét országonként.....	50
18.ábra: A felmérésben résztvevők informatikai végzettsége országonként.....	52
19.ábra: Az okoseszköz használók nemek szerint Szerbiában, Magyarországon és Szlovákiában a felmérés alapján.....	53

20. ábra: Az okoseszköz használók életkora Szerbiában, Magyarországon és Szlovákiában.....	55
21. ábra: Az okoseszköz használók iskolai végzettsége Szerbiában, Magyarországon és Szlovákiában.....	56
22. ábra: Az 5 legtöbbet használt okoseszközök a felmérés alapján Szerbiában.....	57
23. ábra: Az 5 legtöbbet használt okoseszközök a felmérés alapján Magyarországon.....	58
24. ábra: Az 5 legtöbbet használt okoseszközök a felmérés alapján Szlovákiában.....	59
25. ábra: Az okoseszköz márka fontossága Szerbiában, Magyarországon és Szlovákiában.....	60
26. ábra: A 6 legtöbbet használt okoseszköz márka Szerbiában, Magyarországon és Szlovákiában a felmérés alapján.....	62
27. ábra: A legfontosabb vásárlási szempontok Szerbiában, Magyarországon és Szlovákiában a felmérés alapján.....	63
28. ábra: A felmérésben résztvevők válaszai, hogy hogy utána szoktak-e olvasni a megvásárolni kívánt okoseszköz termékleírásának, vásárlói véleményeknek Szerbiában, Magyarországon és Szlovákiában.....	65
29. ábra: Láthatjuk a vírusvédelem használatát Szerbiában, Magyarországon és Szlovákiában a felmérés alapján.....	66
30. ábra: Az applikációk rendszeres frissítése Szerbiában, Magyarországon és Szlovákiában a felmérés alapján.....	67
31. ábra: A firmware frissítések telepítése a felmérés alapján Szerbiában, Magyarországon és Szlovákiában.....	68
32. ábra: A jelszó változtatás gyakorisága Szerbiában, Magyarországon és Szlovákiában a felmérésben alapján.....	70
33. ábra: A felmérés alapján hányan használnak jelszóhasználat, ami tartalmaz kis és nagybetűket, számokat, speciális karaktereket Szerbiában, Magyarországon és Szlovákiában a felmérés alapján.....	71
34. ábra: A felmérés alapján a jelszóhasználat esetében, hogy a jelszó tartalmaz-e személyes információkat Szerbiában, Magyarországon és Szlovákiában a felmérés alapján.....	72

35.ábra: A felmérésben résztvevők a jelszóhasználatra vonatkozóan használnak-e értelmes szót.....	73
36.ábra: A jelszó hosszának a használata Szerbiában, Magyarországon és Szlovákiában a felmérés alapján.....	74
37.ábra: Ugyan az a jelszó használata a felmérés szerint Szerbiában, Magyarországon és Szlovákiában.....	75
38.ábra: A felmérés alapján a képzésen való részvétel szándéka Szerbiában, Magyarországon és Szlovákiában.....	76

FÜGGELÉK

1.számú függelék

A kérdőív magyar nyelven

Az okoseszközök használata a felhasználók körében

Készítette: Mandic Dorottya

Óbudai Egyetem Biztonságtudományi Doktori Iskola

Doktorandusz hallgató

mandic.dorottya@gmail.com

1.Neme:

- ☐ Férfi
- ☐ Nő

2.Kérem adja meg az életkorát:

- ☐ 18-24
- ☐ 25-34
- ☐ 35-50
- ☐ 51-60
- ☐ 60 felett

3.Az Ön legmagasabb iskolai végzettsége?

- ☐ Általános iskola
- ☐ Középiskola
- ☐ Főiskola/BSc
- ☐ Egyetem/MSc
- ☐ Egyéb.

4.Rendelkezik-e informatikai végzettséggel?

- ☐ Igen.
- ☐ Nem.

5.Használ-e okoseszközt/okoseszközöket? (például okostelefon, okosóra, okostévé vagy egyéb okoseszközt)

- ☐ Igen.
- ☐ Nem.

6.Kérem választja ki, hogy a felsorolt okoseszközök közül rendelkezik-e valamelyik eszközzel? (több válasz is megadható)

- ☐ Okostelefon
- ☐ Okosóra
- ☐ Okostévé
- ☐ Okosmérleg
- ☐ Okoshangszóró
- ☐ Okoscsengő
- ☐ Okoskamera
- ☐ Okosporszívó
- ☐ Egyéb okoseszköz

7.Fontosnak tartja-e, hogy olyan okoseszközt vásároljon, melynek márkája ismert?

- ☐ Igen.
- ☐ Nem.

8.A felsorolt márkák közül kérem választja ki, hogy az Ön okoseszköze/okoseszközei melyik márkához tartoznak? (több válasz is megadható)

- ☐ Samsung
- ☐ Huawei
- ☐ Xiaomi
- ☐ Google
- ☐ LG
- ☐ Apple
- ☐ Egyéb.

9.Az okoseszköz megvásárlásakor Ön mit vesz figyelembe? (több válasz is megadható)

- ☐ Ár.
- ☐ Kinézet.
- ☐ Márka.
- ☐ Biztonság.
- ☐ Minél több funkcióval rendelkezzen.
- ☐ Egyéb.

10.Utána szokott-e olvasni a megvásárolni kívánt okoseszköz termékleírásának vagy a vásárlói véleményeknek?

- ☐ Igen.
- ☐ Nem.

11.Használ-e vírusvédelmi alkalmazást?

- ☐ Igen.

- ☐ Nem.

12.Az applikációkat frissíti-e rendszeresen?

- ☐ Igen.
- ☐ Nem.

13.A firmware frissítéseket telepíti-e?

- ☐ Igen.
- ☐ Nem.

14.Milyen gyakran változtatja jelszavát?

- ☐ Napi szinten.
- ☐ Heti szinten.
- ☐ Minden hónapban.
- ☐ Félévenként.
- ☐ Évenként.
- ☐ Soha.

15.A jelszó melyet használ, tartalmaz-e kis és nagybetűket, számokat, speciális karaktereket?

- ☐ Igen.
- ☐ Nem.

16.A jelszó melyet használ, tartalmaz-e személyes információkat (például születési dátumot)?

- ☐ Igen.
- ☐ Nem.

17.A jelszó, amit használ tartalmaz-e értelmes szót?

- ☐ Igen.
- ☐ Nem.

18.Milyen hosszú a jelszó, amit használ?

- ☐ Kevesebb mint 8 karakter.
- ☐ 8-10 karakter.
- ☐ agy ennél is több karakter.

19.Ugyan azt a jelszót, használja-e több helyen?

- ☐ Igen.
- ☐ Nem.

20.Részt venne-e, ha lenne lehetősége egy ingyenes online képzésen, melyben elsajátíthatná az alapvető ismereteket arról, hogy hogyan tudná az okoseszközeit biztonságosan használni?

- ☐ Igen.
- ☐ Nem.

2.számú függelék

A kérdőív szerb nyelven

Upotreba pametnih uređaja među korisnicima

1.Pol:

- ☐ Žensko
- ☐ Muško

2.Molim vas unesite svoje godine:

- ☐ 18-24
- ☐ 25-34
- ☐ 35-50
- ☐ 51-60
- ☐ Preko 60

3.Koji je vaš nivo obrazovanja?

- ☐ Osnovna škola
- ☐ Srednja škola
- ☐ Visoka škola/BSc
- ☐ Univerzitet/MSc
- ☐ Ostalo.

4.Da li imate diplomu iz informatike?

- ☐ Da.
- ☐ Ne.

5.Da li koristite pametne uređaje?(npr.pametni telefon, pametni sat, pametni TV ili drugi pametni uređaj)

- ☐ Da.
- ☐ Ne.

6.Molim vas izaberite da li imate neki od navednih pametnih uređaja?(moguće i više odgovora)

- ☐ Pametan telefon
- ☐ Pametan sat
- ☐ Pametan tv
- ☐ Pametna vaga
- ☐ Pametan zvučnik
- ☐ Pametno zvono
- ☐ Pametna kamera
- ☐ Pametni usisivač
- ☐ Ostalo.

7.Da li smatrate kupiti pametnih uređaj poznatog brenda?

- ☐ Da.
- ☐ Ne.

8.Izaberite brend vašeg pametnog uređaja od navednih brendova.(moguće je više odgovora)

- ☐ Samsung.
- ☐ Huawei
- ☐ Xiomi
- ☐ Google
- ☐ LG
- ☐ Apple
- ☐ Ostalo.

9.Šta uzimate u obzir prilikom kupovine pametnog uređaja? (moguće je više odgovora)

- ☐ Cena.
- ☐ Izgled.
- ☐ Brend.
- ☐ Sigurnost.
- ☐ Da ima što više funkcija.
- ☐ Ostalo.

10.Da li obično čitate opis proizvoda ili recenzije kupaca za pametni uređaj koji želite da kupite?

- ☐ Da.
- ☐ Ne.

11.Da li koristite antivirusnu aplikaciju?

- ☐ Da.

- ☐ Ne.

12. Da li redovno ažurirate aplikacije?

- ☐ Da.
- ☐ Ne.

13. Da li ažurirate firmware?

- ☐ Da.
- ☐ Ne.

14. Koliko često menjate lozinku?

- ☐ Svako dnevno.
- ☐ Na nedeljnom nivou.
- ☐ Svakog meseca.
- ☐ Svaki 6 mesec.
- ☐ Svake godine.
- ☐ Nikad.

15. Da li lozinka koju koristite sadrži velika i mala slova, brojeve i specijalne znakove?

- ☐ Da.
- ☐ Ne.

16. Da li lozinka koju koristite sadrži lične podatke (kao što je datum rođenja)?

- ☐ Da.
- ☐ Ne.

17. Da li lozinka koju koristite sadrži smislenu reč?

- ☐ Da.
- ☐ Ne.

18. Koliko je duga lozinka koju koristite?

- ☐ Manje od 8 znakova.
- ☐ 8-10 znakova.
- ☐ 12 ili više znakova.

19. Da li koristite istu lozinku na nekoliko mesta?

- ☐ Da.
- ☐ Ne.

20. Da imate priliku, da li biste učestvovali u besplatnom onlajn kursu obuke gde biste mogli da naučite osnove kako da bezbedno koristite svoje pametne uređaje?

- ☐ Da.
- ☐ Ne.

KÖSZÖNETNYILVÁNÍTÁS

Szeretnék köszönetet mondani a témavezetőmnek **Dr.habil.Kiss Gábornak** az iránymutatásért és a szakmai segítségért.

Szeretném megköszönni **Prof.Dr.Rajnai Zoltánnak** a támogatását és a szakmai segítségét.

Szeretnék köszönetet mondani a Biztonságtudományi Doktori Iskolának, valamint az ott dolgozóknak és mindenkinek, aki segített és támogatott a doktori tanulmányom során.

Köszönettel tartozom még a családomnak, akik végig támogattak.