HADMÉRNÖK
BIZTONSÁGTECHNIKA

17. évfolyam (2022) 4. szám 5–16.
DOI: 10.32567/hm.2022.4.1

Bak Gerda,[1] Kovács Tibor,[2] Őszi Arnold[3]

A biometrikus azonosítás megítélése – 1. rész

Assessment of Biometric Identification – Part 1

Dr. Kovács Tibor emlékére ajánljuk

A technológiai fejlődés és a biztonság iránti igény növekedésének következtében egyre több helyen találkozhatunk a biometrikus azonosítás különböző módjaival; jelen van az okostelefonokban, illetve számos vállalkozás is alkalmazza, felismerve annak előnyeit.

Jelen tanulmány azt hivatott felmérni, hogy a felhasználók körében a biometrikus azonosításról milyen vélemények alakultak ki, illetve miként vélekednek ezekről a módszerekről. A kutatás jelentősége abban rejlik, hogy 2006-ban és 2014-ben az Óbudai Egyetem keretein belül már lezajlott két hasonló céllal megfogalmazott kutatás, amelyet a jelen kutatás során igyekeztünk folytatni, valamint továbbvinni.

Az első rész a felmérés azon részét hivatott bemutatni, amely a megkérdezettek biometrikus azonosítási rendszerek ismertségével és használatával foglalkozik. Az eredmények alapján elmondható, hogy a biometrikus azonosítás kapcsán a felhasználók ismeretei bővítésre szorulnak, mivel még mindig sokan csak használják ezeket a technológiákat a hozzá tartozó tudásanyag és tudatosság nélkül.

Kulcsszavak: **biometrikus azonosítás, megítélés, elfogadottság, 2006, 2014, 2021**

Nowadays, biometric identification is becoming more and more common, as it is present in smartphones and is also used by many businesses that recognise its benefits.

[1] Óbudai Egyetem Biztonságtudományi Doktori Iskola, e-mail: bak.gerda@uni-obuda.hu
[2] Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, e-mail: kovacs.tibor@bgk.uni-obuda.hu
[3] Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, e-mail: oszi.arnold@bgk.uni-obuda.hu

This study aims to assess the perceptions and opinions of users on biometric identification. The significance of the research lies in the fact that two studies with similar aims were conducted in 2006 and 2014, also at Óbuda University, which we tried to continue and further develop in the present research.

The first part presents the part of the survey dealing with respondents' awareness and use of biometric identification systems. Based on the results, it can be said that the users' knowledge of biometric identification needs to be expanded, as many people still simply use these technologies without the corresponding knowledge and awareness.

Keywords: **biometric identification, perception, acceptance, 2006, 2014, 2021**

1. Bevezetés

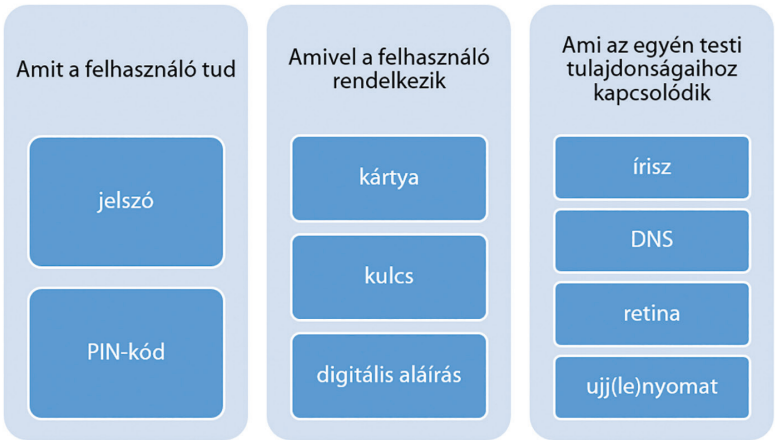
A biometrikus azonosítás iránti igény az elmúlt években megsokszorozódott, amit mi sem bizonyít jobban, mint a rendszer elterjedtsége, sokrétű felhasználtsága és a biometrikus rendszerek piaci részesedése. A Statista[4] adatai alapján a digitális személyazonosítási rendszerek piaci értéke a következő évek során a kétszeresére nő, ami közel 50 milliárd dollárt jelent világszerte, továbbá a biometrikus rendszerekre költött összeg 2025-re globálisan elérheti a 68,6 milliárd dollárt is.

Azonban a biometrikus rendszerek adta kényelemnek számos kockázata is van: az egyes szenzorok megtéveszthetők, az egyén biometrikus adatait tároló adatbázis vagy akár a hálózat célpontja lehet a támadóknak.[5] Az IBM[6] online felméréséből kiderül, hogy bár a megkérdezettek számára fontos a kényelem a különböző applikációkba és alkalmazásokba történő bejelentkezés során, a biztonságot fontosabbnak ítélik meg. Az is kiderült, hogy a megkérdezettek 67%-ának nem okoz gondot valamilyen biometrikus azonosítási módot alkalmazni, 44%-uk az ujjnyomatot mint azonosítási módot tekinti a legbiztonságosabbnak, illetve a pénzügyi alkalmazások kapcsán tekintik igazán lényegesnek a biztonságot, a közösségi média applikációinak esetében pedig a kényelmes, gyors bejelentkezés a fő szempont.

A felhasználók azonban hajlamosak egyszerű, könnyen megjegyezhető jelszavakat, PIN-kódokat használni, amelyeket viszonylag ritkán változtatnak meg, ezzel is növelve a kockázatot.[7]

A digitális technológia fejlődésével és használatával számos információ keletkezik, valamint tárolódik a számítógépeken, telefonokon vagy akár az interneten egyetlen nap leforgása alatt is. Ezeket a tartalmakat pedig érdemes, sőt ajánlott gondosan őrizni, jelszavakkal, azonosítókkal védeni. A jelenlegi technológiát tekintve három azonosítási, hitelesítési módot különböztetünk meg, illetve létezik egy negyedik is, azonban az csak az ötvözete az első két módnak, ezt mutatja be a következő, 1. ábra.

[4] Liu 2021.
[5] Földesi 2015; Rui–Yan 2019; Dargan–Kumar 2020.
[6] IBM 2021.
[7] Shen–Chen–Guan 2018.



1. ábra: Az egyén azonosítási módjainak típusai
Forrás: a szerzők szerkesztése Datta et al. 2020 és Szűcs–Őszi–Kovács 2020 alapján

Jelen kutatás a következőkben a felsorolás utolsó, vagyis az egyén fizikai sajátosságaival foglalkozó azonosítási módokra terjed ki.

2. Biometrikus azonosítás

A biometrikus azonosítás az emberek automatikus hitelesítését jelenti fiziológiai vagy viselkedésbeli jellemzőik vagy tulajdonságaik alapján.[8] A viselkedésbeli jellemzők egyik jelentős hátránya, hogy az idő előrehaladtával változhatnak (mutálódik a hang, változik az aláírás képe, dinamikája), ezzel szemben a fizikai tulajdonságaink, mint az ujj(le)nyomat, nem, mint ahogy a DNS-ünk sem.[9] Azonban a fiziológiai jellemzőknek is van néhány hátránya. Először is, másolhatók: az ujjlenyomatok és a kézgeometria könnyen újraalkotható;[10] másodszor, a fiziológiai jellemzők külső hatásra könnyen torzulnak vagy megváltoznak (például a hegek vagy zúzódások megváltoztatják az ujjlenyomatokat, az arc különböző pózai összezavarhatják az arcfelismerő rendszert);[11] harmadszor, a fiziológiai jellemzők mindig speciális hardveres támogatást igényelnek. Másrészt az okostelefonokban rendelkezésre álló különféle szenzorok, például az érintőképernyő és a mozgásérzékelők képesek átfogó információk hatékony gyűjtésére. Ezért a viselkedésbeli biometria az okostelefon-hitelesítés egyik kutatási fókuszpontjává vált.[12]

A biometrikus rendszerek kapcsán a szakirodalom különbséget tesz az unimodális és a multimodális rendszerek között: míg az unimodális rendszer egyetlen biometrikus tulajdonság alapján hitelesíti, értékeli a felhasználót, addig a multimodális kettő vagy több biometrikus jellemző alapján végzi el ugyanezt, ezzel is növelve a rendszer

[8] Flynn–Jain–Ross 2008; Hazai 2019.
[9] Sarhan–Alhassan–Elmougy 2016.
[10] Tamviruzzaman et al. 2009.
[11] Jain–Ross–Prabhakar 2004.
[12] Shen–Chen–Guan 2018. 9.

megbízhatóságát és pontosságát.[13] Az unimodális rendszerek hátránya lehet a nem megfelelő állapotban tartott érzékelő, aminek következtében a szenzor deformált vagy zajos adatokat eredményezhet, illetve a megkülönböztethetőség is gondot okozhat a rendszernek: a felhasználó nem megfelelő módon lép interakcióba a szenzorral (nem jól tartja az ujját az érzékelőhöz, túl közel vagy távol áll stb.), vagy a felhasználók körének növekedésével előforduló hasonló karakterisztikájú egyének átfedéseket okozhatnak, ami ronthatja a rendszer pontosságát.[14]

A fenti problémák mellett az unimodális biometrikus rendszerek további hátrányokkal is küzdenek, ezek a problémák pedig magasabb hamis elutasítási arányhoz (*false reject rate,* FRR) és hamis elfogadási arányhoz (*false accept rate,* FAR) vezetnek.[15] A biometrikus azonosító rendszerek pontosságának, teljesítményének értékelésére az előbb említett két mutatón kívül még létezik az egyenlő hibaarány (*equal-error rate,* ERR), ami azt a pontot jelöli, ahol az FRR és FAR értéke egyenlő.[16]

3. Módszertan

A kutatáshoz kérdőíves vizsgálati módot alkalmaztunk, amelynek adatbegyűjtési időszaka 2021. október 23. – 2021. december 12. közé esett, hólabda módszerrel. A kérdőívet online és papír formában is terjesztettük, ami 209 kitöltést eredményezett. Az adatok nem tekinthetők reprezentatívnak, elemzésük IBM SPSS 26 programmal történt.

A kérdőív két fő részből tevődött össze: az általános demográfiai részből és a biometrikus azonosítással kapcsolatos részből. A kérdések zárt formában, illetve Likert-skála segítségével voltak megválaszolhatók.

A kutatás legelején négy fő kérdés fogalmazódott meg, amelyek a következőkben láthatók. A negyedik, egyben utolsó kutatási kérdésre a tanulmány második részében kapnak helyet az eredmények.

Kutatási kérdések:

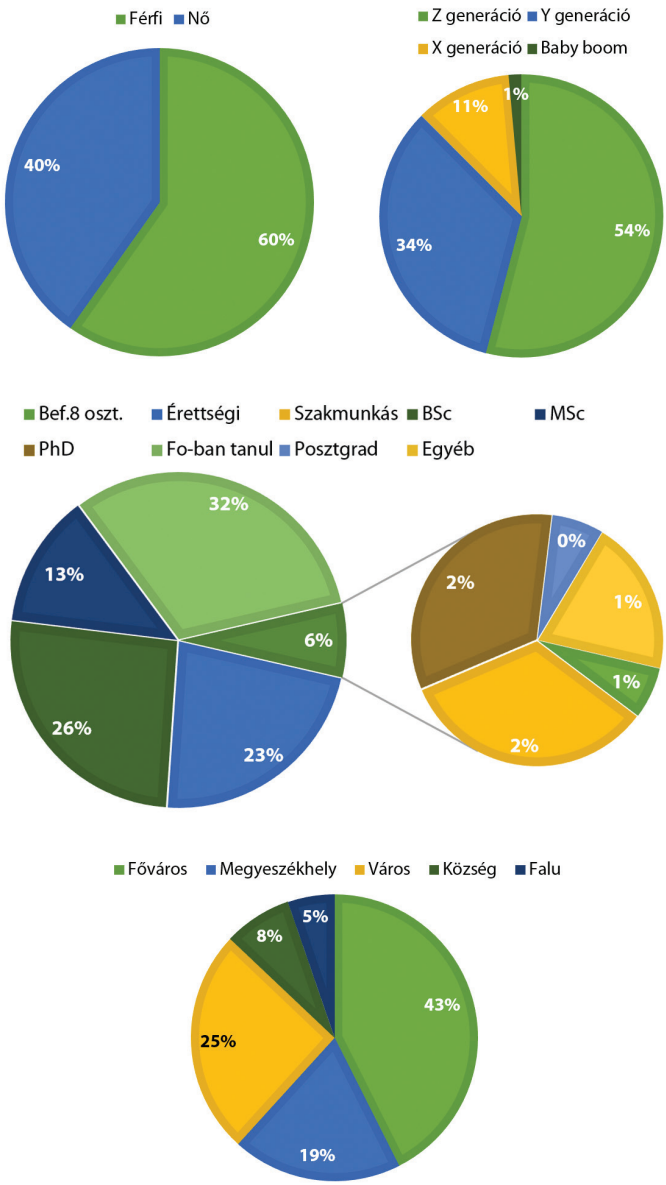
- Mely biometrikus azonosítási rendszereket használják a hétköznapokban az okostelefonjaikon?
- Mennyire elfogadottak ezek a rendszerek a hétköznapokban?
- Van-e különbség a biometrikus azonosítási rendszerek megítélésében a nemek tekintetében?
- Miként vélekednek az emberek a biometrikus azonosítási rendszerekről?

3.1. Minta bemutatása

A kérdőív kitöltőiről nemek szerinti bontásban elmondható, hogy a férfiak nagyobb arányban (60%), főként Z generációs fiatalok (54%) töltötték ki, akik jelenleg is a felsőoktatásban tanulnak (Fo.-ban tanul) (32%), illetve többségében a fővárosban (43%)

[13] Ammour–Bouden–Boubchir 2018.
[14] Gad et al. 2015.
[15] Kovács–Földesi 2021; Devi–Sujatha 2017.
[16] Fejes 2018.

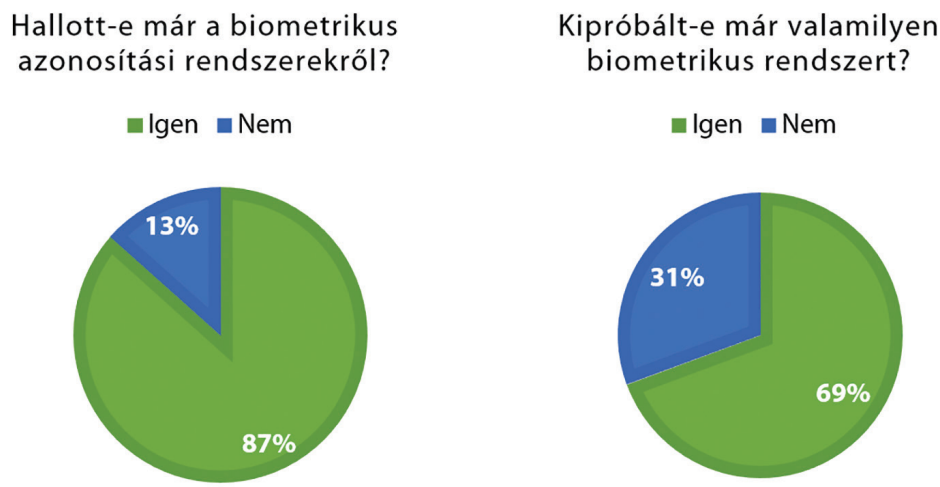
laknak. A kitöltők leíró statisztikai jellemzőit a 2. ábra foglalja össze. A kitöltők között legkisebb arányban a baby boom generáció képviselte magát. A képzettséget tekintve a befejezett 8 osztállyal rendelkezők, a posztgraduális képzést végzettek, a szakmunkásban tanultak, valamint az egyéb képzést végzők szerepeltek alacsony arányban. A lakhelyet tekintve pedig a faluban és községben élőkhöz jutott el kis arányban a kérdőív.



2. ábra: A kérdőív kitöltőinek leíró statisztikája (n = 209)
Forrás: a szerzők szerkesztése a minta adatai alapján

4. Eredmények

A kérdőív első felében megkérdeztük, hogy a kitöltők hallottak-e már róla, illetve kipróbáltak-e már valamilyen biometrikus azonosítási rendszert. Az alábbi, 3. ábra ennek a két kérdésnek az eredményeit mutatja be. Ahogy az látható, a kitöltők 87%-a hallott már erről, illetve 69%-uk ki is próbált már legalább egy biometrikus azonosítási módot.



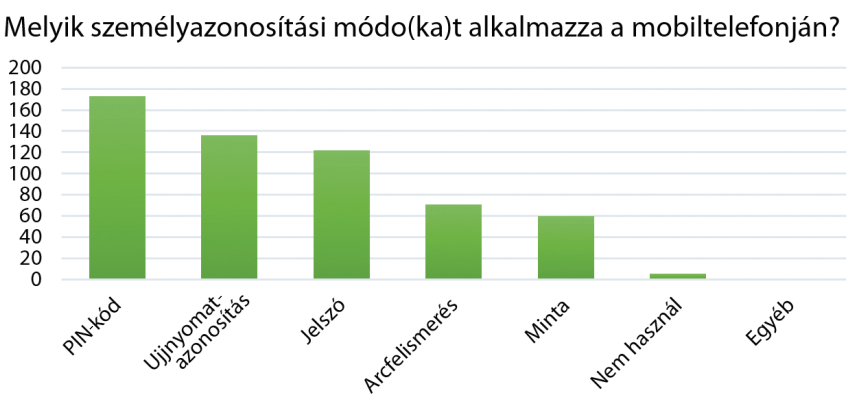
3. ábra: A kitöltők megoszlása aszerint, hogy hallottak-e róla, illetve kipróbáltak-e már valamilyen biometrikus azonosítási módszert (n = 209)

Forrás: a szerzők szerkesztése a minta adatai alapján

Az előbb ábrázolt eredmények két szempontból is jelentősek, illetve érdekesek. Egyrészt érdekesek, mivel a kérdőív további részében, amikor arra kerestük a választ, hogy a megkérdezettek milyen azonosítási módokról hallottak, akkor a kitöltők kivétel nélkül minimum egy azonosítási formát jelöltek az előre megadott opciók közül. Továbbá arra is kerestük a választ, hogy a mobiltelefonjukon milyen azonosítási módo(ka)t alkalmaznak: néhány (5 db) válaszadó kivételével mindegyik alkalmaz valamit. A 4. és 5. ábra az előbb tárgyalt két kérdésre adott válaszokat mutatja be. Mind a két kérdés esetén több válasz megjelölése is lehetséges volt. Ahogy azt az ábra is mutatja, a legismertebb azonosítási módszer az ujjnyomat-azonosítás, amelyet 208 kitöltő ismer, ezt követi a PIN-kód 204 és a jelszó 203 jelöléssel. Az előre felsorolt azonosítási módok közül a legkevésbé ismert a DNS-azonosítás, 92 fő nyilatkozta a módszer ismeretét. A válaszokat tekintve az *egyéb* opciót is jelölhették a kitöltők, ahol megnevezhettek további, számukra ismert módozatokat is. Az egyebek között az írisz-, retinavizsgálat, vénaszkenner fordultak elő többnyire, de említették az aláírást és a mozgáselemzést is.

4. ábra: A válaszadók által ismert személyazonosítási módok (n = 209)
Forrás: a szerzők szerkesztése a minta adatai alapján

A válaszadók által a mobiltelefonokon alkalmazott azonosítási módokat ábrázolja az 5. ábra, itt is több válaszadási lehetőség volt. Látható, hogy a leggyakoribb azonosítási módszer a megkérdezettek körében a PIN-kód 173 válaszadóval, ezt követi 136 jelöléssel az ujjnyomatos feloldás, illetve 122 jelöléssel a jelszó. A legkevésbé előnyben részesített mobiltelefon-feloldási mód a minta, amelyet 60 válaszadó alkalmaz, továbbá 5 kitöltő úgy nyilatkozott, hogy nem használ semmilyen feloldási módot, vagyis bárki feloldhatja a mobiltelefonját. Az általunk előre megadott azonosítási módok mellett a kitöltőknek természetesen lehetőségük volt megnevezni egyéb azonosítási módot is, amennyiben azt alkalmazzák az okostelefonjukon; egy válaszadó jelezte, hogy ő egy általunk nem nevesített módszert is használ, méghozzá a QR-kódos azonosítást.

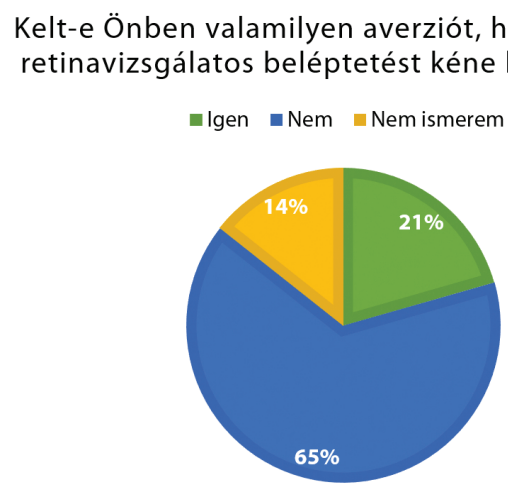


5. ábra: A válaszadók által személyazonosításra használt mobiltelefon-feloldási módok (n = 209)
Forrás: a szerzők szerkesztése a minta adatai alapján

A kérdőív biometrikus azonosítási rendszerek elfogadottságát vizsgáló része előtt négy olyan kérdést tettünk fel a kitöltőknek, amelyek egyrészt átvezetésül szolgálnak a mélyebb kérdésekhez, másrészt a segítségükkel általános képet kaphatunk a felhasználók biometrikus azonosítási módszerekkel szembeni véleményéről és hozzáállásáról. Az említett kérdések esetében, az első kivételével, ötfokozatú Likert-skálán kellett a válaszadóknak jelölniük a válaszukat. A négy kérdés a következő:

- Keltene-e önben valamilyen averziót, ha írisz- vagy retinavizsgálatos beléptetést kellene használnia?
- Általában mennyire tartja korszerűnek a biometrikus azonosításon alapuló beléptetési lehetőséget?
- Ön szerint mennyire könnyű/egyszerű egy biometrikus rendszer használata?
- Mennyire találja gyorsnak a biometrikus azonosítási folyamatot?

A fentebb említett kérdések közül az elsőre – azaz, hogy kelt-e bennük bármilyen kellemetlen, rossz érzést az írisz- vagy retinavizsgálatos beléptetési módszer alkalmazása – adott válaszokat szemlélteti a 6. ábra. Az eredmények alapján elmondható, hogy a megkérdezettek több mint a felét (65%) nem töltené el rossz érzés, ha az írisz- vagy retinavizsgálatos beléptetési módszert kellene használniuk. Ezzel szemben 21%-ot zavarna, valamint 14% a saját elmondása alapján nem ismeri a fent nevezett módszert.

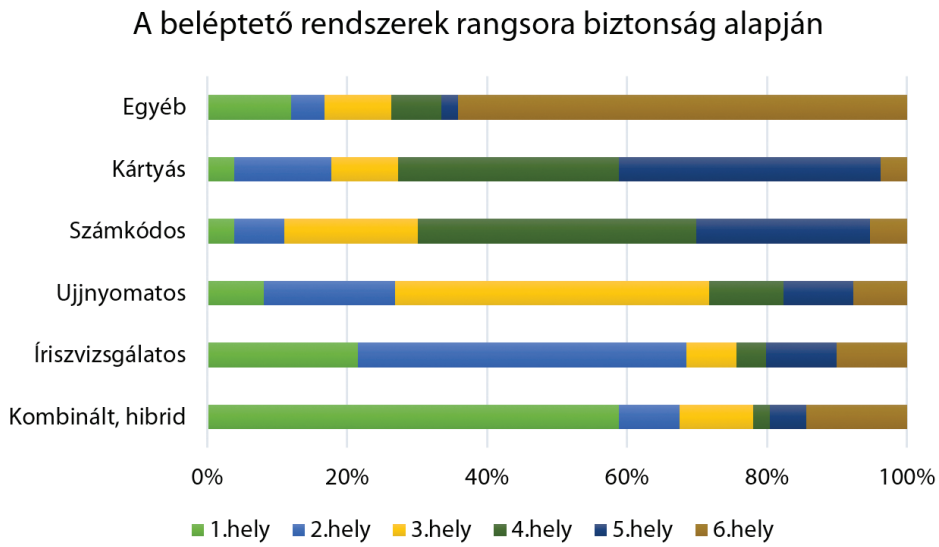


6. ábra: Írisz- vagy retinavizsgálatos beléptetéssel szembeni averzió megjelenése a válaszadók körében (n = 209)

Forrás: a szerzők szerkesztése a minta adatai alapján

A kérdőív során arra kértük a kitöltőket, hogy rangsorolják az egyes biometrikus azonosítási módokat aszerint, hogy melyiket tartják a legbiztonságosabbnak és melyiket a legkevésbé. A 7. ábra ennek eredményeit mutatja be. Az eredmények értelmében elmondható, hogy a megkérdezettek közel 60%-a (58,85%) a kombinált, hibrid módszereket ítéli meg a legbiztonságosabbnak, ezt követi az íriszvizsgálat 46,89%-kal,

az ujjnyomatos 44,98%-kal, a legkevésbé biztonságosnak az egyéb beléptetési módot jelölték 64,11%-kal.



7. ábra: Az egyes biometrikus beléptetési rendszerek megítélése biztonság szempontjából (n = 209)
Forrás: a szerzők szerkesztése a minta adatai alapján

5. Következtetések

A jelen kutatási részt tekintve az látható, hogy a felhasználók sokrétűen és elterjedten használják a biometrikus azonosítási rendszereket. Az eredmények tükrében elmondható, hogy az általunk megkérdezettek körében is nagy elfogadottságnak örvendenek a biometrikus azonosítási módok, különös tekintettel az okostelefonokon. Hayiel Hino az online vásárlás kapcsán vizsgálta, hogy mely tényezők befolyásolják a biometrikus azonosítás elfogadottságát, és arra a következtetésre jutott, hogy többek között az észlelt adatvédelem mértéke, a társadalmi befolyás és a technológiával való ismeretség (tapasztalat) jelentősek. A megkérdezettek szinte mindegyike kettő vagy több azonosítási módról hallott, illetve használja is. A különböző beléptető rendszerek, valamint az azokról alkotott biztonsági megítélés is a többség esetében megfelelő.[17] Lauren Norfolk és Michael O'Regan kutatása hasonló eredményeket hozott; a szerzőpáros az ujj(le)nyomat használatának elfogadottságát vizsgálta a zenei fesztiválokon, ahol a válaszadók majdnem 71%-a vélekedett úgy, hogy szívesen használná, 68,5%-uk az arcfelismerőt is komfortosnak tekinti.[18] Michele Cornacchia,

[17] Hino 2015.
[18] Norfolk–O'Regan 2020.

Filomena Papa és Bartolomeo Sapio szintén speciális közönséget vizsgálva jutott hasonló eredményekre; kutatásuk a hangazonosító rendszerek alkalmazásának elfogadottságát mérte a Milánó-Linatei nemzetközi repülőtéren, ahol a megkérdezettek szintén pozitívan viszonyultak a rendszerhez, elfogadhatónak tartották a használatát.[19]

6. Összefoglalás

A kutatás eredményei alapján elmondható, hogy bár a különféle biometrikus azonosítási módszerek rendkívül elterjedtek, a felhasználók egy része csak használja azokat, a használat mögül pedig hiányzik a kellő tudatosság. Ezt támasztja alá az is, hogy a válaszadók nagy része a saját mobiltelefonja feloldásához is biometrikus azonosítási módot használ (ujjnyomat-azonosítás, arcfelismerés), mégis, közülük sokan azt nyilatkozták, hogy még nem próbáltak ki egyetlen biometrikus azonosítási rendszert sem. Az eredmények másik érdekességét az adja, hogy a biometrikus rendszerek biztonság szerinti rangsorolásánál helyesen jelölték a kitöltők, hogy a kombinált, hibrid rendszerek számítanak a legbiztonságosabbnak, megelőzve az ujjnyomatos, illetve a kártyás módokat, amelyek megtéveszthetőbbek, illetve a kártya sérülékenyebb és el is tulajdonítható. Ez viszont azt feltételezi, hogy bizonyos információkkal, tudással rendelkeznek a témában, még ha akadnak is hiányosságok, illetve az egyes kifejezések kapcsán is érdemes lenne rendet tenni.

Az eredmények alapján megállapítható, hogy az általunk megkérdezettek igénylik és használják is a különféle azonosítási módokat, amelyek révén növelhetik adataik, személyük és mobiltelefonjuk biztonságát. Azonban a biometrikus azonosítási módok általánosítása területén hatalmas eltérések találhatók. Az azonosítási módok megítélése pozitív, nyitottak a használatukra, ám az egyének a biometrikus adataik rögzítése kapcsán már negatívabban vélekednek.

Felhasznált irodalom

Ammour, Basma – Bouden, Toufik – Boubchir, Larbi (2018): Face-Iris Multimodal Biometric System Based on Hybrid Level Fusion. In *2018 41st International Conference on Telecommunications and Signal Processing (TSP)*. IEEE. 1–5. Online: https://doi.org/10.1109/TSP.2018.8441279

Cornacchia, Michele – Papa, Filomena – Sapio, Bartolomeo (2020): User Acceptance of Voice Biometrics in Managing the Physical Access to a Secure Area of an International Airport. *Technology Analysis & Strategic Management,* 32. évf. 10. sz. 1236–1250. Online: https://doi.org/10.1080/09537325.2020.1758655

Dargan, Shaveta – Kumar, Munish (2020): A Comprehensive Survey on the Biometric Recognition Systems Based on Physiological and Behavioral Modalities. *Expert Systems with Applications,* 143. évf. 113114. Online: https://doi.org/10.1016/j.eswa.2019.113114

[19] Cornacchia–Papa–Sapio 2020.

Datta, Priyanka – Bhardwaj, Shanu – Panda, S. N. – Tanwar, Sarvesh – Badotra, Sumit (2020): Survey of Security and Privacy Issues on Biometric System. In *Handbook of Computer Networks and Cyber Security.* Cham, Springer. 763–776. Online: https://doi.org/10.1007/978-3-030-22277-2_30

Devi, R. Subathra – Sujatha, Pothula (2017): A Study on Biometric and Multi-Modal Biometric System Modules, Applications, Techniques and Challenges. In *2017 Conference on Emerging Devices and Smart Systems (ICEDSS).* IEEE. 267–271. Online: https://doi.org/10.1109/ICEDSS.2017.8073691

Fejes Attila (2018): Beszéd alapján történő személyazonosítás új kihívásai a kriminalisztikában. *Magyar Rendészet,* 18. évf. 2. sz. 117–126.

Flynn, Patrick J. – Jain, Anil K. – Ross, Arun A. (2008): Introduction to Biometrics. In *Handbook of Biometrics.* Boston, MA, Springer, 2008, 1–22.

Földesi Krisztina (2015): Paradigmaváltás a biztonságtechnikában — miért alkalmazzunk biometrikus rendszert? *Magyar Rendészet,* 15. évf. 3. sz. 37–48.

Gad, Ramadan – El-Sayed, Ayman – El-Fishawy, Nawal – Zorkany, M. (2015): Multi-Biometric Systems: A State of the Art Survey and Research Directions. *(IJACSA) International Journal of Advanced Computer Science and Applications,* 6. évf. 6. sz. 128–138. Online: https://doi.org/10.14569/IJACSA.2015.060618

Hazai Lászlóné (2019): Módszerek, technikák a biometrikus arcfelismerésben, -azonosításban. *Belügyi Szemle,* 67. évf. 1. sz. 118–126. Online: https://doi.org/10.38146/BSZ.2019.1.9

Hino, Hayiel (2015): Assessing Factors Affecting Consumers' Intention to Adopt Biometric Authentication Technology in E-shopping. *Journal of Internet Commerce,* 14. évf. 1. sz. 1–20. Online: https://doi.org/10.1080/15332861.2015.1006517

IBM (2018): IBM Security: Future of Identity Study. *IBM*, 2021. december 10. Online: www.ibm.com/downloads/cas/PL9VJ9KV

Jain, Anil K. – Ross, Arun – Prabhakar, Salil (2004): An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology,* 14. évf. 1. sz. 4–20. Online: https://doi.org/10.1109/TCSVT.2003.818349

Kovács Tibor – Földesi Krisztina (2021): Összehasonlító kutatáselemzés a biometrikus személyazonosító-beléptető rendszerek, eljárások 2006. és 2014. évi társadalmi averzív reakcióinak vizsgálatára. *SecureInfo,* 2021. december 10. Online: www.securinfo.hu/wp-content/uploads/2015/06/20150602_osszehasonlito_elemzes_a_biometrikus_szemelyazonosito_rendszerek.pdf

Liu, Shanhong (2021): Biometric Technologies – Statistics & Facts. *Statista,* 2021. október 30. Online: www.statista.com/topics/4989/biometric-technologies/#dossierKeyfigures

Norfolk, Lauren – O'Regan, Michael (2020): Biometric Technologies at Music Festivals: An Extended Technology Acceptance Model. *Journal of Convention & Event Tourism,* 22. évf. 1. sz. 36–60. Online: https://doi.org/10.1080/15470148.2020.1811184

Rui, Zhang – Yan, Zheng (2019): A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification. *IEEE Access,* 7. évf. 5994–6009. Online: https://doi.org/10.1109/ACCESS.2018.2889996

Sarhan, Shahenda – Alhassan, Shaaban – Elmougy, Samir (2016): Multimodal Biometric Systems: A Comparative Study. *Arabian Journal for Science and Engineering,* 42. évf. 2. sz. 443–457. Online: https://doi.org/10.1007/s13369-016-2241-0

Shen, Chao – Chen, Yufei – Guan, Xiaohong (2018): Performance Evaluation of Implicit Smartphones Authentication via Sensor-Behavior Analysis. *Information Sciences,* 430–431. évf. 538–553. Online: https://doi.org/10.1016/j.ins.2017.11.058

Szűcs, Kata Rebeka – Őszi, Arnold – Kovács, Tibor (2020): Mobile Biometrics and their Risks. *Hadmérnök,* 15. évf. 4. sz. 15–28. Online: https://doi.org/10.32567/hm.2020.4.2

Tanviruzzaman, Mohammad – Ahamed, Sheikh Iqbal – Hasan, Chowdhury Sharif – O'Brien, Casey (2009): ePet: When Cellular Phone Learns to Recognize Its Owner. In *SafeConfig '09: Proceedings of the 2nd ACM Workshop on Assurable and Usable Security Configuration.* ACM. 13–18. Online: https://doi.org/10.1145/1655062.1655066