Óbudai Egyetem

Doktori (PhD) értekezés

Biometriaalapú beléptető rendszerek alkalmazhatósága tömegtartózkodású helyeken

Otti Csaba

Prof. Dr. Kovács Tibor, egyetemi docens

Biztonságtudományi Doktori Iskola

Budapest, 2019.

Szigorlati Bizottság:

Elnök:

Prof. Dr. Berek Lajos, egyetemi tanár (ÓE)

Tagok:

Dr. Hanka László, adjunktus (ÓE)

Dr. habil. Simon Ákos ny. egyetemi docens (külső)

Nyilvános védés bizottsága:

Elnök:

Prof. Dr. Berek Lajos, egyetemi tanár (ÓE)

Titkár:

Dr. Szűcs Endre, egyetemi docens (ÓE)

Tagok:

Dr. habil. Simon Ákos ny. egyetemi docens (külső)

Dr. Kiss Sándor ny. egyetemi docens (külső)

Dr. habil. Farkas Tibor egyetemi docens (külső - NKE)

Bírálók:

Dr. Nagy Rudolf, adjunktus (ÓE)

Dr. Balla József egyetemi docens, (külső – NKE)

Nyilvános védés időpontja

……..

TARTALOMJEGYZÉK

BEVEZETÉS

"It is the purpose of this article to present, together with some evidence of its feasibility, a method by which decentralized automatic identity verification, such as might be desired for credit, banking or security purposes, can be accomplished through automatic comparison of the minutiae in finger-ridge patterns."[1] [115]

Magyarországon az 1990-es évek végén kezdett a biztonsági szakma megismerkedni a biometrikus adatokon alapuló személyazonosítási rendszerekkel. Az egyik vállalkozás a Guardware Kft. volt, amely a világon elsőként – messze megelőzve a versenytársakat – fejlesztett élőujj-felismeréssel ellátott ujjnyomat-azonosító eszközöket. A másik piaci szereplő a német–magyar tulajdonú Login Autonom Kft., amely külföldön gyártott rendszereket terjesztett el a magyar piacon. A technológiák között szerepeltek ujjnyomat-azonosító, hangfelismerő, írisz- és kézgeometria-azonosító rendszerek is. Én a Kandó Kálmán Műszaki Főiskola elvégzése után 1998-ban ennél a cégnél ismerkedtem meg a biometrikus azonosítási eljárásokkal, mint projekttámogató mérnök. A kezdetben forgalmazott öt gyártó mintegy tíz megoldása közül a gyakorlatban mindössze kettő működött, az egyik a Crossmatch által felvásárolt Digital Persona Magyarországról már nem elérhető számítógépes beléptetést megvalósító ujjnyomat-azonosítója, a másik a Recognition Systems kézgeometria felismerője volt. A teszteket akkor még tudományos megközelítés nélkül hajtották végre a vállalatnál dolgozó mérnökök, egyszerűen a gyártói specifikáció szerint telepítették egy valós alkalmazásban, és a felhasználói eredmények alapján alkalmazták a rendszert.

Akkor még nem értettük az okát,[2] de klasszikusan biztonságosnak vélt körülmények között (banki, IT-, telekomszektorok) nem volt komoly érdeklődés a biometrikus megoldásokra, azonban termelő (ipari) vállalatok szívesen alkalmazták beléptetési és munkaidő-nyilvántartási célokra. Ezeken a tendereken rendszeres volt az a pályázói felosztás, hogy legalább az egyik ajánlatadó ujjnyomatolvasókkal indult, mi pedig a kézgeometria-azonosítókkal. A tesztjeink alapján pontosan

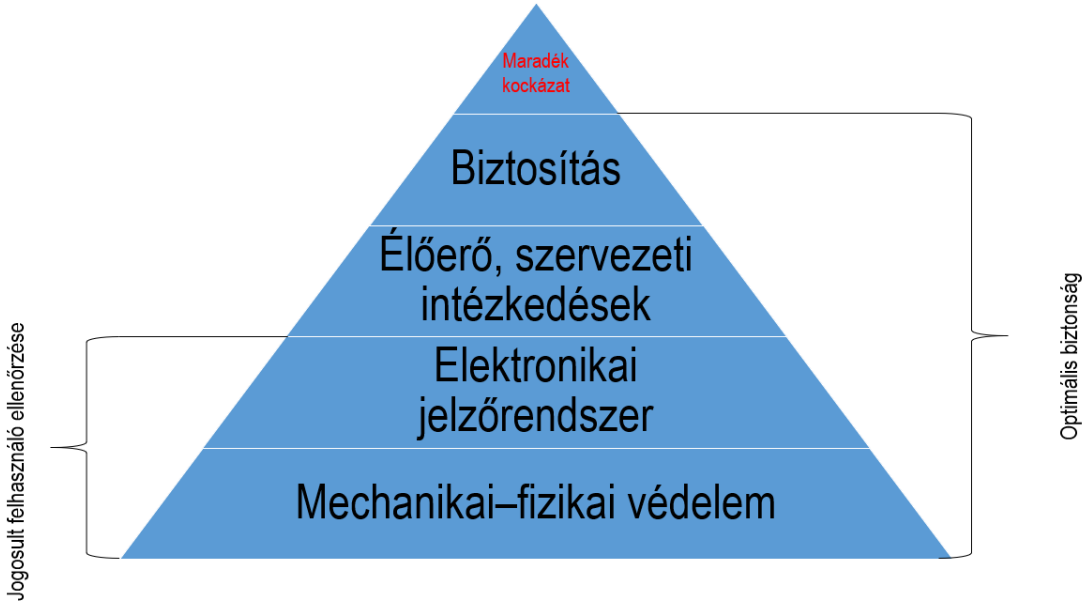
[1] Mitchell Trauring, *Nature,* 1963. március. Az első tudományos dolgozat, amelyet publikáltak az automatikus ujjnyomat-azonosításról: *„Jelen cikk célja, hogy bemutasson és példákkal szemléltessen egy olyan módszert, amely az ujjlenyomat fodorszálak aprólékos vizsgálatával és automatikus felismerésével teszi lehetővé a decentralizált automatikus személyazonosítást. Ez rendkívül hasznosnak bizonyulhat banki és hitelügyintézés, valamint biztonsági ellenőrzések során."*

[2] A vonatkozó szabványok (pl. ISO27001, PCI DSS) megfelelő biztonsági szinten ugyan előírják a kétfaktoros azonosítást, de erre bőven megfelel a kártya + PIN-kód is. Termelő környezetben viszont sokkal fontosabb, hogy valóban az embert azonosítsák.

tudtuk, hogy termelői környezetben nem fog működni az ujjnyomatolvasó, de ez a döntéshozóknak nem volt nyilvánvaló. Az adatlapok, a szállító véleménye vagy csupán a kis létszámú tesztek alapján döntöttek a bevezetésről. Ennek eredményeképp számos sikertelen rendszerbevezetés történt, ahol az üzleti döntéshozók csalódtak a biometriában, függetlenül attól, hogy a kiválasztott eszköz eleve alkalmatlan volt az adott körülmények közötti megfelelő működésre. A 2000-es évek elején kezdtem el együtt dolgozni és gondolkodni prof. dr. Kovács Tiborral, jelenlegi témavezetőmmel, azon, hogyan lehet egységes szakterminológia használatát elősegíteni, amely hozzájárul a biometrikus adatokon alapuló személyazonosítási rendszerek következetes, azonos elveken alapuló alkalmazásához. Vajon lehet hiteles tájékoztatást adni a biztonsági szakembereknek a különböző technológiák és eszközök gyakorlati alkalmazhatóságáról? Ennek eredményeképpen jött létre 2011-ben az Óbudai Egyetem keretein belül az Applied Biometrics Institute, röviden ABI (www.abibiometrics.org), amely felvállalta ezt a tevékenységet.

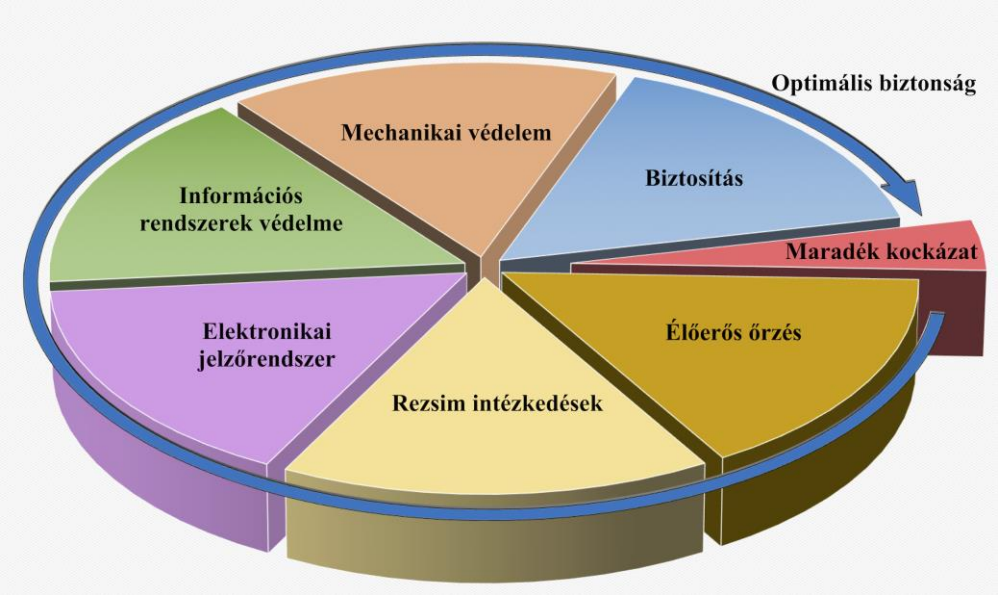
A tudományos probléma megfogalmazása

A magánbiztonság megteremtésének egyik elsődleges feladata a hozzáférési jogosultság hiteles eldöntése egy személyről, akár egy objektumba vagy területre történő fizikai belépésről, akár egy adathoz vagy információhoz történő hozzáférésről van szó. [1] A fizikai biztonság hagyományos ábrázolása a védelmi háromszöggel történik (1. ábra). Alsó két szintjén, a mechanikai és elektronikai védelem feloldásához a jogosult felhasználó szükséges. [2] [3]



1. ábra: Védelmi háromszög; [3] alapján

Ez a felépítés azonban félrevezető lehet, mivel azt sugallja, hogy méretbeli vagy fontosságbeli megkülönböztetés van az egyes szintek között. A fizikai biztonság területeit eredményesebben és holisztikusabban mutatja meg a védelmi kör:



2. ábra: Védelmi kör; forrás: [4]

Informatikai biztonság és információbiztonság tudományágaiban a három alapelv, a bizalmasság, sértetlenség és rendelkezésre állás megvalósításánál az elsőnél kell garantálni a hozzáférés jogosultságát. [5] [6]

Az elektronikus jogosultság hagyományos, tudás- és birtokalapú azonosítása mellett a technológia fejlődésével előtérbe került a felhasználók hiteles, automatikus, egyedi testi jellemzőin alapuló, azaz biometrikus azonosítási igénye.

Doktori értekezésem a biometrikus felhasználói azonosítás alkalmazhatóságát elemzi tömegtartózkodású objektumok esetében.

A biometrikus azonosítás bevezetésére számos oka lehet egy entitásnak, azonban minden ilyen ok egy közös elvárásra vezethető vissza: egy adott személy pontos azonosításának igényére egy, a személyhez közvetlenül és elválaszthatatlanul tartozó tulajdonsággal. Napjainkban egyre nagyobb igény mutatkozik az emberek egyértelmű azonosíthatósága iránt – tekintetbe véve, hogy a globális biztonsági helyzet egyre romlik. Az elmúlt időszakban nyilvánosságra került hackertámadások, felhasználó-, jelszó- és identitáslopások pedig egy jobb megoldás alkalmazását igénylik. A biztonsági és egyéb, például kereskedelmi és marketing igények miatt a biometrikus azonosításra egyre inkább szükség van – azonban nem mindegy, hogy melyik alkalmazáshoz

milyen technológiát és eszközt választunk ki. Esettanulmányok alapján elmondható, hogy napjainkban sincs jól használható keretrendszer a biometrikus rendszerek vállalatokhoz történő bevezetésére, amely alapján kiválasztható, értékelhető és megvalósítható a legjobb megoldás. A különböző biometrikus adatokon alapuló azonosítási technológiák, a legismertebb ujjnyomat-azonosítástól a legbiztonságosabbnak tekintett íriszfelismerésig sem alkalmasak minden feladatra, ezért szükséges a MOA[3] megközelítéssel elemezni minden tipikus alkalmazást. [7]

Feltevésem szerint kialakítható egy olyan szempontrendszer, amely képes lefedni a lehetséges alkalmazási területeket, iránymutatást adni a megfelelő biometrikus rendszer kiválasztásához és rámutatni arra, hogy melyek azok az alkalmazások, ahol kritikus a biometrikus adatokon alapuló személyazonosítási technológia bevezethetősége. A kritikus fogalmát abban az értelemben használom, hogy kétséges kimenetelű, a magyar értelmező szótár alapján: *„Olyan <helyzet, állapot, időszak, időpont>, amely valamiben fordulatot hoz, valaminek a menetét, sorsát döntő módon alakítja, befolyásolja, megszabja; fontos, nehéz, válságos, (sors)döntő."* [8] A legfőbb probléma ezen a területen az, hogy a biztonság nem mindig mérhető pénzben és megtérülésben. Amennyiben a védendő tárgy, személy vagy információ értéke felbecsülhetetlen, úgy a befektetés megtérülése nehezen értelmezhető, illetve csak oly módon, hogy a védendő elemekben nem következett be olyan negatív állapotváltozás, amely egyébként védelem nélkül bekövetkezhetett volna. [9] [10] Ugyanakkor más alkalmazásokban a beruházás gazdasági megtérülése egy mérhető és jól meghatározható érték. [11] Ilyen tipikus alkalmazás például egy nagy munkavállalói létszámú vállalatnál bevezetendő dolgozói azonosításnál annak eldöntése, hogy biometrikus vagy kártyás megoldást alkalmazzanak. Jól körvonalazhatóak azok az alkalmazások a biztonság területén, ahol az alkalmazott biometrikus felhasználó-azonosítási eljárások bevezetése technológiai korlátokba ütközik. Egyszerűbben fogalmazva, jelen dolgozat keretében rámutatok arra, hogy miért működik a biometria minden további megfontolás nélkül egy szerverhelyiség védelménél vagy egy reptéri utasazonosítási rendszernél, míg egy néhány száz fős termelő vállalatnál komoly kockázatot jelent a rendszer sikeres bevezetése.

Célkitűzések

Kutatásom célja, hogy a tömegtartózkodású területeken olyan elemzési és alkalmazási követelményrendszert alkossak, melynek felhasználásával biztosítható a sikeres rendszerbevezetés és üzemeltetés. A terület tudományos jelentősége, hogy a hiteles személyazonosítás egyre nagyobb jelentőséggel bír, azonban az alkalmazhatósági aspektusok

[3] MOA (Mission Oriented Application): feladatorientált alkalmazás, mely, mint mutató arra vonatkozik, hogy az adott eszközt milyen biztonsági igényű feladatokra lehet alkalmazni.

területe kevéssé kidolgozottak. Sem a megrendelők, sem a biztonsági szakemberek számára nem állnak rendelkezésre olyan, a gyakorlatban is hasznosítható eszköztárak, melyek felhasználásával mérhetők és előre jelezhető módon értékelhetők a különböző biometrikus megoldások. Célkitűzésemet a vonatkozó iparági szabványok és „*best practice*", azaz széles körű tapasztalaton alapuló, számos szervezetnél, vállalatnál is sikeresen bevált jó gyakorlat felhasználásával és továbbfejlesztésével, valamint az évek során elvégzett forgatókönyvi és működési tesztek eredménye alapján terveztem elérni. Ezek a tesztek az Óbudai Egyetem keretében valósultak meg, eredményeik a www.abibiometrics.org (letöltés ideje: 2019. 04. 01.) weboldalon, valamint tudományos publikációkban jelentek meg. A biztonsági rendszerek egyik elsődleges tulajdonsága, hogy milyen mértékben képes kizárni a hibásan elfogadott jogosulatlan személyeket. **Kutatásom fókusza azonban egy másik, kevésbé fontosnak tartott tulajdonság, nevezetesen a hibásan elutasított, jogosult felhasználó problémája.** A tömegtartózkodású objektumoknál a gyakorlatban mindig ez a kérdés kerül előtérbe, hiszen lehet bármilyen biztonságos egy rendszer, ha a felhasználók üzemszerűen nem tudják azt használni.

A kutatási területek kiválasztásánál azokra a részfeladatokra koncentrálok, melyek világszerte kidolgozatlan és megoldatlan problémaként jelentkeznek.

Stratégiai célként határoztam meg feltérképezni a tömegtartózkodású objektumok biztonsági beléptetésének sajátosságait, valamint feltárni az ott dolgozók biometrikus beléptetéséhez kapcsolódó szubjektív tényezőket.

Kihangsúlyozott figyelmet fordítottam és pontos, matematikai leírását adtam meg az egyik legnagyobb problémának, a dolgozók vagy felhasználók sorban állására és várható várakozási idejére, mely alapján tervezhető és értékelhető bármilyen beléptető rendszer.

A forráskutatás alatt szembesültem azzal a problémával, hogy a beléptető rendszerekkel és ezen belül a biometrikus azonosítókkal milyen kevés szakirodalom foglalkozik magyarul, de még a nemzetközi szakmában elsődlegesen elfogadott kommunikációs nyelven, angolul is meglehetősen kevés a forrás. A munka alatt fontos mellékcéllommá vált, hogy olyan értekezést hozzak létre, amely a lehető legjobban feldolgozza a témámhoz kapcsolódó releváns hazai és nemzetközi szakirodalmat, megfelelő alapot kínálva a további elemzésekhez, vizsgálatokhoz és tudományos kutatásokhoz.

Végül pedig személyes motivációm az volt, hogy a szakmai tapasztalatom és kutatásaim alapján olyan metodikát dolgozzak ki, melynek alkalmazása kiküszöböli a jövőbeni sikertelen biometrikus adatokon alapuló beléptető rendszer bevezetésének előfordulási lehetőségét.

Az értekezésemet és a hipotéziseket úgy építettem fel, ahogy azok logikailag a probléma felmerülés sorrendjében jelentkeznek. Először a felmerült biztonsági-üzleti problémákat ismertetem, majd ezek alapján alkotom meg az igazolni kívánt hipotézisket.

C1. Melyek azok az alkalmazási területek, ahol tipikusan problémás a biometrikus beléptetés használata?

A biometrikus azonosítás a legkülönbözőbb területeken került alkalmazásra és folyamatosan újabb és újabb területekre tör be. Az egyes technológiák, valamint eszközök nem alkalmasak arra, hogy mindenhol azokat vegyék igénybe. A biztonságtudományi doktori iskolában már kidolgozásra került néhány szempontrendszer, elsősorban rendészeti alkalmazásokon belül. Ezeket, a nemzetközi szakirodalmat és a saját tapasztalataimat felhasználva létrehozható a teljes szempontrendszer, melynek célja, hogy az üzleti-biztonsági körülményeket ismerve megválaszolja azt a kérdést, hogy mely berendezések alkalmazása vetődhet fel egyáltalán egy projekt kapcsán.

A kiindulási pont az volt, hogy az általam elemzett területeken nem, vagy csak egyes részterületeken belül folyt olyan kutatás Magyarországon, melyre támaszkodhattam. Feltételeztem, hogy az általános ajánlásokon túl nincs konkrét követelményrendszere használati szempontból a biometrikus alkalmazásoknak. Feltételeztem továbbá, hogy az egyes alkalmazásoknak jól körülírható tulajdonságai vannak, melyek meghatározásával a kritikus alkalmazások egyértelműen azonosíthatók. Az alkalmazások fejlődésével és terjedésével egyes területek összemosódhatnak vagy újak jöhetnek létre. A most problémásként azonosított alkalmazásoknál használt modell és számítási eljárások bárhol máshol felhasználhatók.

C2. Milyen matematikai modellel írható le az beléptetési folyamat?

A beléptető rendszerek méretezése jellemzően a menekülési útvonalakra vonatkozó életvédelmi szempontok szerint történik, azonban a tömegtartózkodású helyeken ezen túlmutató biztonsági és üzleti igények merülnek fel. Az egyik elsődleges kérdés, hogy a felhasználók mennyit fognak várakozni az áthaladáskor. A biometrikus rendszerek működése valószínűségi változókkal jellemezhető, amely jelentősen képes negatívan befolyásolni az áthaladási folyamatot. Feltételeztem, hogy megalkotható a biometrikus beléptető rendszerek folyamatmodellje, valamint pontos számítási eljárások adhatók meg a tervezéshez, amellyel biztosítható a bevezetési projekt sikeressége a felhasználói elfogadottság oldaláról is.

C3. Mit fogadnak el az emberek még „jónak”, ha nem működik tökéletesen a beléptető rendszer?

A hibás elutasítási arányra a gyártók jellemzően 0,01% algoritmikus értéket adnak meg, ami azt jelenti, hogy a sikeresen prezentált biometrikus minta után ennyi esetben utasítja el a jogosult felhasználót a berendezés. Ennek az értéknek a statisztikai értékelhetőségéhez mintegy 3000 mérést kell elvégezni mérési pontonként, ami nem, vagy csak nagyon komoly erőforrások igénybevételével oldható meg. A valóságban mért hibás elutasítási arány legalább egy, de inkább két nagyságrenddel magasabb (1–50%) és az emberek ebben a tartományban határozzák meg egy rendszer használhatóságát. Feltételeztem, hogy kvalitatív és kvantitatív kutatási módszerekkel meghatározhatók az emberek általános elfogadási küszöbe, amely eredmények alapján a biometrikus rendszerekről egyértelműen eldönthető, hogy megfelelnek-e az elvárásoknak.

A téma kutatásának hipotézisei

1. **Megalkotható a biometrikus alkalmazások osztályozási rendszere, ahol az azonosítási módszerek az alkalmazásnak megfelelő szempontok szerint értékelhetők.**

2. **Matematikai modellel leírható és hatékonyan vizsgálható a tömegtartózkodású helyek beléptetési folyamatmodellje.**

3. **Biometrikus alkalmazásoknál meghatározható a felhasználók elfogadási intervalluma a téves elutasításokkal szemben, és ez alapján a biometrikus beléptető rendszerek értékelhetők.**

Kutatási módszerek

Kutatási témámat eredetileg tisztán műszaki és biztonságtudományi megközelítéssel szerettem volna feldolgozni. Azonban minél mélyebben ástam bele a témába magam, annál több tudományterület került a látómezőmbe, mint az informatikatudomány, közgazdaságtudomány, később a társadalomtudományok, a pszichológia és szociológia is. Az elemzések elvégzéséhez komolyan el kellett mélyülnöm a matematikában, pontosabban a statisztikában és döntéselméletben, végül a hálózatok tudományában. Kutatási témám interdiszciplináris jellege miatt nehéz volt valamennyi tudományág vonatkozó szakirodalmát a szükséges mélységig megismerni, annak érdekében, hogy értékelhető következtetéseket tudjak levonni.

A kutatásaim során mindig elsődleges szempont volt az eredmények gyakorlati alkalmazhatóságának figyelembevétele. Ez sokszor nehézséget okozott a hatályos jogi normák és az elméleti megfontolások inerciarendszerében.

Az eredeti problémafelvetés gyakorlati tapasztalatok alapján született meg, ez a teljes kutatást végigkövette. Alkalmaztam tartalomelemzést, folytattam szakértői mélyinterjúkat, a következtetések megfogalmazásakor az induktív és deduktív eljárást egyaránt felhasználtam. Kutatásom során kiemelt figyelmet fordítottam gyakorlati tapasztalatok összegyűjtésére és elemzésére. A tapasztalataimat tájékoztatási céllal írtam le, nem használtam fel tudományos következtetésekre. A kvalitatív kutatás során számos interjút készítettem a téma elismert szakembereivel és a szakma érintettjeivel. Számos magyar és nemzetközi konferencián vettem részt, ahol a téma szakértőivel mélységében egyeztettem.

A kvantitatív kutatásaim eredményeit a statisztika eszköztárát felhasználva elemeztem, így azonosítva az ok-okozati összefüggéseket.

Az értekezés kidolgozásakor figyelembe vettem a hatályos jogi szabályozást, amely folyamatosan változik: egyrészt a személyes adatok védelmével foglalkozó rendeleteket és törvényeket, másrészt a migráció és a terrorhelyzet okozta jogszabályváltozásokat.

Az egyes személyazonosítási eljárások analízisénél mind matematikai, mind összehasonlítási módszert alkalmaztam.

Kutatásom során figyelembe vettem a tudományosság alapvető feltételeit, mint az általánosíthatóságot, a megbízhatóságot és az érvényességet.

Mindig ismert volt a számomra, hogy a biometrikus azonosítás témája rendkívül szerteágazó, de valódi terjedelme akkor látszódott igazán, amikor szisztematikusan elkezdtem feldolgozni a szakirodalmat, melynek eredményeképp később szűkítenem kellett az érintett területeket. A biometrikus megoldások rendészeti és jogi vonatkozásait kiválóan tárgyalja dr. Balla József értekezése és tanulmányai, elsősorban ezeket a forrásokat dolgoztam fel. Továbbá felhasználtam dr. Fialka György és dr. Földesi Krisztina PhD-értekezéseit is, számos helyen hivatkoztam az eredményeikre, ezeket részletesen feltüntettem az értekezésemben.

A kutatásaimat 2019. január 31-én lezártam, majd a bírálatok alapján 2019. május 31-i dátummal aktualizáltam.

1 A BIOMETRIKUS ALKALMAZÁSOK OSZTÁLYOZÁSI RENDSZERE, KRITIKUS ALKALMAZÁSOK

A biometria napjainkra az élet minden területén megjelent. [12] Biztonsági szempontból vizsgálva a megoldások széles körben elérhetők a szakemberek számára, mégis számos sikertelen bevezetési projektet ismerünk. A biometrikus rendszerek felhasználóiminta-pozícionálásának kérdéseiről publikációmban ismertettem néhány tipikus esetet:

„1999-ben került kereskedelmi forgalomba Magyarországra először íriszazonosító beléptető rendszer, ez egy német gyártmány volt, ami azóta megszűnt. Az azonosító algoritmus hatékonysága nem különbözött számottevően a napjaink rendszereitől, mégis gyakorlatilag használhatatlan volt. Ennek az volt az oka, hogy a kamera előtt 30±3 cm távolságra kellett mozdulatlanul 0,2 s időtartamban stabilizálni a biometrikus mintát, azaz ennyi ideig kellet pislogás és mikromozgások nélkül állni a felhasználónak.

A 2000-es évek közepétől a Széchenyi István Egyetem győri kollégiumában ujjnyomat azonosító biometrikus beléptető rendszer működött. A technológiából adódó nehézségeken túlmenően komoly felhasználói problémákat is tapasztaltam az évek során. Jellemző volt, hogy a gondok jelentős része szeptember-október hónapokban fordult elő, amikor a „gólyák" beköltöztek. Helyszíni megfigyeléseket végeztem az okok feltárására. A legtöbb esetben az új regisztrált felhasználó ráhelyezte az ujját a szenzorra, ez valamilyen oknál fogva sikertelen volt, a második próbálkozásnál pedig teljes erejével nyomta rá az ujját az érzékelőre, aminek következtében biztos volt az elutasítás, ezután a biztonsági őr gombbal beengedte a diákot.

Egy 500 fős termelő cégnél ujjnyomat felismerő beléptető rendszert telepítettek 2004-ben. A bevezetés után 3 hónappal a rendszert 70 dolgozó nem tudta használni, ez az arány a rendszer teljes élettartamán fennmaradt, 2010-ben váltották le kártyás azonosításra.

Az Óbudai Egyetem Bánki Donát Karának Népszínház utcai épületében több mint 10 éve biometrikus beléptető rendszer működik, három beléptetési ponttal, különböző telepítési pozíciókkal, itt szignifikáns eltéréseket tapasztaltam az azonosítás sikerességében függően a telepítési elrendezéstől, ami közvetlen hatással van a felhasználói minta pozicionálására.

Egy bróker cég szerverszobájára ujjnyomat-azonosító beléptető rendszert telepítettek. A jogosult felhasználók száma 10 alatt volt, mindenkit könnyen be lehetett regisztrálni, mégis a használat során folyton problémák léptek fel a magas hibás elutasítási arány miatt. A tesztek során kiderült, hogy az 500 DPI-s felbontású szenzor felülete túl nagy volt, az ujj megfelelő elhelyezését nem

segítette a hardveres kialakítás és az algoritmus különböző pozíciókban más, nem regisztrált ujjakat ismert fel." [13, pp. 252-253]

Jelen fejezet célja, hogy tudományos megközelítéssel azonosítsa a biometrikus alkalmazások tipikus területeit és meghatározza azokat a tényezőket, amelyek alapján egy ilyen rendszer bevezetése kockázatosabb, mint a többi esetben. A kockázati tényezők is megvizsgálásra kerülnek, ezek alapján azonosítom azokat az alkalmazásokat, ahol a legnagyobb a veszélye a sikertelen bevezetésnek.

A biometrikus rendszerek gyártói megadják a téves elutasítási (FRR)[4] és elfogadási arányokat (FAR)[5] az eszközökre, **melyek algoritmikus eredmények, a valóságban több nagyságrenddel rosszabb értékek mérhetők**. Mégis, a nagyságrendekkel rosszabb eredményekkel működő rendszerek is tekinthetők jónak a valós tapasztalatok alapján – ez a jelenség részletesen tárgyalásra kerül a 3. fejezetben.

1.1 Alapok

A biometria kifejezés a görög „*bio*" – élet és „*metria*" – mérés szavak összeillesztéséből ered. A felhasználók hiteles azonosításának igényével – legyen az fizikai vagy informatikai – az emberek egyedi jellemzőit akarjuk automatikus rendszerekkel megmérni, azaz a biometrikus azonosítás emberek valamely testi jellemzőjének felismerése elektronikus rendszerekkel.

A biztonság megteremtésének egyik alapvető feladata, hogy az adott objektumhoz, személyhez vagy információhoz történő hozzáférést csak az arra jogosultak tehessék meg. A biztonságtechnikai rendszerek jelentős része erre a feladatra fókuszál. Az ajtón lévő rácson a kulcs, a vagyonvédelmi rendszerek PIN-kódja, a beléptető rendszerek kártyái vagy a videó megfigyelő alkalmazások jelszóalapú hozzáférés vezérlése mindegyike azt a célt valósítja meg, hogy csak az arra jogosultak férhessenek hozzá értékeikhez. [14]

Az automatikus személyazonosítás feladatában három alaptechnológia létezik:

1. tudásalapú;
2. birtokalapú;

[4] FRR (False Reject Rate): hibás elutasítási arány – megmutatja annak a valószínűségét, hogy egy rendszer elutasít egy érvényes mintát, amely benne van az adatbázisában. A téves elutasítási arány a téves elutasítások számának és az összes azonosítási kísérletnek a hányadosa. A gyakorlati tapasztalatok szerint ez a mutató az egyik legfontosabb, nagyban meghatározza a biometrikus rendszer használhatóságát. A létszám növekedésével értelemszerűen statisztikailag egyre nagyobb a valószínűsége, hogy a felhasználóknál problémát fog jelenteni a téves elutasítás.
[5] FAR (False Accept Rate): hibás elfogadási arány – a téves elfogadási arány annak a valószínűségét írja le, hogy a rendszer hibásan elfogad egy olyan személyt, aki nincs benne az adatbázisban vagy hibásan azonosít valaki mást az adatbázisból.

3. biometrikus azonosítás.

A szükséges biztonsági szint eléréséhez ezeket az alapeljárásokat kombinálni is lehet. [15]

1.1.1 Tudásalapú azonosítás

A tudásalapú azonosításra jó példa a számítógépes rendszerbe jelszóval történő belépés, de ilyen a bankautomatánál megadott PIN-kód is. Modern beléptető rendszerekben önmagában nem alkalmazzuk.

Előnyei:

- alacsony költség: nincs felhasználói oldali eszközköltség, pl. kártya;
- könnyen cserélhető;
- a felhasználók elfogadják és képesek használni.

Hátrányai:

- átruházható;
- könnyen ellopható, kifigyelhető, kölcsönadható.

1.1.2 Birtokalapú azonosítás

A birtokalapú azonosítás azt jelenti, hogy van valami tárgy (pl. kártya), amely a felhasználóhoz van rendelve és ezzel a tárggyal azonosítja magát. Ez a technika a legelterjedtebb napjainkban és létezik néhány olyan felhasználási terület, ahol muszáj ezt használni.

Előnyei:

- **Egyszerűség:** könnyű a használata, mindössze az olvasó használatát kell elsajátítani, a felhasználók általában ismerik.
- **Elfogadottság:** a dolgozók könnyen elfogadják a használatát, alacsony az ellenállás a technika bevezetésénél.
- **Gazdaságosság:** egy azonosítási végpont kiépítésének költsége jelentősen kisebb, mint például egy biometrikus eszköznél.
- **Vizuális azonosítás lehetősége:** a fényképpel ellátott beléptető kártyák révén könnyen azonosítani lehet az illetéktelen behatolót.
- **Egyéb felhasználási lehetőségek:**
  - hálózati bejelentkezés a számítógépes rendszerbe;
  - digitális aláírás tárolása;
  - étel-ital automaták vezérlési lehetősége;

- kantinos fizetés;
- targoncavezérlés;
- öltözőszekrény-vezérlés;
- nyomtató- és fénymásoló-vezérlés**.**

Hátrányai:

- ellopható, kölcsönadható;
- másolható, habár egyre inkább elterjednek a biztonságos intelligens chipkártyák, azonban idővel minden technikát feltörnek.

1.1.3 Biometrikus azonosítás

A biometrikus azonosítás az emberek egyik legalapvetőbb társas funkciója, a születéstől kezdve nap mint nap alkalmazzuk. A gyermek először szülei hangját, illatát és arcát ismeri fel. Később a rokonokat, osztálytársakat, barátokat is így azonosítja. A technika fejlődése azonban csak az elmúlt néhány évtizedben tette lehetővé, hogy automatikus biometrikus azonosító rendszereket hozzanak létre. Valójában ezek az új fejlesztések mind visszavezethetők a már évezredekkel ezelőtt használt eljárásokra. Az egyik legrégebbi és legalapvetőbb példa az arcfelismerés. A civilizáció kezdete óta az emberek ismerős és ismeretlen kategóriákba sorolják találkozáskor az egyéneket az arcuk alapján. Ez az egyszerűnek tűnő feladat egyre bonyolultabbá vált a népesség növekedésével és az utazási lehetőségek gyorsabbá és egyszerűbbé válásával. Az addig zárt közösségekben lévő ismerős arcok egyre több új és ismeretlen látogatóval bővültek.

Az emberek legtöbb jellemzője egyedi, a kérdés csak az, hogy ezek adott körülmények között, megfelelő költség/haszon mellett azonosíthatók-e.

Ilyen körülmény lehet például a technológiai fejlettség vagy a biometria jellemző adottságai. Az egyik legpontosabb biometriai jellemző a DNS-szekvencia, azonban automatizált felhasználóazonosításra jelen technikai fejlettség mellett mégsem alkalmas, egyrészt mert lassú (a leggyorsabb eszközök 10 perc alatt működnek, az eljárás általános hossza 90 perc), másrészt pedig nem biztosítható, hogy a DNS-t csak a jogosult felhasználó juttatja az azonosítóba. Egy hajszál, vagy a számítógép billentyűzetére hullott elhalt bőrdarab is alkalmas az azonosításra.

A jövőbeni fejlesztési irányok egyértelműen az emberek automatizált biometrikus megoldásai felé mutatnak, mivel ez az egyetlen olyan módszer, ahol valóban az ember kerül azonosításra.

A biometrikus rendszereket a szakirodalomban számos szempont szerint értékelik. A legfontosabb általános szempontok [13]:

1. ***„Hatékonyság:*** *Az eredeti biometrikus minta megfelelő levétele, kódolása és összevetése elengedhetetlen a rendszerek megfelelő működéséhez. A cél az, hogy a kód legalább annyira megkülönböztető legyen, mint az eredeti minta. A jó megkülönböztető algoritmus kiválasztja azokat a jellemzőket, amelyek valóban megkülönböztetik a mintákat és ezeket felülsúlyozva magasabb stabilitást és pontosságot eredményez."* [16]
2. ***„Biztonság:*** *A kódolás magas információtartalma segít megakadályozni a brute force*[6] *jellegű támadásokat. A biometrikus kód biztonsága mérhető Shannon entrópia függvényével. Az algoritmikus biztonság mellett vizsgálni kell a biometrikus minta reprodukálhatóságát, az eszközök fizikai és logikai-, a hálózati kommunikáció és a felügyeleti szoftver biztonságát is."* [16]
3. ***„Privacy:*** *A felhasználók személyes adatainak magas fokú védelme szükséges. A legfontosabb, hogy a biometrikus kódból semmilyen módon ne legyen reprodukálható az eredeti minta, mert ebben az esetben ugyanaz lenne a kockázat, mintha az eredeti minta képét tárolnánk. A biometrikus minta mellett az összes tárolt személyes adat védelmére ügyelni kell."* [16] Ennek különös jelentőséget ad a 2018. május 25-én hatályba lépett Európai Uniós rendelet, a GDPR.[7] [17]

Ahhoz, hogy egy biometrikus adatokon alapuló személyazonosítási rendszer használható legyen, meg kell felelnie az alábbi kritériumoknak:

1. **Univerzalitás:** minden személynek rendelkezni kell az adott jellemzővel.
2. **Egyediség:** bármely két személynek kellően eltérőnek kell lennie a mért jellemző vonatkozásában.
3. **Állandóság (stabilitás):** a mért jellemzőnek egy jól meghatározható időintervallumon belül időinvariánsnak kell lennie.
4. **Megszerezhetőség (begyűjthetőség):** a mérni kívánt jellemzőt mennyiségileg is be kell tudni gyűjteni.
5. **Teljesítmény:** a rendszernek a működési és környezeti körülmények függvényében is el kell érni az elvárt pontosságot és sebességet.

[6] Brute force (nyers erő): működésének lényege, hogy a rendszer kódolásának ismeretében az összes lehetséges kulcsot megpróbálva tör be a rendszerbe. Definíció szerint mindig eredményes, a kérdés az, hogy az adott műszaki körülmények között valós időben megoldható-e.
[7] GDPR (General Data Protection Regulation): általános adatvédelmi rendelet.

6. **Elfogadottság:** azt jelzi, hogy az emberek milyen mértékben hajlandóak elfogadni egy adott biometrikus azonosító használatát a mindennapi életükben.
7. **Megtéveszthetőség:** a kockázat mértéke, amely megadja, hogy a mért biometrikus jellemző külső támadó által befolyásolható. [15] [18] [19] [20]

1.2 A biometria alkalmazási területei

Az automatizált, elektronikus biometrikus személyazonosítás hatalmas fejlődésen ment keresztül az elmúlt ötven évben.[8] [21] A rendészeti szerveknek és hatóságoknak egyre nagyobb az igénye arra, hogy személyeket hitelesen és gyorsan, gyakorlatilag bárhol képesek legyenek azonosítani. [22] Ezzel párhuzamosan az élet minden területén egyre inkább szükséges a felhasználók, belépők azonosítása, a hozzáférés hitelesítése. Emellett világosan látszik, hogy a felhasználók hozzáállása, az elfogadottság a technológia irányában döntő szerepet játszik ezek sikerességében, mindennapos használhatóságában. [23]

A biztonsági célú alkalmazásokban a felhasználók sokkal elutasítóbbak és gyanakvóbbak, mint a kereskedelmi alkalmazásokban, ahol az ő döntésük, hogy akarják-e használni vagy sem, a biometrikus minta nem kerül ki a felügyeletük alól, ezenkívül kényelmes is az alkalmazása. [24] Erre jó példa, hogy míg az általános célú biometrikus azonosítást elutasítják a felhasználók, addig az iPhone-nal rendelkező fogyasztók 89%-a veszi igénybe ezt a megoldást a telefonján. [25]

Jogosan vetődik fel a kérdés, hogy vajon mi különbözteti meg az egyes alkalmazási területeket egymástól, mik a jellemzőik és hogyan osztályozhatók. A fejezet következő részében ezek kerülnek ismertetésre. [21]

Az Encyclopedia of Biometrics 2015-ös második kiadását tekintem kiindulásnak, amelyet feldolgoztam, kategorizálás szempontjából elfogadtam, ezt a kutatásaim alapján kiegészítettem és az alábbiak szerint összesítettem: [26]

1. **Rendészeti alkalmazások:** A rendészetnek számos definíciója létezik a magyar szakirodalomban, én Katona Géza definícióját választottam, mivel ez illeszkedik legjobban az értekezésemhez: *„A rendészet a közrend megzavarásának megelőzésére, a közvetlenül zavaró magatartások, események, veszélyek megakadályozására, elhárítására, a megzavart rend helyreállítására irányuló tevékenység.”* [27, p. 12] A feltételezett elkövetők azonosítására már régóta hasznosítják a biometrikus megoldásokat

[8] 1969-ben kezdte meg az FBI az első automatikus ujjlenyomat-azonosító rendszer felépítését (AFIS), az első kereskedelemben kapható biometrikus beléptető eszköz a kézgeometria-azonosító volt 1974-ben.

a bűnüldöző szervek. Elsősorban AFIS[9]-megoldásokról van szó. Rendészeti alkalmazásokban használják, bármilyen ujjlenyomat-töredék betölthető, és a rendszer visszaadja a legjobb egyezéseket. Ezután törvényszéki szakértők vizsgálják a mintákat hagyományos módszerekkel, [28] azonban több, jövőbe mutató kutatás is folyik a rendészeti egységek terepen, valós időben történő támogatására. [18]

Magyarországi vonatkozás a 2006-tól bevezetett biometrikus útlevelek, első lépcsőben az arcképek, 2009-től az ujjnyomatok rögzítésével is. Az új biometrikus személyi igazolványokat 2016-ban vezették be, amivel lehetőség nyílik a rendészet számára az okmány és a tulajdonosa közötti közvetlen kapcsolat megállapítására, ezzel hatékonyabb személyazonosítási módszereket biztosítva. [29] A személyi igazolvány az útlevelekhez hasonlóan RFID[10] technológiás chipkártya, amelyen tárolható a felhasználó ujjnyomata, továbbiakban pedig egyéb biometrikus minták és adatok. [30]

A biometrikus személyazonosítás lehetővé teszi, hogy igazoltatásnál egy hordozható eszközzel automatizálja a hatóság az adatbevitelt és lekérdezést, valamint a személyazonosság nagy pontossággal történő ellenőrzését. Megállapításra alapvetően nincs lehetőség, mert a biometrikus adatokat a jogszabályok szerint csak a kártyán tárolják, központi adatbázisban nem. Más a helyzet a körözés alatt álló személyek esetén: ekkor további lehetőség rejlik az ujjnyomatok ellenőrizhetőségében, ugyanis ilyen esetekben az említett mintákat központi nyilvántartásban tárolják. Megfelelően kiépített rendszer esetén, ha az hálózati kapcsolatban áll a központtal, önmagát álcázni kívánó személyek azonosítására is lehetőség nyílik. A kártyákban található adatok védelme azonban kockázatot jelent, ugyanis a tárolt adatok és a kártya biztonsági szintjének függvényében lehetőség nyílhat hamis személyazonosító igazolványok előállítására. További kockázat rejtőzhet a nagy felhasználószámban. Egy hatósági ellenőrzésnél az idő nem elsődleges szempont – a hatóságnak legfeljebb saját érdekében kell foglalkoznia az ellenőrzés idejével, ugyanakkor a rendszernek rendkívül nagy pontossággal kell üzemelnie – nem keverheti össze egy körözött személy ujjnyomatát egy ártatlanéval. Ez azonban pontos mintarögzítést, hatékony algoritmust és megfelelő számítási kapacitást igényel.

2. **Határforgalom-ellenőrzés:** A folyamatosan növekvő nemzetközi utasforgalom szükségessé teszi a fejlett technológiák bevezetését, amelyek automatizálják, egyszerűsítik és meggyorsítják a határátlépést. [31] Nemzetközi szabványok alapján egyre

[9] AFIS (Automated Fingerprint Identification System): Automatikus Ujjlenyomat Felismerő Rendszer.
[10] RFID: Rádiófrekvenciás, kontaktusmentes intelligens chipkártya.

szélesebb körben vezetik be a biometrikus útleveleket, amelyek ujjlenyomatot, arc- és íriszmintákat[11] tartalmazhatnak. [32] Egyes helyeken, mint például az USA és az EU, megkövetelik a biometrikus útlevél alkalmazását, míg más országokban egyelőre csak lehetőség van biometrikus útlevelek beszerzésére és használatára. A megfelelően kialakított biometrikus azonosító rendszerek lehetővé teszik, hogy az élőerős védelem az ismeretlen kockázatú személyekre összpontosítson. Az adatbázis olyan személyek adatait tartalmazza, akik a társadalomra veszélyesek, így az adataik kezeléséhez való hozzájárulásuk és hozzáállásuk figyelmen kívül hagyható. Működésük támogatható más rendszerekkel, amelyek további szűrési szinteket biztosítanak. A határforgalom ellenőrzésnél használatos biometrikus rendszerek téves azonosítási aránya nagyságrendekkel kisebb, mint a téves elutasítási arány, így egy, az ellenőrzést akadályozni kívánó személy számára sokkal egyszerűbb fel nem ismerhető mintát produkálni, mint átverni a rendszert, hogy az másnak higgye. Ha a felhasználónak nem teszik lehetővé az alternatív azonosítási módszer alkalmazását, kötelező használni a biometrikus rendszert. A határátlépésnél – amennyiben megkövetelik a biometrikus minta használatát – a célszemélynek csak két lehetősége van: együttműködni vagy visszafordulni (kockáztatva a gyanús viselkedés miatti további eljárást). A hatóságokat nem kell, hogy „érdekelje" a felhasználók véleménye, az egyetlen kritérium a rendszer hatékonysága és a biztonság garantálása. Természetesen ez nem jelenti azt, hogy a hatóságok számára nem célszerű egy utasbarát rendszert kialakítani a saját érdekükben is, azonban ez nem tekinthető kockázati tényezőnek. A biometrikus útlevelek kompatibilitásához szükséges kitételeket az ICAO9303 rögzíti, amely lehetővé teszi, hogy bármely biometrikus azonosítást megkövetelő ország el tudja fogadni más országok útleveleit.

[11] Az Európai Unióban nem került szabványosításra.

3. ábra: FASTPASS kísérleti rendszer határőr által látott felület, a személygépjárművekkel érkező utasok biometrikus azonosítására; forrás: [29]

Napjainkban az EU-ban és ezen belül Magyarországon az egyik legnagyobb biztonsági kihívást a migráció jelenti [30]. Görbe Krisztina rendőr alezredes szerint *„Migráció volt, van és lesz. A XXI. században az egyik legmarkánsabb globalizációs tényező a migráció, amely egyszerre gazdasági-társadalmi-szociális-etnikai-vallási stb. problémákat kiváltó, összetett jelenség, a nemzeti-regionális biztonságot fenyegető tényező, de forrása lehet a jólét fenntartásának, a népesség szinten tartásának, a statisztikák javításának, humanitárius megoldásnak. Összegezve: nehezen kezelhető, de kezelendő kategória."* [33, p. 4] Böröcz Miklós rendőr alezredes kutatásában megvizsgálta 2001-től a nyugati országokat ért terrorcselekményeket és eredményeiből kiderült, hogy ezeket jellemzően legálisan betelepült bevándorlók másod- vagy harmadgenerációs leszármazottjai követték el, azonban tény, hogy az illegális migráció és a szervezett bűnözés összefonódása is jelentős. [34] Következésképpen a bevándorlók biometriai adatainak rögzítése alapvető fontosságú lenne, annak érdekében, hogy a kriminalizálódó egyéneket a korai szakaszban a hatóságok képesek legyenek kiszűrni.

A biometrikus útlevelek alkalmazása azonban komoly adatvédelmi problémákat vet fel több szempontból is. Ezeket az útleveleket a gyakorlatban egy RFID Smart Cardnak tekinthetjük, ahol egy chipen tárolják a biometrikus mintát. A kártyákat megfelelő védelemmel kell ellátni, mivel érintés nélkül olvashatók, így egy megfelelő olvasóval adatok

nyerhetők ki belőlük. Ezért fontos, hogy az adat milyen jellegű (pl. titkosított) és milyen formában található meg a chipben. Az ISO/IEC 14443 szabvány alapján legalább 32 kilobájtnyi biometrikus adatot tárolnak. Az említett ICAO dokumentum definiálja, hogy az egyes biometrikus gyártók más és más algoritmusokkal alakítják sablonná a levett mintákat, amelyeket titokban tartanak, ezért az interoperabilitás érdekében nyers biometrikus mintákat tárolnak a memóriában. Ez adatvédelmi szempontból súlyos kockázattal jár, ugyanis míg a nyers biometrikus mintához való hozzáférés a visszaélések egész sorát teszi lehetővé, addig egy irreverzibilis kódolással létrehozott sablonhoz való hozzáférés nem okoz ekkora problémát.

3. **Regisztráltutas-program:** *„A regisztráltutas-program a határregisztrációs rendszerrel együtt jelentősen javítani fogja a határigazgatást azáltal, hogy megerősíti az ellenőrzéseket, ugyanakkor felgyorsítja az EU-ba gyakran utazó, előzetes ellenőrzésnek alávetett nem uniós személyek határátkelését."* [32, p. 282] Ez az alkalmazás lehetővé teszi az utazóknak, hogy az ellenőrző pontokon gyorsabban juthassanak át, valamint alacsonyabb valószínűséggel kerüljenek kiválasztásra szigorú biztonsági átvilágításra. Az ilyen jellegű programokban való részvétel önkéntes alapon működik és megfelelő háttérellenőrzések után van rá lehetőség [35]. *„Az illetékes hatóságok elbírálják a kérelmet, megvizsgálják, hogy a kérelmező eleget tesz-e az 562/2006/EK rendelet 5. cikkének (1) bekezdésében meghatározott belépési feltételeknek, valamint, hogy esetében korábban megadták-e, meghosszabbították-e, elutasították-e vagy visszavonták-e a regisztráltutas-programban való részvételt. Az ellenőrzéskor különös figyelmet kell fordítani annak megvizsgálására, hogy »a kérelmező nem jelent-e kockázatot az illegális bevándorlás vagy a tagállamok biztonsága tekintetében, továbbá, hogy a kérelmezőnek szándékában áll-e az engedélyezett tartózkodási időn belül elhagyni a tagállamok területét.«"* [32, p. 282]
4. **Háttérellenőrzés:** Elsősorban az Egyesült Államok használ biometrikus ellenőrzést számos kormányszerv vagy gazdasági szereplő bizonyos pozíciók betöltéséhez. A jelentkező biometrikus jellemzőit (általában ujjlenyomat, arc) rögzítik, és elküldik a hatóságoknak abból a célból, hogy információt kapjanak az esetleges múltbeli kihágásokról. A polgári lekérdezéseknél biometrikus minta és a lekérdezés megsemmisítésre kerül a folyamat végén.[12] Ez a folyamat végső soron a rendészeti

[12] Magyarországon gazdasági szereplőnek erre nincs lehetősége és az állami szerveknek is csak rendkívül korlátozottan.

alkalmazás kiterjesztésének is tekinthető. Az Európai Parlament és a Tanács 562/2006/EK[13] rendelete (2006. március 15.) a személyek határátlépésére irányadó szabályok közösségi kódexének (Schengeni határ-ellenőrzési kódex) létrehozásáról 5. cikke rendelkezik a *„Beutazási feltételek harmadik országok állampolgárai számára"* szabályozásáról.

5. **Beléptető rendszerek:** A fizikai beléptetés ellenőrzésére kiváló megoldás a biometrikus azonosítás, amellyel a személy igazolja a jogosultságát. [7] Beléptető rendszerek esetében az általánosan használt technológiák az ujjnyomat-, írisz-, arc-, illetve erezetfelismerés. A rendszerek kétféle csoportra bonthatók működésük szerint, ezek az 1:1 és 1:N. Az első esetben a rendszer egy előre kiválasztott sablonnal veti össze a felhasználó által prezentált mintát, és megállapítja, hogy egyezik-e azzal. A sablon tárolható helyi adatbázisban, de birtokolhatja a felhasználó is. Magyarországon a jogszabályok nem teszik lehetővé a sablonok központi tárolását, így a helyes eljárás a sablonok egy felhasználó által birtokolt eszközön (RFID-kártya) való tárolása. 1:N üzemmódban a teljes adatbázissal összehasonlítja a prezentált mintát és a legjobban hasonlító sablont keresi – természetesen a rendszer beállításai által megszabott szigorúság mellett. Az alkalmazás típusa negatív, célja, hogy kiszűrjön minden olyan személyt, aki nem jogosult egy adott időpontban és belépési ponton történő áthaladásra. A beléptetésre léteznek alternatív – korábbi – megoldások, például tudásalapú (PIN-kódos) vagy tulajdonalapú (kártyás) rendszerek, azonban ezek kijátszhatósága bizonyos alkalmazások esetén megköveteli a magasabb biztonsági szint biztosítását. A biometrikus beléptető rendszerekkel szemben általában szigorú teljesítménybeli elvárásokat támasztanak azok, akik alkalmazzák, ugyanis egyensúlyt kell biztosítani a negatív azonosítási elv miatt megkövetelt alacsony téves elfogadási értékek és a megfelelő átbocsájtási képesség miatt megkövetelt alacsony téves elutasítási értékek között (bár ez utóbbi az olyan alkalmazásoknál, ahol a működési idő nem kardinális, elhanyagolható). [36]
6. **Munkaidő-nyilvántartás:** A dolgozók munkaidejének biometrikus ellenőrzésével a hibák, tévedések, túlfizetések és csalások minimalizálhatók, továbbá jelentősen csökkenthető az adminisztrációra fordított idő. [37] A munkaidő-nyilvántartás működhet a beléptető rendszer részeként, vagy önállóan is. Célja, hogy egyértelműen hozzárendelje a blokkolást az adott dolgozóhoz ezzel elejét véve a vitás helyzeteknek, továbbá lehetővé teszi a

[13] Jelenleg már nem hatályos, a 399/2016 számú EU rendelet van helyette.

munkaidőadatok kezelésének automatizálását, valamint szükség esetén a dolgozónak is könnyen elérhetővé tehetők a munkaidőre vonatkozó adatai. A beléptető rendszereknél felállított teljesítménykritériumok megfelelő működési sebességgel egészülnek ki. A munkaidő-nyilvántartó rendszereknél fontos, hogy lehetőleg ne alakuljanak ki hosszú sorok. Mind a beléptető, mind pedig a munkaidő-nyilvántartó rendszerek esetében lényeges, hogy a rendszert ténylegesen használó személyek elfogadják azt, valamint képesek legyenek használni. [38] Fontos változás a 2019. 04. 26-án hatályba lépett 2012. I. törvény a munka törvénykönyvéről változása, amelyben a GDPR rendelettel került harmonizálásra. A 11 § (1) bekezdésében tételesen felsorolásra került, hogy milyen esetekben kezelhető a munkavállaló biometrikus adata:

„11 § (1) A munkavállaló biometrikus adata az érintett azonosítása céljából abban az esetben kezelhető, ha ez valamely dologhoz vagy adathoz történő olyan jogosulatlan hozzáférés megakadályozásához szükséges, amely

a) a munkavállaló vagy mások élete, testi épsége vagy egészsége, vagy

b) törvényben védett jelentős érdek

súlyos vagy tömeges, visszafordíthatatlan sérelmének a veszélyével járna.

(2) Az (1) bekezdés b) pontja alkalmazásában jelentős védett érdek különösen

a) a legalább „Bizalmas!" minősítési szintű minősített adatok védelméhez,

b) a lőfegyver, lőszer, robbanóanyag őrzéséhez,

c) a mérgező vagy veszélyes vegyi vagy biológiai anyagok őrzéséhez,

d) a nukleáris anyagok őrzéséhez,

e) a Btk. szerint legalább különösen nagy vagyoni érték védelméhez fűződő érdek." [39]

Ez alapján világos, hogy **munkaidő-nyilvántartási céllal Magyarországon nem kezelhető a munkavállaló biometrikus adata**.

7. **Videomegfigyelő rendszerek (CCTV):** a hagyományos kamerás megfigyelő rendszereket a nap 24 órájában figyeli az arra beosztott őrszolgálat. Ez a munka rendkívül monoton és fárasztó, a biometrikus arcfelismerés és egyéb intelligens algoritmusok nagyban segítik az élőerő koncentrációképességének fenntartását és érdemi munkáját: Berek szerint: *„Ezeknek a fejlesztéseknek a célja az volt, hogy a megfigyelő személyzetet segítsék, ugyanis felmérésekből kiderült, hogy egy megfigyelést végző személy 20 perc után a monitoron látható események akár 95%-át is figyelmen kívül hagyja."* [40, p. 34] Az ilyen jellegű megfigyelő rendszerek alapját az arcfelismerésre alkalmas kamerák és egy vezérlőszoftver képezik. Az ideális működéshez a mintát a rendszernek meg kell tanulnia, amelyhez erre alkalmas alapmintát kell regisztrálni. Amennyiben a kamerarendszer a

megfigyelt terület nagy részét lefedi, úgy lehetőség van a területen tartózkodók helyzetének és tevékenységének automatikus nyomon követésére. [41] [42]

8. **Csalások csökkentése:** A különféle csalások – pénzügyi és személyes adatokkal való visszaélések – visszaszorítására jó lehetőséget nyújt a biometrikus azonosítás bevezetése. A biometrikus azonosítással védett ATM-ek csökkentik a visszaélések lehetőségét, és azok számára is hozzáférhetővé teszik a készpénzfelvételi lehetőségeket, akik egyébként valamilyen oknál fogva nem lennének képesek rendesen használni az automatákat. Erre tervek léteznek Indiában, ahol a hatóságok a világ egyik legnagyobb biometrikus adatbázisát építették fel, amely minden állampolgár számára hozzáférhetővé teszi az állami szolgáltatásokat (ahogy az állam számára a lakosokat is), pénzügyi szolgáltatásokat, egészségügyi ellátást stb. Az első ilyen automatát 2016-ban helyezték el, amelynél a tranzakciót vagy a biometrikus mintához tartozó azonosítószám, vagy a bankkártya indítja el, befejezéséhez azonban már biometrikus mintára van szükség. A szerződések megkötésekor személyazonosító lehetőséget és visszakövethetőséget is biztosít a megfelelő biometrikus minta alkalmazása (ilyen lehet az írásminta, így az aláírás is).
9. **Vagyonvédelem:** A biometrikus azonosítás ebben az alkalmazásában a klasszikus vagyonvédelmi eszközöket váltja vagy egészíti ki. Ilyenek például egy NATO-szobában a papíralapú dokumentumokat őrző széf ujjnyomat-azonosítással történő nyitása vagy egy riasztó kézerezet-felismeréssel történő hatástalanítása. [40] Ez az alkalmazási terület szervesen kapcsolódik a beléptető rendszerekhez.
10. **Logikai hozzáférés védelem:** Biometrikus azonosítás használható a hozzáférés hitelességének biztosítására szerverekhez, adatbázisokhoz, egészségügyi vagy pénzügyi adatokhoz. Michelberger szerint a logikai védelem alatt az adatok integritása, vírusvédelem, számítógépes hozzáférés és titkosítási eljárások érthetők [43]. A biometrikus minta alkalmazása ezen a területen csökkenti a biztonsági szint végfelhasználótól való függését, valamint érvényesülnek az egyszerűségi és kényelmi szempontok, tekintve, hogy nem kell elvárni a felhasználótól, hogy hosszú, bonyolult, nehezen megjegyezhető (de nehezen is törhető) jelszavakat használjon. [44]
11. **Távoli hitelesítés:** A számítógépes rendszerek távoli elérése és a jogosultság hiteles eldöntése alapvető feladat az információbiztonság megteremtésekor. Leggyakoribb alkalmazásai a telefonos, mobil vagy internet banki szolgáltatások, webes applikációk és vállalatok dolgozóknak biztosított távoli hozzáférései a belső rendszerekhez. [45]

12. **Vásárlói azonosítás:** A kereskedelmi tranzakciók, vásárlók azonosítására napjainkig elsősorban PIN-kód, kulcskártya (token) és aláírás használatos. Biometria alkalmazásával mérsékelhető vagy megszüntethető ezek használata, és a biztonságérzet is jelentősen növelhető. További lehetőség, hogy olyan felhasználói köröket vonjanak be a kereskedelembe, akik a hagyományos azonosítási eljárásokat nem tudják készség szinten használni, például a nagyon fiatalok és az idősek. [46] [47]
13. **Mobileszközök biometrikus hozzáférésvédelme**: Androidos készülékekben, laptopokban már a 2000-es évek elejétől folyamatosan megjelentek biometrikus megoldások. Az áttörés azonban 2014-ben következett be, amikor az Apple az iPhone 5S készülékében mutatta be először az ujjnyomat-azonosítást, így több millió fogyasztót vonva be a biometria lelkes felhasználói közé. Ugyanekkor természetessé vált, hogy az Android operációs rendszert futtató telefonokon már elérhetőek a különböző biometrikus azonosító eljárások, mint az arcfelismerés, az ujjnyomat-, és újabban íriszazonosítás. Az iPhone 6S készülékében már elérhetővé vált a biztonságos mobilos fizetés az Apple Pay szolgáltatáson keresztül. Fontos azonban megemlíteni, hogy a biometrikus azonosítás mellett minden mobileszköz megkövetel egy fallback opciót, amely a hagyományos azonosítási megoldások egyike. Újraindításnál a telefont nem lehet biometrikus azonosítás segítségével feloldani, csak hagyományosan PIN-kóddal vagy feloldási mintázattal, amely megerősítést napjainkban már többször kér a telefon. Ez azt jelenti, hogy a telefon alapvető védelme csak olyan erős, amilyen erősre a fallback opciót állította a felhasználó. Mivel a legtöbb telefonban nem található kötelező jelszópolicy (tehát nem követelik meg, hogy a fallback opció egy erős jelszó legyen), a biometrikus azonosítás a telefon feloldására egy egyszerű kényelmi funkcióvá redukálódhat. Például egy mintázatalapú[14] képjelszó esetén a biometria csak attól kíméli meg a felhasználót, hogy azt minden alkalommal le kelljen rajzolni és lehetővé teszi az egy mozdulattal történő képernyőfeloldást. Azonban bárki, aki a felhasználó tudta nélkül megfigyeli a mintát (amelyet jelentősen könnyebb végrehajtani, mint egy bonyolult jelszót megszerezni) egyszerűen átléphet a biometrikus védelem fölött, ezután akár a saját mintáját is rögzítheti az eszközben. Mivel a rögzített minták számának megtekintéséhez mélyen a menürendszerbe kell belépni (jellemzően az új minták rögzítését lehetővé tévő biztonsági menübe, a felhasználók ritkán teszik ezt meg. Ennek következtében, amennyiben a jogos

[14] Egy 3 × 3-as, körökből álló rács, amelyen az egyes köröket töréspontnak használva ki kell rajzolni egy egyenes vonalszakaszokból álló mintázatot, amely a feloldáshoz szükséges. Az egyes vonalak metszhetik egymást, azonban egy kör csak egyszer érinthető.

tulajdonos nem használt fel minden lehetséges minta memóriát,[15] úgy a támadó gyakorlatilag észrevehetetlenül rögzítheti a saját mintáját, ezzel tartós hozzáférést biztosítva a készülékhez, de akár ki is zárhatja a tulajdonost a készülékből. [48]

A mobileszközök biztonsági beállításai lehetővé teszik, hogy adott számú (eszközönként eltérő) hibás próbálkozás után automatikusan töröl minden adatot, amely az eszközön található. További lehetőség a biometrikus azonosítás kiterjesztése az internetes honlapokra történő bejelentkezéshez. Ekkor a belépéshez szükséges felhasználónév-jelszó páros az ujjnyomatra cserélődik, amely egyértelműen azonosítja a felhasználót.

A biometrikus megoldások alkalmazási területei szerteágazóak és a szakirodalmi áttekintésből jól látszik, hogy az egyes területek különböző követelményrendszereket fogalmaznak meg biometrikus eszközöknek. [49]

1.3 A biometria és az emberi hozzáállás

Kutatásom során folyamatosan abba a problémába ütköztem, hogy nincs olyan biometrikus eszköz vagy rendszer, amelyik bármilyen alkalmazási területen ugyanolyan jól teljesítene. Ezért az előző pontban ismertetett területeket különböző tényezők alapján osztályozni és csoportosítani fogom, mivel ezeknek szignifikáns különbségei vannak. Elemzésükkel kiderül, hogy a kritikus alkalmazások a beléptető- és munkaidő-nyilvántartó rendszerek lesznek.

1. **Az azonosítandók létszáma:** A biometrikus azonosító berendezések és algoritmusok egyik legnagyobb kihívása a regisztrált létszám. Míg egy okostelefonnak általában egy, maximum néhány embert kell felismernie, addig egy tömegtartózkodású objektumban az azonosítandók köre akár több ezer vagy tízezer is lehet, és ezt a létszámot sokszor csak biometrikus minta alapján (1:N) akarják azonosítani a vezetők. A probléma oka a rendszerek működésének valószínűségi tulajdonsága. A biometrikus eszközöket jellemző általános valószínűségi változók, mint a FAR, FRR, EER[16] még akkor sem jelentenek biztos elfogadást vagy elutasítást, ha nagyon jó az eszköz és az algoritmus. Általában az EER algoritmikus értékének 0,01%-ot adnak meg a gyártók. Ezt vizsgálva 10.000 felhasználónként biztosan lesz egy problémás eset, azonban ezek az értékek a

[15] A legtöbb készülékben alacsony számú mintát lehet tárolni, technológiától függően 1–5 darabot.
[16] EER (Equal Error Rate): egyesített hibaarány – az az arány, ahol a téves elfogadás (FAR) és a téves elutasítás (FRR) közel megegyezik egymással. Ez a pont a berendezés és algoritmus optimális beállítsa, a két görbe itt metszi egymást, innen biztonságosabb vagy kényelmesebb irányba elmozdulni csak a másik rovására történhet. Kényelmesebb a rendszer, ha kevesebbszer utasítja el a jogosult felhasználókat tévesen, biztonságosabb, ha alacsonyabb a hibás elfogadási aránya.

valóságban 1-2 nagyságrenddel rosszabbak, így viszont már 100 felhasználónként akad néhány hiba. [50]

2. **Kényelmi vagy kötelező a használat:** Amikor a felhasználóknak érdekük fűződik a használathoz, teljesen más lesz a hozzáállásuk a rendszerekhez. Például a mobiltelefonok ujjlenyomat vagy arcfelismerő hozzáférési védelmei egyértelműen kényelmi szolgáltatások. A másik véglet a munkaidő-nyilvántartás, melyet a felhasználók a legjobban elutasítanak.
3. **Alternatív azonosítási eljárás lehetősége:** Lehetséges és elfogadható-e alternatív azonosítása a felhasználónak egy alkalmazásban? Rendészeti és katonai alkalmazásoknál minden esetben rendelkezésre áll a hagyományos, élőerő-alapú azonosítás igénybevétele, de például a mobileszközöknél is használható az alternatív PIN-kód vagy minta.
4. **Pozitív vagy negatív azonosítás:** Bunyitai a pozitív azonosítást az 1:1 felismerésre használja, míg a negatívat az 1:N-re.[17] [51] Értekezésemben másképp használom ezt a megközelítést, mégpedig abból a szempontból, hogy a humán erőforrásnak mikor kell beavatkozni az adott alkalmazásban. Pozitív az azonosítási módszer, amikor egy populációból a valamilyen oknál fogva a kiemelt egyedeket keressük, például VIP azonosítás, körözött személyek vagy terroristák megtalálása, tehát akkor kell reagálni a humán erőforrásnak, ha pozitív egyezést talál a biometrikus személyazonosító rendszer. Ilyen esetekben a pozitív találatokat kell további vizsgálat alá venni. Negatív azonosítású egy rendszer, ha a célja a jogosultak biztonságos felismerése, és akkor kell a humán erőforrásnak beavatkozni, ha valakit elutasít a rendszer.

1.4 Az alkalmazások osztályozása

Az 1.2 fejezetben ismertetetett alkalmazásokat osztályozom az 1.3 fejezet szempontjai szerint és ezek alapján meghatározom, hogy melyekkel érdemes foglalkozni a továbbiakban. Az osztályozást az alábbi táblázat tartalmazza. [21] A táblázatban szereplő adatok tartalomelemzés, szakmai tapasztalat és szakértői mélyinterjúk alapján kerültek összeállításra.

[17] Az 1:1 azonosítás, amikor a felhasználó valamilyen egyéb módon állítja magáról a személyazonosságát, például egy kártyával vagy egyedi PIN-kóddal. 1:N azonosításnál csak a biometrikus mintáját mutatja be, és a teljes adatbázisban történik keresés.

1. táblázat: Biometrikus alkalmazások osztályozása; forrás: [26]

Alkalmazás	**Adatbázis tipikus létszáma**	**Kényelmi/ kötelező**	**Alternatív módszer**	**Pozitív/negatív**
Rendészeti	1.000.000+	Kötelező	Van	Pozitív
Határforgalom ellenőrzése	1.000.000+	Kötelező	Van	Pozitív
Regisztrált utas	1.000.000+	Kötelező	Van	Pozitív
Háttérellenőrzés	100.000+	Kötelező	Van	Pozitív
Beléptetés	**1–5.000**	**Kötelező**	**Problémás**	**Negatív**
Munkaidő-nyilvántartás	**100–5.000**	**Kötelező**	**Nincs**	**Negatív**
Videó megfigyelés	1.000.000+	Kötelező	Van	Pozitív
Csalások	100.000+	Kötelező	Van	Pozitív
Vagyonvédelem	10-100	Kötelező	Van	Pozitív
Logikai védelem	10.000+	Kötelező/ Kényelmi	Van	Pozitív
Távoli hitelesítés	10–100.000+	Kényelmi	Van	Pozitív
Vásárlói azonosítás	10.000+	Kényelmi	Van	Pozitív
Mobil	1–10	Kényelmi	Van	Pozitív

Felhasználói vélemények alapján kevésbé érdekesek azok az alkalmazások, amelyeket kényelmi okok miatt használnak vagy létezik alternatív azonosítási lehetőségük (például egy reptér, ahol, ha valakinek nincs biometrikus útlevele, a hagyományos eljárást használja), hiszen aki nem akarja vagy nem képes rá, az nem használja a biometrikus eljárást.

A fenti táblázat elemzésében jól látszik az a két alkalmazási terület, ahol kötelező a használat, nincs alternatívája a biometrikus azonosításnak, és negatív a kiválasztás, azaz a teljes felhasználószámnak használnia kell a rendszert. A következő fejezetben ezeket részletesen meg is vizsgálom.

1.5 Kritikus alkalmazások

A beléptető rendszerek az elektronikus védelem egyik meghatározó területét képezik. Rendeltetésük, hogy az objektumba csak a jogosult személy léphessen be. Az objektumokon belül további jogosultsági szintek alakíthatók ki területenként, például aki a főbejáraton beléphet, még

nem biztos, hogy a szerverhelyiséghez is kap hozzáférést. A beléptető rendszer alapvetően a személyek, a védett objektum és annak részeihez történő hozzáférést szabályozza, azonban a tulajdonosnak, üzemeltetőjének lehetősége van a rendszer más szolgáltatásait is igénybe venni, ilyen például a munkaidő-nyilvántartás. [40]

Az 1. táblázat bemutatja azokat az alkalmazásokat, ahol a biometrikus azonosítás bevezetése a legnagyobb kockázattal jár.

1.5.1 Létszám

Az alacsony, körülbelül néhány tíz fős alkalmazásokban nem okoz problémát a biometria használata, mert könnyen letesztelhető bevezetés előtt a teljes létszámra, átláthatóbb, jobban kontrollálható a működés. Az alacsony létszámból fakadóan statisztikailag is kisebb az esélye a ténylegesen problémás mintáknak. [52] A gyakorlatban azt jelenti, hogy ebben a tartományban bármilyen biometrikus eszköz a specifikációknak megfelelően fog működni, ha azt egyébként más alkalmazási körülmények nem befolyásolják. Ilyen alkalmazási körülmény lehet – ami jelentősen ronthatja időszakosan a rendszer teljesítményét –, amikor az arcfelismerő berendezést kültéren telepítik, ahol a nap bizonyos időszakokban belesüt a szenzorba, ezzel megzavarva vagy ellehetetlenítve az eszköz optimális működését. [53] Egy másik valós szituáció alapján az egyik felhasználónak egyáltalán nem működik az ujjnyomat-azonosító, mert nincs ujjlenyomata, és ezért a teljes technológiát elvetik, holott más biometrikus megoldás megfelelően működhetne. [54]

A biometriaalapú személyazonosító rendszereknek kihívást jelentő felhasználói létszám a tömegtartózkodású objektumoknál merül fel, és itt már statisztikailag is bizonyos, hogy szignifikáns mennyiségben fordulnak elő téves esetek.

1.5.2 A használat motivációja

Ahol a felhasználók saját akaratból vagy kényelmi szempontok miatt használják a biometriát, az együttműködésük teljesen más, mintha rájuk kényszerítik azt. Ebből a szempontból a beléptetés és munkaidő-nyilvántartás szintén kritikus alkalmazásnak minősül. A biometrikus megoldásoknál a legalacsonyabb a felhasználói elfogadottság. [24]

A munkaidő-nyilvántartás feladata, hogy rögzítse a dolgozók jelenlétét (és bizonyos esetekben tevékenységét), majd az összesített adatokat hó végén átadja a bérszámfejtő szoftver részére. Egy pontos munkaidő-nyilvántartó rendszer a vállalat számára előnyt jelent, mivel komoly megtakarításokat jelent, ha csak a ténylegesen elvégzett munka után fizet a munkáltató. Előnyös

azonban a munkavállalók számára is, mivel konfliktushelyzetben egyértelműen eldönthetők a viták a megfelelő adatok rendelkezésre állása esetén.

Empirikus tapasztalataim alapján, valamint az elmúlt 10 évben számos HR-konferencián részt véve, nagyvállalatok HR-vezetőivel egyeztetve kimondható, hogy a munkaidő-nyilvántartás vezetésénél a munkavállaló és munkáltató között általában egymással ellentétes érdekek ütköznek. Míg a munkáltató érdeke, hogy a lehető legrövidebb munkaidőt számolja el, a munkavállalóé pedig, hogy a lehető legtöbbet. A hagyományos munkaidő-nyilvántartás megkerülésének különböző módszereit ismerjük, mint elsősorban a „*buddy punching*". [37] Ez esetben egy tudás- vagy birtokalapú azonosító segítségével nem az adott ember azonosítja magát, azt a látszatot keltve, hogy a területen tartózkodik (és munkát végez), ezzel elfedve az esetleges késéseket és igazolatlan hiányzásokat, hanem egy másik kollégáját kéri meg erre. Rosszabb esetben kölcsönadják egy másik személynek, aki helyettük megy be illetéktelenül az objektumba. A következő neuralgikus terület a túlóra elszámolása, mert ilyenkor a munkavállalót jelentős pótlék is megilleti a pluszban elvégzett munkáért.

A visszaélések jellemzően akkor következnek be, ha a dolgozók komolyabb felügyelet nélkül, rugalmas munkarendben dolgoznak, vagy éppen túl nagy a létszám ahhoz, hogy hatékonyan ellenőrizhető legyen a blokkolás.

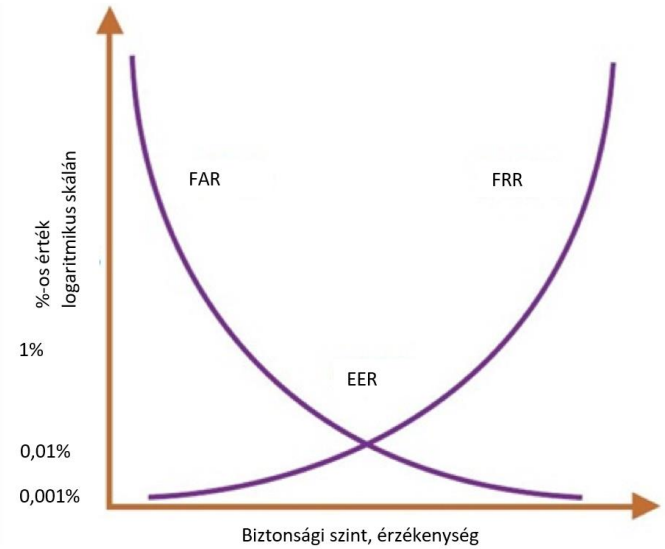
1.5.3 Alternatív azonosítási módszer lehetősége

Az előző fejezetben kifejtett felhasználói ellenérdekek és a működési jellemzők okozzák, hogy a nagy létszámú beléptetésnél és munkaidő-nyilvántartásnál nem, vagy nagyon nehezen adható alternatív belépési módszer. Alternatív módszeren értem a hagyományos, nem biometrikus személyazonosítási eljárásokat: tudás-, birtokalapú vagy humán erőforrással megoldott. A hagyományos azonosítási módszerek természetesen ez esetben is rendelkezésre állnak beléptetés és munkaidő-nyilvántartási célokra is. Ezek jellemzően PIN-kódos, kártyás vagy humánerőforrás-alapú megoldások, mégsem célszerű ezeket használni, mert egyrészt jelentősen növeli az illegális belépés kockázatát (ez addig nőhet, amíg már nincs értelme bevezetni a biometrikus rendszert), másrészt gyakori, hogy akik ki akarják játszani a hiteles munkaidő nyilvántartását, azok szabotálják a biometrikus rendszert és az alternatív megoldást igyekeznek kikényszeríteni. Ha ennek a vállalatok teret engednek, rossz esetben a biometrikus beruházást ki kell vezetni a használatból. [52]

1.5.4 A kiválasztás típusa

Az 1.3 fejezetben pozitív-negatív kiválasztásra adott definícióm alapján a munkaidő-nyilvántartás és beléptetés esetén a kiválasztás negatív, mivel meg kell állapítani, hogy ki nem jogosult belépésre és ekkor kell beavatkozni a humán erőforrásnak. Meg kell vizsgálni, hogy a biometrikus azonosító eszközök teljesítménymutatói közül melyek a legfontosabbak. A releváns teljesítménymutatók ebben az esetben a már definiált FAR, FRR, EER, működési idők és a különböző beregisztrálási (enrollment) értékek.

A FAR és FRR értékek általában egy közös pontra, az EER-re vannak beállítva alapértelmezetten a biometrikus eszközöknél, ezek jellemző értéke 0,001%–0,1% (4. ábra.).



4. ábra: Biometrikus rendszerek érzékenység függése, forrás: [26] alapján saját szerkesztés.

Biztonsági rendszer lévén első pillantásra a hibás elfogadás (FAR) értéke tűnik a legnagyobb kockázatnak, azonban ez önmagában nem igaz. A tömegtartózkodású objektumoknál két tényező az, ami ezt módosítja. Az első, amikor a belépési pontokat nem, vagy csak rendkívül nehezen lehet úgy kialakítani, hogy valóban csak egy ember mehessen át rajtuk. Gondoljunk csak egy kamionbejáratra vagy rakodórámpára, ahova párhuzamosan 10-15 kamion is be tud állni. Itt élőerő felügyelete nélkül csupán technikával nem garantálható, hogy nem jutnak be illetéktelenek. A másik szempont, hogy a fizikailag védett értékek jellemzően sokkal könnyebben támadhatók más módszerekkel (pl. hackelés, social engineering stb.), mint személyek illetéktelen bejuttatásával.

Másik nézőpontból, a hibás elutasítás (FRR) nem megfelelő értéke viszont teljesen meghiúsíthatja egy rendszer üzemszerű használatát. Nagy létszámú beléptetésnél még akkor is komoly problémát

jelent a magas FRR, ha egyébként a védendő objektum biztonsági szintje ezt indokolja és az ott dolgozók erre ki vannak képezve. A gyakorlatban egy ilyen helyzetben hibás elutasításnál akár már az első alkalommal is be kell avatkoznia az élőerőnek és lefolytatni a hitelességi vizsgálatot.

Munkaidő-nyilvántartási alkalmazásnál egyéb szempontok is közrejátszanak. Ahhoz azonban, hogy ezt vizsgálni lehessen, tisztázni kell, hogy milyen hátrányokkal jár egy hibás munkaidő-kimutatás. A legjobb esetben extra munkaórákat igényel a hibás munkaidőadatok javítása, amit produktív tevékenységekre is lehetett volna fordítani. Legrosszabb esetben azonban jogi következményei lehetnek, mint egy munkaügyi per vagy bírság. Éppen ezért fontos, hogy minden felhasználó csak a saját maga nevében tudja használni a rendszert (ez a rendszer bevezetésének a célja). Ugyanakkor, ahogy az az előző fejezetben kifejtésre került, egy rosszul összeállított rendszer arra ösztönözheti a dolgozókat, hogy megpróbálják azt megkerülni, vagy akár ellehetetleníteni. Emiatt nem elég, hogy a rendszer nagy biztonsággal meg tudja határozni azt, hogy a mintát prezentáló személy megegyezik-e az adatbázisban szereplő személlyel. Arra is szükség van, hogy ezt határozottan tegye, tehát ne utasítsa el tévesen a felhasználót, de legalábbis a lehető legkisebb mértékben. A biometrikus azonosítás a tudás- és birtoklásalapú azonosítási módszerekhez képest minden esetben relatív kellemetlenséget okoz a felhasználónak, mivel minden esetben extra erőfeszítést kell tennie a sikeres azonosításhoz, azaz szükséges az együttműködése. Ha ez nem hatékony működéssel párosul, úgy a felhasználó frusztráltsága könnyen megnövekedhet (főleg akkor, ha már alapvetően negatív diszpozícióval rendelkezik a rendszer felé). A működési idők tekintetében is lényeges a „jó” teljesítmény (ahol a „jó” mindig egy relatív fogalom az aktuális felhasználó értékelésének függvényében). Annak meghatározása, hogy mi jelent a „gyors” teljesítmény, nem egyszerű feladat, hiszen azt mindenképpen el lehet mondani, hogy még a leggyorsabb biometrikus azonosító eszköz is lassabb, mint a kártyás rendszer – amely így ismét kényelmetlenséget okoz a felhasználó számára. A regisztrációs teljesítmény pedig mind a rendszer működésének, mind bevezetésének szempontjából fontos. Az üzemeltető szempontjából a legfontosabb kérdés, hogy a rendszer minden felhasználóra működni fog-e megfelelő biztonsági szint mellett (például kézgeometria alkalmazása esetén feltétel a teljes kéz, azaz meg kell lennie minden ujjnak). A felhasználók szempontjából azonban lényegesebb, hogy jó eséllyel a regisztráció folyamán találkoznak először az adott rendszerrel és az első benyomás a későbbiekben kulcsfontosságú lehet a rendszerhez való későbbi hozzáállás tekintetében.

1.5.5 További tényezők

A továbbiakban összegyűjtöttem néhány objektíven nem mérhető, mégis lényeges szempontot, amely szintén befolyásolja a rendszer elfogadottságát:

- **Tévhitek:** Egyes technológiák esetében a tévhitek domináns helyet foglalhatnak el a kevésbé tájékozott felhasználók attitűdjének kialakításában. Ilyen az íriszolvasókkal szemben előforduló bizalmatlanság. Filmekben gyakran látható „szemszkennelést" (amelyet ott retinavizsgálatnak neveznek, azonban ezek a szemet azonosító eszközök döntő többségben az íriszt vizsgálják), ahol egy lézersugár segítségével vizsgálják a mintát. Emiatt a felhasználók tarthatnak attól, hogy károsodik a szemük, pedig a valóságban az íriszvizsgálat kamerával és közeli infratartományú (NIR) fénnyel történik, amely teljes mértékben ártalmatlan a szemre. Egy másik tévhit az eszközök piszkossága. A felhasználók gondolkodás nélkül megfognak egy szennyezett kilincset, mégis aggódnak, ha használniuk kell egy biometrikus azonosító eszközt a piszok és az abból eredő problémák miatt. A megfelelő oktatás és az emberek elkötelezése a rendszerek mellett vagy kontaktusmentes technológiák alkalmazása megoldhatja ez utóbbi problémakört. [112]
- **Privacy:** A korábbiakban már említésre került, hogy a biometrikus mintát gyakran a vállalatok saját adatbázisukban tárolják (bár egyes országokban kötelező a felhasználó birtokában lévő kártyán tárolni).[18] A felhasználók aggódhatnak egyrészt amiatt, amennyiben az adataikat a vállalat a beleegyezésük nélkül kiadja egy harmadik félnek. [55] Másrészt az adatok általános biztonsága miatt, hiszen az adatbázis és környezete biztonsága nagyban függ attól, hogy ki férhet hozzá. A biometrikus eszközök által generált és használt sablonok irreverzibilis algoritmusokat használnak, melyek biztonságosak, azonban ezt a végfelhasználók nem feltétlenül tudják, de ha tudják is, kételkednek benne – megjegyzem sok esetben jogosan, mert mi is találkoztunk olyan mintával, amely visszafejthető volt, sőt a kód mellett tárolásra került a biometrikus minta képe is. [56]
- **Morál:** A tisztességes dolgozók úgy érezhetik, hogy a vezetők nem bíznak meg bennük, emiatt feszültség alakul ki, holott a rendszer ebben az esetben is az ő érdekeiket szolgálja, hiszen az kiszűri a hanyag munkatársakat, melyre nem kell további erőforrásokat áldoznia a vállalatnak, ezáltal az alapbér növekedhet. [37] Ezért

[18] A NAIH (Nemzeti Adatvédelmi és Információszabadság Hatóság) hatályos állásfoglalásai (2017. 03. 19.) alapján Magyarországon is.

rendkívül fontos, hogy a rendszer előnyeiről és szükségességéről a dolgozók folyamatosan tájékoztatva legyenek. Azon dolgozók körében is csökkeni fog a morál, akik ténylegesen meg akarják téveszteni a rendszert, hiszen ezt a lehetőséget jó eséllyel elveszítik. [35]

Fenti faktorok figyelmen kívül hagyása hiba a rendszer üzemeltetőjének részéről, ugyanis komoly munkavállalói elégedetlenséget szülhet, melyek megoldása többnyire bonyolultabb, mint a felmerülő problémákat megelőzni megfelelő előkészítéssel, tervezéssel és kommunikációval. Ez nem jelenti azt, hogy a rendszernek alkalmazkodnia kell minden dolgozói igényhez, ugyanakkor világossá kell tenni a bevezetés célját és annak előnyeit a munkavállalókra nézve is. [57]

A tömegtartózkodású objektumoknál bevezetett biometrikus beléptető és munkaidő-nyilvántartó megoldások kritikus pontja, hogy a rendszer képes-e mindenkit kellően gyorsan beléptetni, miközben fenntartja az elvárt biztonsági szintet is.

1.6 A fejezet összefoglalása

Szakmai interjúim alapján sokszor előkerült, hogy a biztonsági szakemberek és üzleti döntéshozók fejében felmerül a biometrikus felhasználóazonosítás igénye, azonban hajlamosak elfeledkezni arról, hogy a rendelkezésre álló technológiák és eszközök nem alkalmasak valamennyi feladatra minden körülmények között. Itt nyer értelmet a MOA (Mission Oriented Application – feladatorientált megközelítés) megközelítés, amely a biometrikus rendszerek tekintetében nemcsak egy elméleti kérdés, hanem nagyon éles és kritikus határvonal húzódik a használhatatlan és az elfogadható megoldás között.

Tartalomelemzéssel és szakértői mélyinterjúk során összegyűjtöttem, rendszereztem és definiáltam a biometria alkalmazási területeit, illetve azokat a szempontokat, amelyek általánosan elfogadottak a biometrikus megoldások osztályozásánál, mint az univerzalitás, egyediség, állandóság, megszerezhetőség, teljesítmény, elfogadottság és megtéveszthetőség. Ezután a felhasználók hozzáállását elemeztem és kiemeltem négy olyan szempontot, amelyek a használati körülményeket osztályozzák és szükségesek ahhoz, hogy az adott alkalmazásról el tudjuk dönteni, hogy mely biometrikus eszköz lesz a megfelelő. Ez lehet a létszám, hogy a használat jellege kényelmi vagy kötelező, létezik-e alternatív megoldás, valamint a kiválasztás módja pozitív vagy negatív-e.

Az azonosított alkalmazási területeket a használati körülmények függvényében osztályoztam, hogy melyek **a kritikus területek:** ezek **a beléptetés és a munkaidő-nyilvántartás,** ennek okait részletesen elemeztem.

Megadtam azokat a szempontokat, amelyeket a döntéshozóknak mindenképpen figyelembe kell venniük üzleti-biztonsági szempontból annak érdekében, hogy sikeres biometrikus bevezetési projekteket tudjanak menedzselni.

A következő két fejezetben folytatom a kritikus alkalmazások további elemzését. Egyrészről matematikai modellt állítok fel, és levezetem hogyan kell a létszámra méretezni a belépési pontokat, másrészről az emberek elfogadási küszöbét mérem/elemzem kvalitatív és több lépcsős kvantitatív kutatással.

2 TÖMEGTARTÓZKODÁSÚ OBJEKTUMOK BELÉPÉSI FOLYAMATÁNAK ELEMZÉSE SORBANÁLLÁSI MODELLEL

A beléptető rendszerek biztonsági felhasználása természetessé vált a vállalati alkalmazásokban. Szakmai észrevételek alapján egyetértek azzal, hogy helyesebb lenne átléptető rendszernek vagy átléptetésnek hívni a folyamatot, mivel jellemzően nemcsak beléptetésre, hanem kiléptetésre is használatosak az áthaladási pontok. Értekezésemben mégis a beléptetés fogalmánál maradok, mivel az MSZ EN 50133-1:2006 *„Riasztórendszerek. Beléptetőrendszerek biztonságtechnikai alkalmazásokhoz. 1. rész: Rendszerkövetelmények”* szabvány egyértelműen így használja a fogalmat. [58]

Általában különösebb megfontolást és méretezést [59, p. 59 § (8)] – a menekülési útvonalakon szükséges előírásokon túlmenően – nem igényelnek ezek a rendszerek. Problémák ott merülnek fel, ahol vagy hosszadalmas a beléptetési procedúra az objektum biztonsági fokozata miatt (fémkereső kapu, csomagátvizsgálás) vagy nagy létszámú felhasználó érkezik rövid idő alatt.[19] A belépési folyamat egyes lépései jól azonosíthatók és becsülhető az időtartamuk, azonban biometrikus beléptetés esetén valószínűségi változóval leírható tevékenységet viszünk a rendszerbe, mely működési bizonytalansága komoly kockázatot jelent a teljes rendszerbevezetés sikerességének összefüggésében. Ezért fontos, hogy kidolgozásra kerüljön egy olyan eljárás, amely az üzleti és biztonsági kérdésekre egyértelmű, megbízható válaszokat szolgáltat már a tervezési szakaszban. [52]

Jelen fejezetben tudományos megközelítéssel vizsgálom a beléptető rendszereket, amelyek egy objektumba történő személybeléptetés a belépés előkészítésére, az ellenőrzési feladatokra, az azonosításra, és az APAS (Access Point Actuators and Sensors – Beléptetőpont működtetett szerkezetei és érzékelői)[20] működtetésére épülő sztochasztikus folyamatként írhatók le. [60] A belépési folyamat modellvizsgálatával megállapítható, hogy a távozások függetlenek a múltbeli eseményektől, az csak a vizsgált időpont állapotától függ, mely alapján matematikailag Markov-folyamatnak tekinthető és sorbanállási modellel leírható. [61]

A fejezet célja a fenti üzemeltetéselméleti, valószínűségszámítási, matematikai modellezési, valamint műszaki diagnosztikai munkák tudományos eredményeinek, módszereinek összegzése

[19] A két jelenség együttes fellépésére jó példa a repülőtér, ott viszont azért nem probléma, mert az emberek kivárják a sorukat, akár több órás várakozási idővel is. Ez nyilván nem elfogadható egy munkahelyi beléptetésnél.
[20] Például egy mágneszár, forgóvilla vagy nyitásérzékelő.

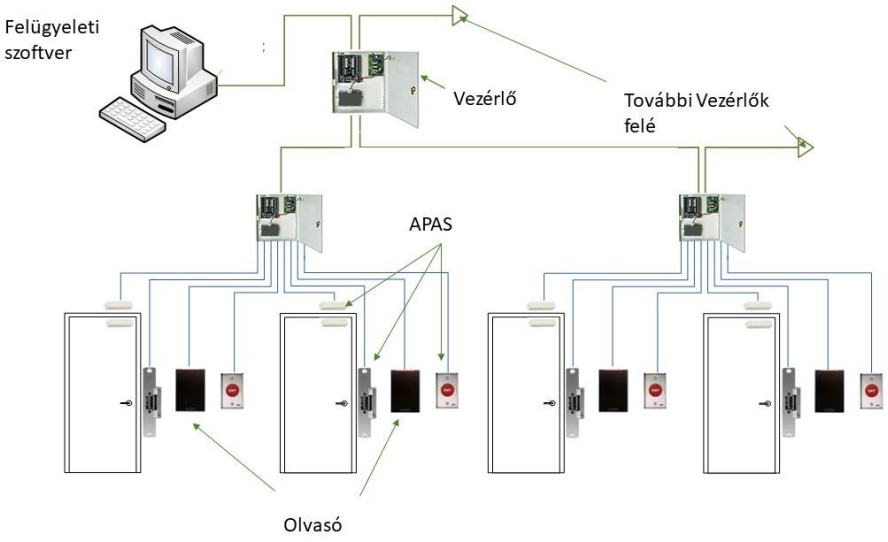
és a kitűzött specifikus alkalmazás a beléptetési folyamatainak sorbanállási modellel történő leírása, illetve gyakorlati alkalmazásuk vizsgálata.

Fontos kiemelni azt a tényt, hogy a matematikai modell kizárólag statisztikai alapokon közelíti meg a problémát, ezért a **várakozási idők kizárólag átlagos** értékeket tudnak megadni. Ebből az következik, hogy a felhasználók és szakemberek „valóságérzékelése" vagy „gyakorlati tapasztalata" nem biztos, hogy visszaigazolja a kapott eredményeket.

2.1 A beléptetés

A beléptető rendszer Bunyitai szerint: *„Komplex elektromechanikai-informatikai rendszer, amely telepített ellenőrző pontok segítségével lehetővé teszi objektumokban történő személy- és járműmozgások hely, idő és irány szerinti engedélyezését vagy tiltását, az események nyilvántartását, visszakeresését."* A beléptető rendszer feladata pedig: *„a belépő azonosítása, a belépési jogosultság megállapítása, az esemény dokumentálása, valamint az áthaladás szabályzása"*. [62, p. 18]

A beléptető rendszerek általános felépítése:



5. ábra: Beléptető rendszerek általános felépítése, forrás: saját szerkesztés

- **Olvasók:** Az azonosítási ponthoz érkező felhasználót azonosítja. Lehet kódos, kártyás, biometrikus vagy ezek kombinációja.
- **Vezérlők:** Az olvasó által azonosított kódról dönti el, hogy az adott helyen és időben jogosult-e a belépésre a felhasználó.

- **APAS:** A rendszer által vezérelt fizikai korlátozó és mechanikus eszközök, illetve érzékelők tartoznak közéjük. A vezérelt eszközök lehetnek: mágneszár, ajtótartó mágnes, forgóvilla, forgókereszt, forgókapu, automata ajtó stb. Érzékelők például infrakapu, nyitás- vagy mozgásérzékelő.
- **Felügyeleti szoftver:** A rendszer és felhasználói beállítások kezelésére, valamint a rendszer begyűjtött jelzéseinek feldolgozására, naplózására, tárolására szolgáló alkalmazás.

2.1.1 A biometrikus beléptetés

A világban tapasztalható biztonságérzet csökkenésével párhuzamosan egyre nagyobb az igény a felhasználók hiteles azonosítására. Balla József értekezésében ezt így fogalmazza meg, amellyel teljesen egyetértek: *„Az EU polgárai számára a legfőbb prioritást a biztonság jelenti, amely biztonságot folyamatosan fenyegeti és »ostromolja« többek között a terrorizmus, a szervezett bűnözés, a kábítószerkereskedelem, az emberkereskedelem és az illegális migráció is."* [30, p. 5] Egyedül a biometrikus azonosítás az a technológia, amely az emberek egyedi, lehetőség szerint megmásíthatatlan és hamisíthatatlan tulajdonságait vizsgálja. A jelenlegi rendszerek sem sebezhetetlenek (ujjnyomat, arcfelismerő, ujjerezet, kézerezet, kézgeometria és íriszazonosító berendezések sebezhetőségeit mutattam be a Hacktivity nemzetközi etikus hacker konferencián 2011, 2012, 2013, 2014 és 2015-ben), azonban a folyamatos fejlesztéseknek köszönhetően egyre magasabb biztonsági és kényelmi elvárásoknak felelnek meg. [13] [63]

Biometrikus adatokon alapuló azonosítási technológiák csoportosítása: [64]

- Képalkotás-alapú technológiák:
    - ujjnyomat-azonosítás;
    - íriszazonosítás;
    - arcazonosítás;
    - erezetazonosítás;
    - kézgeometria-azonosítás; [65]
    - aláírás vizsgálata.
- Nem (vagy nem közvetlenül) képalkotással dolgozó technológiák:
    - hangazonosítás;
    - DNS-vizsgálat;
    - viselkedésalapú vizsgálatok. [66]

A beléptetési folyamatban a biometrikus azonosítás a „minta pozícionálása” és az „algoritmikus feldolgozás” lépéseket befolyásolja. A sorbanállási modellt a biometrikus eszközök kiszolgálási tényezője módosítja (8. ábra). A kiszolgálás – ellentétben a hagyományos azonosítási eljárásokkal – valószínűségi változó, mely legnagyobb mértékben a rendszert jellemző FRR értéktől függ. Definiálható ξ valószínűségi változó a következő módon: legyen egy adott időszakban az n darab regisztrált felhasználó egyszeri belépése esetén r azok száma, akiket a rendszer elutasít. Ekkor ξ definíció szerint binomiális eloszlású:

$$P(\xi = r) = \binom{n}{r} p^r (1-p)^{n-r}; r = 0, 1, 2, \dots, n \quad (1)$$

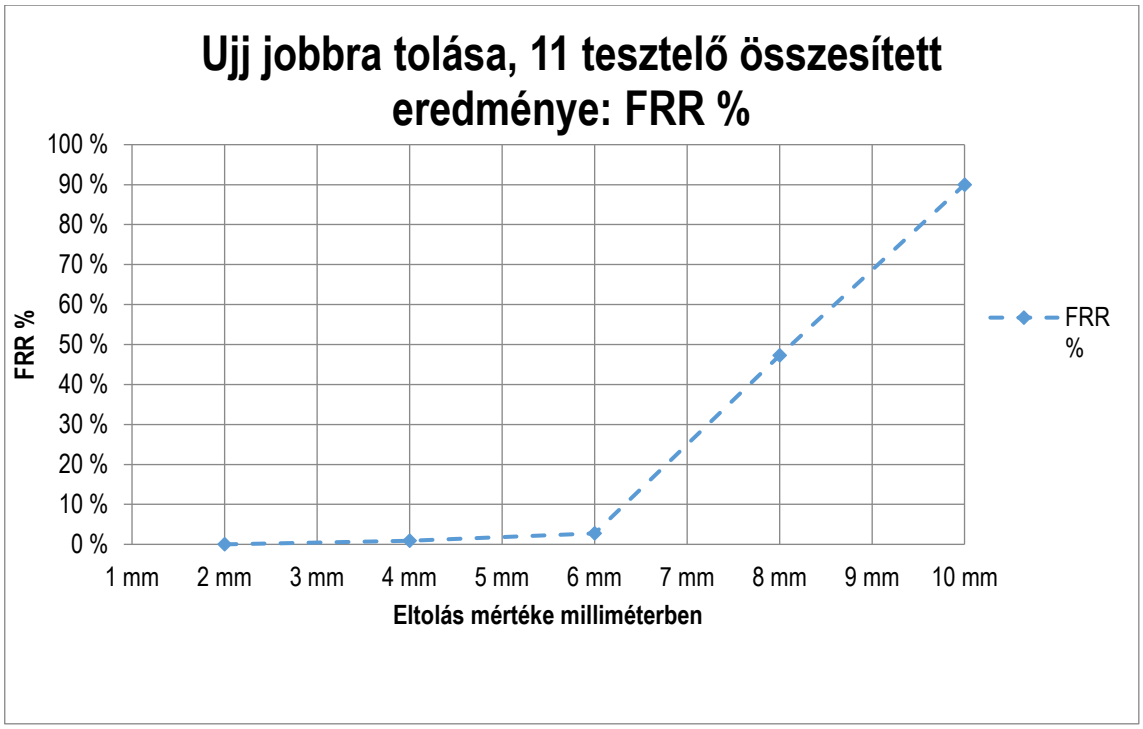
A relatív gyakoriság sztochasztikusan konvergál a p valószínűséghez, ha a megfigyelések száma, n minden határon túl növekszik. Amennyiben ezt a paramétert szeretnénk megbecsülni, akkor a legjobb becslés a vizsgált esemény relatív gyakorisága (Maximum Likelihood), ami esetünkben éppen az FRR-értékkel egyezik meg. Részletes levezetése Hanka *Matematikai módszerek a biometriában 1.* publikációjában megtalálható. [67]

Az FRR definíciójából következik, hogy

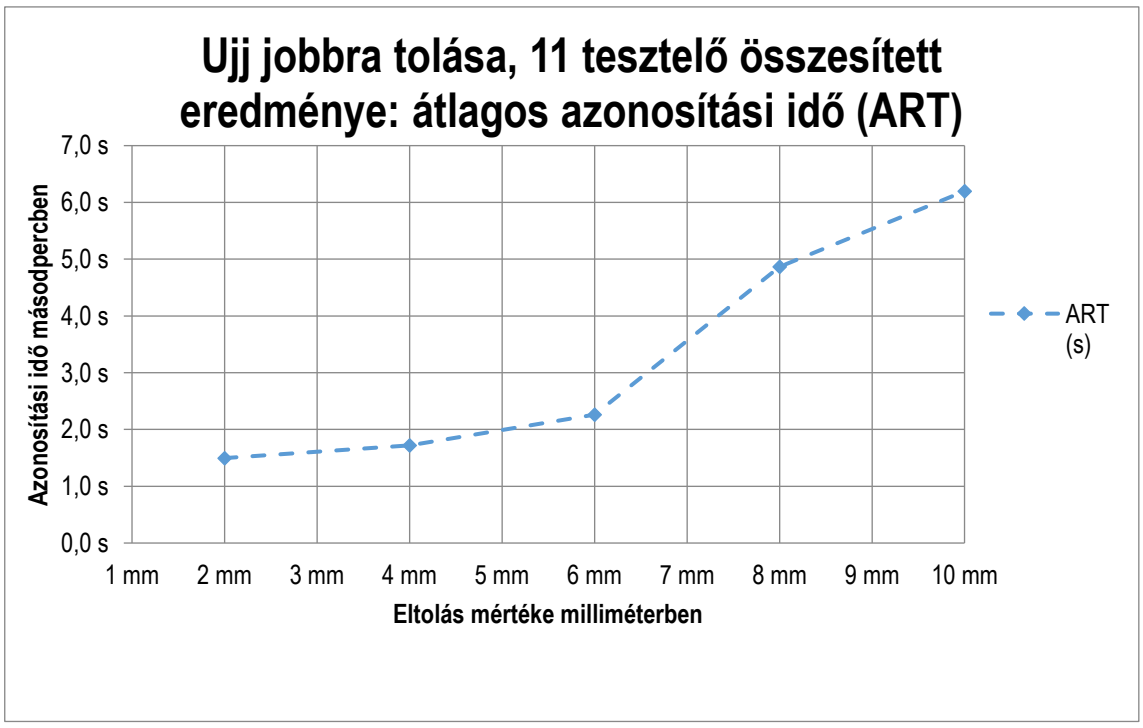
- az algoritmus futási idejének várható értéke a legmagasabb bármilyen sikeres azonosításhoz képest, mivel
    - a téves elutasítás megalapozott meghozatalához a teljes adatbázist végig kell vizsgálni[21] (1:N azonosításnál, azaz amikor nincs előválasztás PIN-kóddal vagy kártyával),
    - 1:1 azonosítás esetén is igaz, hogy az algoritmus a sikertelen esetben próbálkozik a legtovább a felismeréssel, valamint a teljes folyamatot meg kell ismételni,
- továbbá mindkét metódusnál a felhasználónak újra kell a mintát prezentálnia, ami a teljes azonosítási ciklus megismétlését jelenti. [52]

Az ABI-ban számos mérést végeztem e témában, itt egy ujjnyomat-azonosító eszköz 2013. novemberi mérési eredményeit mutatom be ennek alátámasztására. A forgatókönyvi teszt célja az volt, hogy megállapítsa, miként reagál az FRR akkor, amikor az azonosítandó mintát elkezdjük eltolni jobbra a szenzor felületén. Ennek a vizsgálatnak azért van értelme, mert egy eszköz minél inkább mintaeltolás és -forgatás invariáns, annál jobban működik valós körülmények között – kevesebb a hibás elutasítás.

[21] Vagy nem keresi végig az algoritmus az adatbázist, hanem egy beállított idő letelte után automatikusan elutasítja, de ebben az esetben is a maximális ideig tart a felismerés.



6. ábra: Ujjnyomat-azonosító eszköz forgatókönyvi tesztjének eredménye. FRR % a minták jobbra tolásának függvényében; forrás: saját szerkesztés



7. ábra: Ujjnyomat-azonosító eszköz forgatókönyvi tesztjének eredménye. Átlagos azonosítási idő (ART[22]) a minták jobbra tolásának függvényében; forrás: saját szerkesztés

Ez a két tényező azokat az azonosítási folyamatokat, amelyek hibás elutasítással végződnek, a normál, sikeres folyamathoz képest körülbelül két-háromszoros időtartamúra növeli. Ez igaz az 1:1-

[22] Average Recognition Time – Átlagos azonosítási idő.

es azonosításnál is: ha egyszer utasítja el az eszköz, akkor legalább kétszeresére nő a sikeres azonosítás ideje.

Fentiekből következik, hogy a biometrikus eszközök kiszolgálási idejének a legnagyobb a szórása, továbbá az FRR-től közvetlen függ az átlagos kiszolgálási idő, amely kritikus a beléptető és munkaidő-nyilvántartó alkalmazásoknál. [68]

2.1.2 A biometrikus beléptetés folyamatállapotai

A biometrikus rendszerek beléptetési folyamatállapotait a következő ábra mutatja be.

8. ábra: A beléptetési folyamat állapotai; forrás: saját szerkesztés

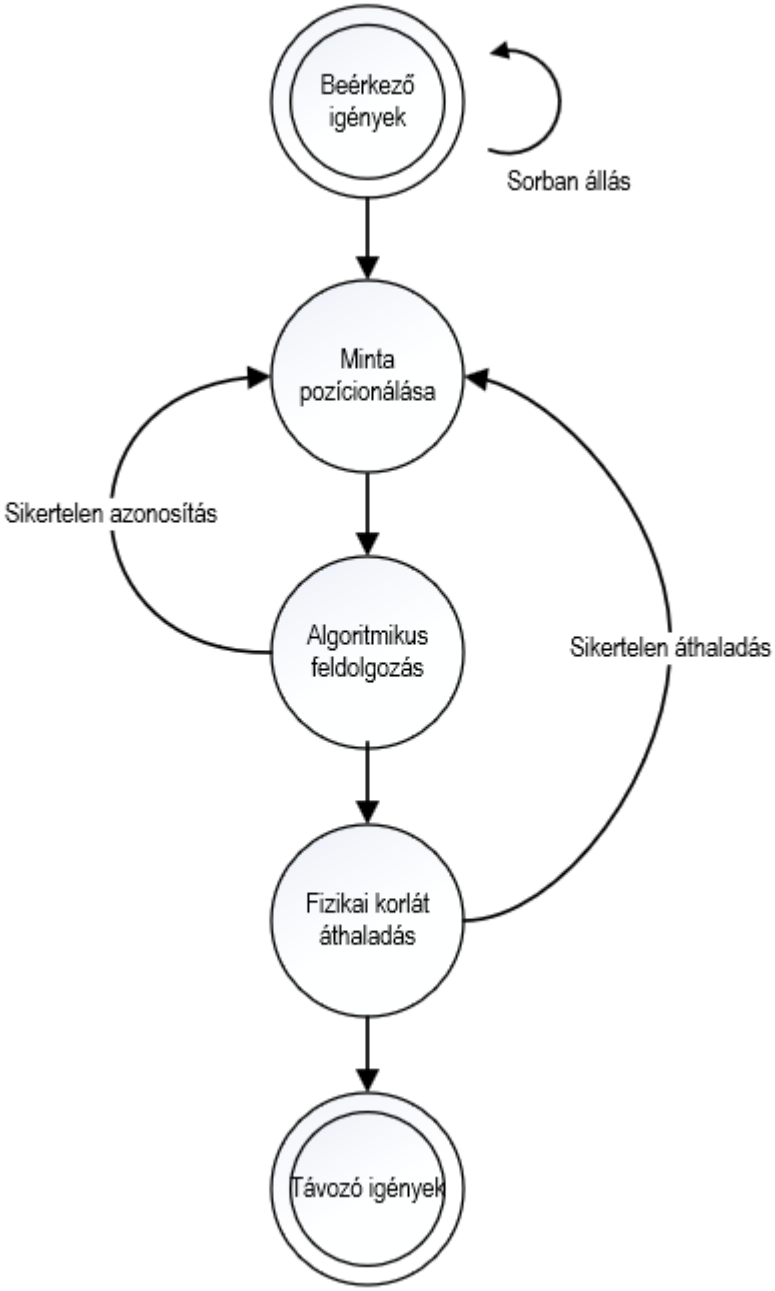
Az egyes állapotok leírása és jellemzői:

- **Beérkező igények:** A dolgozó vagy felhasználó megérkezik az áthaladási ponthoz és sorban áll.
- **Minta pozícionálása:** A felhasználó felkészül az azonosításra és biometrikus mintáját a szenzornak bemutatja, hogy áthaladhasson. Analóg módon értelmezhető a kártyás beléptetésnél a kártya olvasóhoz történő érintése.
- **Algoritmikus feldolgozás:** A prezentált mintát feldolgozza az olvasó és sikeres vagy elutasított jelzést ad. Ezt a lépést csak a biometrikus rendszereknél értelmezzük, és itt tapasztalható meg a biometria valószínűségi jellege, mivel soha nem 100%, hogy egy jogosult személy elsőre át fog tudni haladni az azonosítási ponton. Másik következménye a tulajdonságnak, ami biztonsági kockázatot hordoz magában, hogy az sem biztos 100%-ig, hogy egy jogosulatlan nem jut át. Ez a valószínűségi jelleg kártyás vagy PIN-kódos rendszereknél nem áll fenn.
- **Áthaladás a fizikai korláton:** A sikeres azonosítást követően a vezérlő jelt ad a fizikai korlátozó elemnek, hogy az áthaladást szabaddá tegyék.
- **Távozó igények:** A felhasználó elhagyja az azonosítási pontot.

Egy ideális környezetben a jogosultak mindig át tudnak haladni az azonosítási ponton, a támadókat pedig mindig elutasítja a rendszer, ezért ismerni kell azokat a pontokat, ahol a valóságban ettől eltérően működhet a rendszer.

- A beérkező igények lépésnél sorban állás lehetséges.
- A minta pozícionálása lehet sikertelen, ilyen eset, amikor az áthaladó személy helytelenül teszi oda az ujját az ujjnyomat-azonosító szenzorra, vagy a regisztrációt követően szakállat növeszt és emiatt nem működik az arcfelismerő stb.
- Az algoritmikus feldolgozás rossz eredményt ad vissza és újra kell próbálkozni.
- A fizikai korlát nem működik megfelelően, beragad az ajtó, nem fordul át a korlát vagy a felhasználó használja rosszul az eszközt, így lehet, hogy túl gyorsan lép be a forgóvillához, emiatt az megszorul, és újra kell próbálkozni.

Ezek alapján a belépési folyamat leírható egy, az alább látható irányított gráffal.



9. ábra: Belépési folyamat gráfja; forrás: saját szerkesztés

2.2 Sorbanállási modell

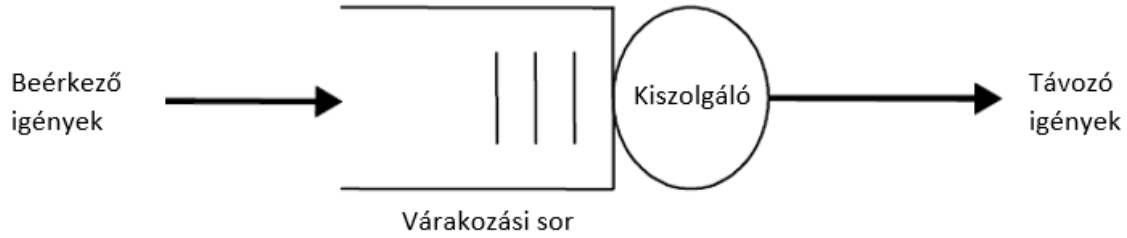
Sorbanállási rendszerek az élet számos területén megjelennek, ahol kiszolgálás történik valamilyen elosztott erőforrás hozzáféréséhez. Bármely rendszer, ahol a vevő kiszolgálása véges erőforrással történik, tekinthető sorbanállási rendszernek. [69] Ilyen rendszerekre példa egy fagyizóban a fagyira várakozás, egy bankban történő sorban állás, a repülőgépek leszállási és karbantartási kiszolgálása, a számítógép processzorának adatfeldolgozása vagy akár a vizsgára várakozó hallgatók is.

Pokorádi szerint: *„Sorbanállási, kiszolgálási rendszeren olyan rendszert értünk, amelybe a fogyasztók véletlenszerűen érkeznek be, az eltérő igényeik kielégítésére várnak, majd a kiszolgálásuk után távoznak.”* [61] A sorbanállási rendszereket Tömegkiszolgálási Rendszernek is szokás nevezni. A sorbanállási problémákat analitikus modellezéssel vagy szimulációs eljárásokkal lehet becsülni, elemezni és értékelni. Az analitikus eljárás egyszerűbb sorbanállási rendszereknél használható, ahol a valóságos folyamat feltételeinek szűkítésével egyszerűen előállíthatók a modell egyenletei. A valóságban sokszor nagyon nehéz leírni egy ilyen rendszert, mert nem vehető figyelembe minden tényező, vagy olyan bonyolult egyenlet keletkezik, amely algoritmikus futásideje nem polinomiális idejű. [70] Ezekben az esetekben hatékony vizsgálati eljárás a szimulációs módszer. A működési elve az, hogy a rendszerműködést szimuláljuk nagy elemszámmal és ezek eredményeiből vonjuk le a következtetéseket. [71]

Ezekben a rendszerekben közös:

- a rendszer felépítése;
- a beérkező igények;
- a várakozási sorok;
- a kiszolgálók;
- a kiszolgálás;
- a távozó igények.

A következő ábra a legegyszerűbb sorbanállási rendszert mutatja be sematikusan.



10. ábra: Legegyszerűbb sorbanállási rendszer, forrás: [71]

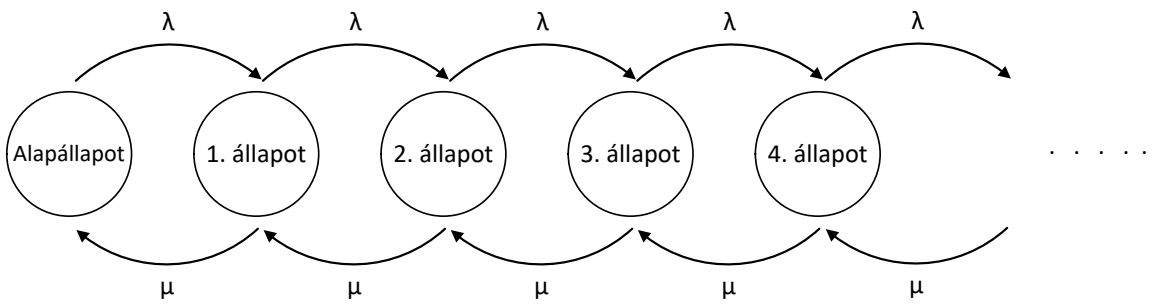
2.2.1 Markov-folyamat

A műszaki tudományok területén sokszor előfordul, hogy az analízishez szükséges alapvető mennyiségek $\{X(t), t \in T\}$ alakulása a véletlenen múlik. Ezek a mennyiségek jellemzően a vizsgált tényező idő és/vagy térbeli változásait írják le. Ekkor az $\{X(t), t \in T\}$ mennyiségeket értelmezhetjük a T paraméterhez tartozó valószínűségi változók együtteseként. Ha T

paraméterhalmaz a pozitív félegyenes $T \subseteq [0, \infty)$ részhalmaza lesz, akkor t tekinthető időparaméternek, röviden időnek. A valós számok halmaza rendezett, ezért értelmezhető a folyamat múltja és jövője. Ha jelen időpillanatnak tekintjük $t \in T$ rögzített értéket akkor értelmezhető az $\{X(s): s > t\}$ folyamat jövője, az $\{X(s): s < t\}$ pedig a múltja. [72]

Markov-folyamatnak nevezzük azokat a sztohasztikus folyamatokat, amelyek jövőbeli állapotait a folyamat múltja csak a jelen állapoton keresztül befolyásolja, más szóval a folyamat emlékezet nélküli. Ha egy forgóvillás beléptető kapunál öten állnak sorban, akkor nem számít, hogy hatan voltak és egy áthaladt, vagy hárman voltak és ketten még érkeztek hozzá. **A beléptetési folyamat tekinthető** folytonos idejű, diszkrét állapotterű Markov-folyamatnak, más néven **Markov-láncnak**.

A következő ábra egy-egy kiszolgálós sor diszkrét állapotterű Markov-lánc reprezentációját mutatja be.



11. ábra: Egycsatornás Markov-lánc; forrás: [71]

Minden állapot a rendszerben várakozók és az aktuálisan kiszolgálásra kerülők darabszámát jelenti. A rendszerben várakozók számának növekedését a λ – érkezési intenzitás, a csökkenésüket pedig a μ – kiszolgálási intenzitás írja le. A rendszer alapállapota az, hogy senki nincs a rendszerben.

2.2.2 Kendall jelölésrendszere

A tömegkiszolgálási rendszerek leírásához szükséges általános jelölésrendszert Kendall dolgozta ki 1953-ban. Eszerint a sorbanállási rendszerek típusai akkor írhatók le, ha ismerjük a beérkezési eloszlást, a sor tulajdonságait és a kiszolgálási mechanizmust. [73] Értekezésem céljait legjobban Sztrik *A sorbanállási elmélet alapjai* című könyvének modellje írja le. [74] A sorbanállási rendszerek jellemzésére használható jelölésrendszer:

$$A / B / m / K / n / E \tag{2}$$

ahol:

- *A*: a beérkező igények idejének eloszlásfüggvénye;
- *B*: a kiszolgálási idők eloszlásfüggvénye;
- *m*: a kiszolgálók száma;
- *K*: a rendszer befogadóképessége, azaz a kiszolgálóegységben és a várakozási sorban tartózkodó igények maximális száma;
- *n*: az igényforrás számossága;
- *E*: a kiszolgálás elve.

Az eloszlásfüggvények (*A* és *B*) lehetnek:

- determinisztikus (*D*);
- exponenciális (*M*) vagy
- általános (*G*) típusúak.

A rendszer befogadóképessége (*K*) és igényforrása (*n*) lehet:

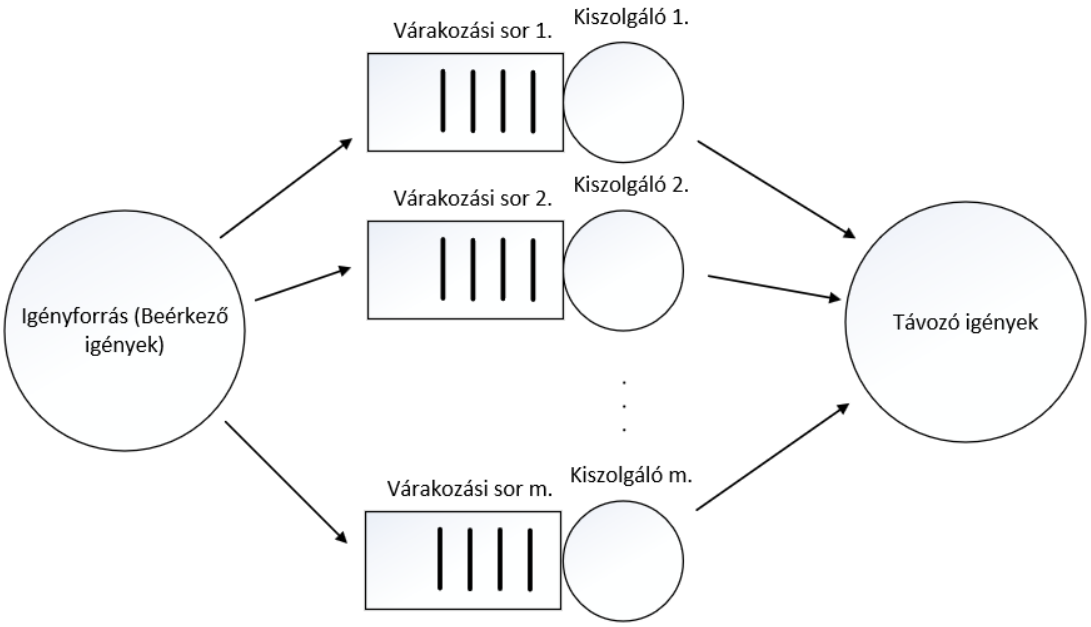
- véges vagy
- végtelen – általában ez utóbbit alkalmazzuk, mivel véges esetben a matematikai modell nagyon bonyolulttá válik és kellően nagy létszám esetén nem releváns.

A kiszolgálás elve (E) lehet:

- FIFO (First In First Out) – az elsőként beérkező kerül először kiszolgálásra;
- LIFO (Last In First Out) – az utolsóként beérkező kerül elsőként kiszolgálásra;
- véletlenszerű vagy
- prioritásos.

2.2.3 A beléptetési folyamat modellje

A beléptető rendszerek általában több kiszolgáló egységből álló párhuzamos kiszolgáló egységes rendszerként írhatók le, grafikusan a következő ábra mutatja be általános formában.



12. ábra: Többkiszolgálós beléptető rendszer modellje; forrás: [74]

A sorbanállási rendszerek matematikai tárgyalásához szükséges, hogy néhány megszorítást tegyek a feltételekben. Ezek érdemben nem befolyásolják a modell valósághűségét, azonban, ha mégis el kell ezektől térni, akkor valamilyen szimulációs eljárás használható a modellezésre. [75] A feltételeket a (2) Kendall jelölésrendszere alapján veszem sorra.

- *A*: a beérkező igények eloszlásfüggvénye Poisson-eloszlású;
- *B*: a kiszolgálási idők eloszlásfüggvénye szintén exponenciális;
- *m*: a kiszolgálók száma véges, természetes szám;
- *K*: a rendszer befogadóképessége végtelen;
- *n*: az igényforrás számossága végtelen;
- *E*: a kiszolgálás elve FIFO.

Ez alapján a beléptető rendszerek modellje:

$$M / M / m / \infty / \infty / FIFO.$$

Ilyen esetekben az utolsó három paramétert nem szokás kiírni, ez alapján egy egycsatornás beléptető rendszer:

$$M / M / 1,$$

egy többcsatornás:

$$M / M / m$$

tömegkiszolgálási rendszerrel modellezhető.

2.2.4 Terminológia és mérőszámok

A modellalkotás célja, hogy képesek legyünk meghatározni a rendszert jellemző mérőszámokat, amelyek leírják a teljesítményét. [74] [76] [77]

- a rendszer állapota = a rendszerben várakozók száma;
- a sor hossza = a várakozók száma, akik a kiszolgálási eljárás megkezdésére várnak;
- $N(t)$ = a *t (t ≥ 0)* időpillanatban várakozók száma;
- $P_n(t)$ = bármely *t (t ≥ 0)* időpillanatban annak a valószínűsége, hogy pontosan n várakozó van jelen a rendszerben;
- *s* = a párhuzamos kiszolgálók száma a rendszerben;
- λ = adott időintervallumon belüli beérkezési intenzitás;
- μ = adott időintervallumon belüli kiszolgálási intenzitás;
- a kihasználtsági tényező:

$$\varrho = \frac{\lambda}{s\mu} \quad . \tag{3}$$

Amikor a rendszer stabil és beállt (a sorbanállási modellek általában – ahogyan én is – ezt az állapotot vizsgálják):

- P_n = annak a valószínűsége, hogy pontosan *n* várakozó van jelen a rendszerben;
- a várakozók száma a rendszerben:

$$L = \sum_{n=0}^{\infty} nP_n \quad ; \tag{4}$$

- a várható sorhosszúság:

$$L_q = \sum_{n=s}^{\infty} (n-s)P_n \quad ; \tag{5}$$

- W = a rendszerben töltött átlagos idő a várakozással és a kiszolgálással együtt;
- W_q = sorbanállási idő.

A következő egyenletek kapcsolatot teremtenek a fenti jelölések között:

- A Little-formula szerint a rendszerben levő igények átlagos száma egyenlő a beérkező igények intenzitásának és a rendszerben töltött átlagos idő szorzatával [78]:

$$L = \lambda \mathrm{W} \quad ; \tag{6}$$

$$L_q = \lambda W_q \quad ; \tag{7}$$

$$W = W_q + \frac{1}{\mu} \quad . \tag{8}$$

2.3 Beléptető eszközök tipikus kiszolgálási ideje

A beléptetés funkciója jellemzően valamilyen fizikai korlát működtetéséhez kapcsolódik, azonban kiemelt biztonságú objektumokban ezeken túlmenően további biztonsági lépések is beiktatásra kerülnek. [79] A következő táblázat összefoglalja a jellemző elemeket és azok gyártók által megadott, illetve valós rendszerekben tapasztalt kiszolgálási idejét. [80] Az alábbi táblázatban szereplő adatok egy kiemelt állami objektum biometrikus beléptetési projektjéhez készült átfogó tanulmány és elemzés alapján kerültek begyűjtésre és validálásra. Az objektumba mintegy 1000 munkavállaló lépett be és ki naponta.

2. táblázat: Belépési folyamat jellemző elemei; forrás: saját szerkesztés

Megnevezés	**Kiszolgálási idő (s)**	**Átlag (s)**	**μ (kiszolgálás /perc)**	**Megjegyzés**
Kártyás azonosítás	1–2	1,5	40	
PIN-kód	1–4	2,5	24	
Biometrikus azonosítás	1–9	5	12	A kiszolgálási idő nagy szórását az FRR okozza.
Ajtó	0–2	1	60	Mágneszár, ajtótartó mágnes.
Forgóvilla, gyorskapu, forgókereszt	2–3	2,5	24	20-30 ember/perc átbocsátási képesség.
Forgókapu, személyzsilip	3–10	6,5	9,23	
Vendégregisztráció	30–180	105	0,57	Személyi igazolvány vizsgálata, adatrögzítés, kártyakiadás, kísérő értesítése.
Csomagröntgen	30–150	90	0,67	
Fémdetektorkapu	10–30	20	3	
Kézi átvizsgálás	20–60	40	1,5	

2.4 A rendszer matematikai modellje

A matematikai modell kidolgozása legfőképp Hillier & Lieberman: *Introduction to operations research* munkáján alapszik, azonban felhasználtam Sztrik: *Sorbanállási elmélet alapjai,* Fischwick: *Queue Modeling and Simulation,* valamint Lukács *Beléptető kapu elhelyezési stratégia fejlesztése és bemutatása néhány kiválasztott metróállomáson keresztül* munkáit is. [74] [76] [77] [81]

A modellhez a beléptető rendszert, mint tömegkiszolgálási (sorbanállási) rendszert vizsgálom. A beérkező igények a felhasználók, a kiszolgálás pedig maga a belépési folyamat. Következésképpen a beléptetési folyamat leírását a sorbanállási modell jellemzői adják. Ezek az alapvető jellemzők:

- a rendszerben lévő felhasználók átlagos száma: *L*;
- a várható sorhosszúság: L_q;
- az átlagos várakozási idő a rendszerben beleértve a várakozási és kiszolgálási időt is: *W*;
- várható várakozási idő: W_q.

Fenti egységek várható értéke a legfontosabb kérdés mind a munkáltató, mind a munkavállaló számára. Mindegyik függ a λ – beérkezési intenzitás, és a μ – kiszolgálási intenzitás adott időintervallumon belüli várható értékétől. A reciprok értékeiknek szemléletes jelentése van:

- $\frac{1}{\lambda}$ = átlagos beérkezési idő, azaz érkezési ráta;
- $\frac{1}{\mu}$ = átlagos kiszolgálási idő, azaz kiszolgálási ráta.

Általában ezek az értékek függenek a rendszerben lévő igények számától, azonban a beléptetési folyamatban az érkezési és kiszolgálási ráták függetlenek a rendszer állapotától, azaz az aktuális felhasználói létszámtól, ezért ezek az értékek konstansok.

Amikor elég nagy a felhasználói létszám, akkor egy csatorna – áthaladási pont – nem elegendő a biztonsági és üzleti igények kielégítésére. Egyszerűbben megközelítve, túl hosszú a várakozási idő, ezért több kiszolgálós rendszert kell létrehozni (ilyen esetben több forgóvillát kell egymás mellé telepíteni).

- *s* = kiszolgáló szerverek száma.

A megfelelő darabszámú csatorna létrehozása alapvető fontosságú és ennek méretezését a következő részben tárgyalom. Továbbá a beérkezési és kiszolgálási intenzitások függetlenek

egymástól, nyilvánvaló, hogy ezek eloszlása exponenciális, így az ***M / M / 1*** és ***M / M / s*** modellek használhatók a beléptető rendszerek elemzésére.

A rendszer állapota mindig leírható a $P_n(t)$ valószínűségi eloszlással, ami annak az eseménynek a valószínűségét jelenti, hogy a t időpillanatban n felhasználó van a rendszerben. Az eloszlás függ a t-től, azonban, ha a kiszolgálási tényező $\varrho = \frac{\lambda}{s\mu}$ kisebb, mint 1, akkor a rendszer stabilan beáll, ekkor az eloszlás független az időtől, és az L, L_q, W és W_q várható értékei kiszámíthatók.

A kapcsolat a várható értékek között, ezzel párhuzamosan a legegyszerűbb matematikai formulák a Little-formulák a (6), (7) és (8) egyenletek.

Ha bármelyik egyenlet ismert, a többi kiszámítható. A matematikai formulák jelentősen egyszerűbbek, ha a felhasználók száma végtelen. A valóságban a beléptetési folyamatoknál a felhasználók száma mindig véges, ezért a véges és végtelen esetet elemezni kell, hogy valóban élhetünk az egyszerűsítésekkel. A Little-formulák miatt elegendő, ha az egyikre bebizonyítom a helyességet, a levezetésre az L_q-t választottam. [82]

Egykiszolgálós rendszerekben, ha populáció végtelen, az L_q kiszámítása az alábbi formulákkal történhet:

$$P_0 = \left[\sum_{n=0}^{\infty}\left(\frac{\lambda}{\mu}\right)^n\right]^{-1} = 1 - \rho \quad ; \tag{9}$$

$$P_n = P_0\rho^n \quad ; \tag{10}$$

$$L_q = \sum_{n=1}^{\infty}(n-1)P_n = \frac{\lambda^2}{\mu(\mu-\lambda)} \quad ; \tag{11}$$

valamint a (3) egyenlet alapján $\varrho = \frac{\lambda}{\mu}$.

Amennyiben a populáció véges, az értéke legyen N, akkor a P_n valószínűségeloszlás nyilvánvalóan más lesz, és az L_q szummázása szintén véges összeg lesz.

$$P_0 = \left[\sum_{n=0}^{N}\left(\frac{\lambda}{\mu}\right)^n\right]^{-1} \quad ; \tag{12}$$

$$P_n = P_0\rho^n \quad ; \tag{13}$$

$$L_q = \sum_{n=1}^{N}(n-1)P_n \quad . \tag{14}$$

Többkiszolgálós rendszerben, ha a felhasználók száma végtelen, L_q az alábbiak szerint számítható ki:

$$P_0 = \left[\sum_{n=0}^{s-1} \frac{(\rho s)^n}{n!} + \frac{(\rho s)^s}{s!(1-\rho)}\right]^{-1} \quad ; \tag{15}$$

$$P_n = \begin{cases} \frac{(\rho s)^n}{n!} P_0, 0 \le n \le s \\ \frac{(\rho s)^n}{s! s^{n-s}} P_0, s < n \end{cases} \quad ; \tag{16}$$

$$L_q = \sum_{n=s}^{\infty} (n-s) P_n = \frac{P_0 \rho (\rho s)^s}{s!(1-\rho)^2} \quad . \tag{17}$$

ahol ebben az esetben $\varrho = \frac{\lambda}{s\mu}$.

Ha a populáció mérete N, feltételezve, hogy *N* > *s,* a különbség az, hogy a (15) kifejezésben a P_0 kiszámítása a következőképpen módosul:

$$P_0 = \frac{(\rho s)^s}{s!} \sum_{n=s}^{N} \rho^{n-s} \quad . \tag{18}$$

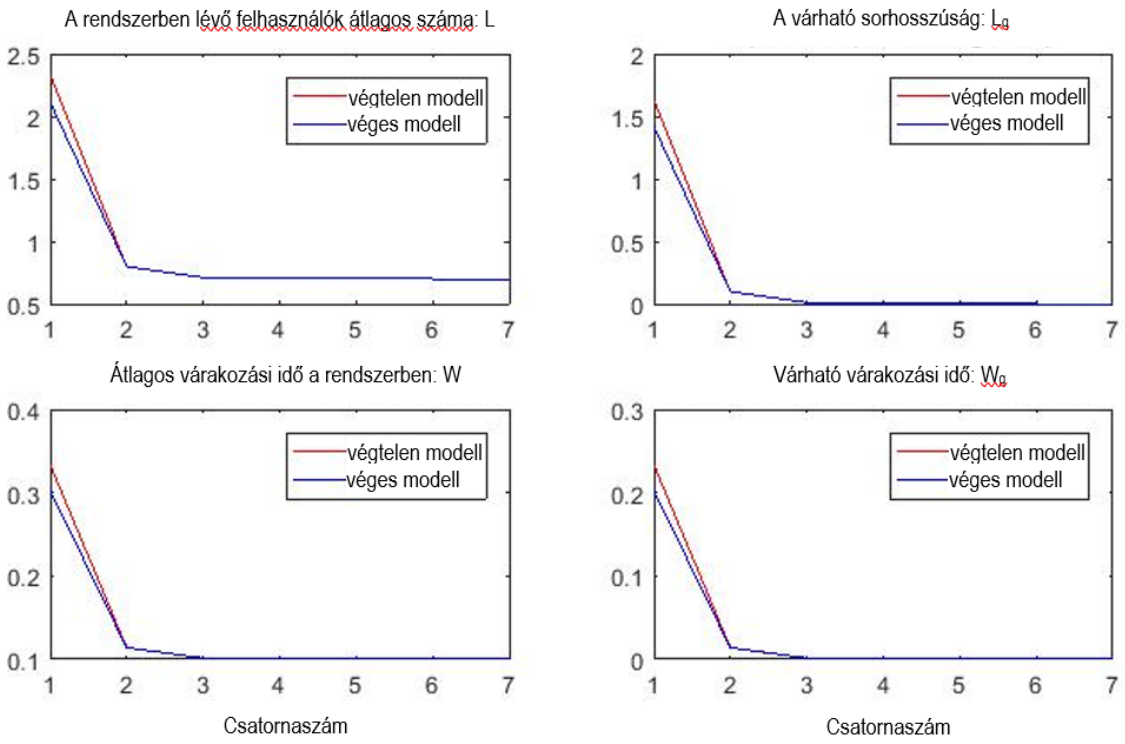
P_N ugyanúgy kalkulálható, mint a (16)-ban, ha *n* ≤ *N*, és a sorhosszúság várható értéke:

$$L_q = \sum_{n=s}^{N} (n-s) P_n \quad . \tag{19}$$

A véges számítások eredménye ebben az esetben is sokkal bonyolultabb.

Hasonlítsuk össze a véges és végtelen modelleket egy hipotetikus eseten keresztül. Tegyük fel, hogy λ = 7 és μ = 10, a beregisztrált felhasználók száma extrém alacsony, *N* = 10.

A következő grafikonok ábrázolják a különbséget a véges és végtelen modellek között.



13. ábra: Véges és végtelen jellemzők értékei; forrás: [82]

Azonnal látható, hogy érzékelhető különbség csak az $s = 1$, egycsatornás modellben van. Ha $s \geq 2$, több csatorna van a rendszerben, akkor a görbék praktikusan egybevágnak.

A következő táblázatokban a grafikonok numerikus értékei láthatók.

3. táblázat: a felhasználók várható értékei véges és végtelen esetben, N =10; forrás: [82]

	L		L_q	
csatornák	végtelen	véges	végtelen	véges
1	2.333333333333334	2.111439832061711	1.633333333333333	1.417491473005482
2	0.797720797720798	0.797585759409489	0.097720797720798	0.097585759409489
3	0.711236954181682	0.711234263822279	0.011236954181682	0.011234263822279
4	0.701276992779638	0.701276774578602	0.001276992779638	0.001276774578602
5	0.700131650913239	0.700131613387380	0.000131650913239	0.000131613387380
6	0.700012132389969	0.700012122200533	0.000012132389969	0.000012122200533
7	0.700001001761946	0.700000998055427	0.000001001761946	0.000000998055428

4. táblázat: a várakozási idők várható értékei véges és végtelen esetben, N = 10; forrás: [82]

	W		W_q	
csatornák	végtelen	véges	végtelen	véges
1	0.333333333333333	0.302498781857926	0.233333333333333	0.202498781857926
2	0.113960113960114	0.113940822772784	0.013960113960114	0.013940822772784
3	0.101605279168812	0.101604894831754	0.001605279168812	0.001604894831754
4	0.100182427539948	0.100182396368372	0.000182427539948	0.000182396368372
5	0.100018807273320	0.100018801912483	0.000018807273320	0.000018801912483
6	0.100001733198567	0.100001731742933	0.000001733198567	0.000001731742933
7	0.100000143108849	0.100000142579347	0.000000143108849	0.000000142579347

Értékelhető különbség csak az s = 1, egycsatornás esetben figyelhető meg.

Amennyiben a regisztrált felhasználók száma eléri a néhány százat, az egycsatornás modell már nem kielégítő. Vegyünk egy esetet, amikor a populáció 500 fő, az átlagos beérkezési intenzitás $\lambda = 50$, az átlagos kiszolgálási intenzitás $\mu = 70$, az elemzendő jellemzők várható értéke a következő két táblázatban látható.

5. táblázat: a felhasználók várható értékei véges és végtelen esetben, N = 500; forrás: [82]

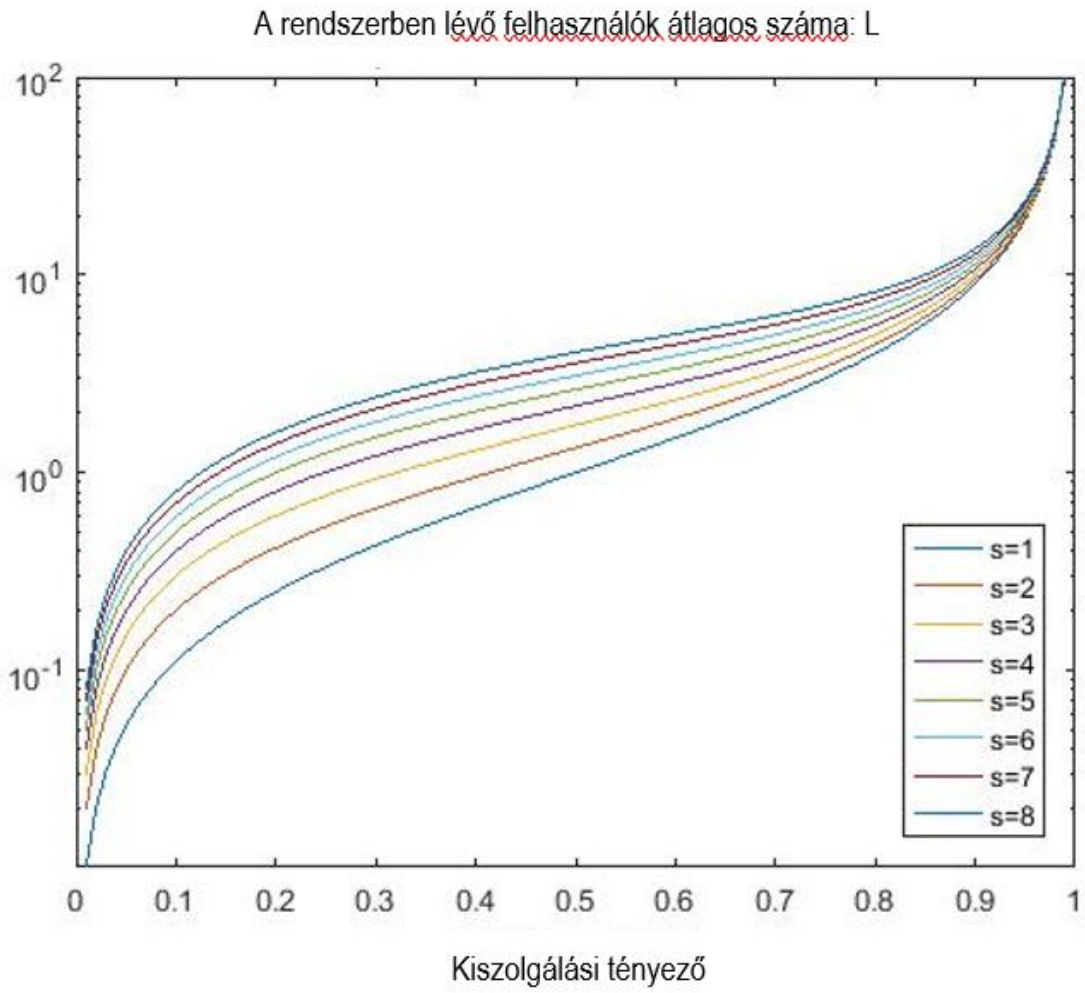
	L		L_q	
csatornák	végtelen	véges	végtelen	véges
1	2.500000000000000	2.500000000000001	1.785714285714286	1.785714285714286
2	0.818713450292398	0.818713450292398	0.104427736006683	0.104427736006683
3	0.726443355119826	0.726443355119826	0.012157640834111	0.012157640834111
4	0.715690500989644	0.715690500989644	0.001404786703930	0.001404786703930
5	0.714433200854997	0.714433200854997	0.000147486569283	0.000147486569283
6	0.714299566011384	0.714299566011384	0.000013851725669	0.000013851725669
7	0.714286880352793	0.714286880352793	0.000001166067078	0.000001166067078

6. táblázat: a várakozási idők várható értékei véges és végtelen esetben, N = 500; forrás: [82]

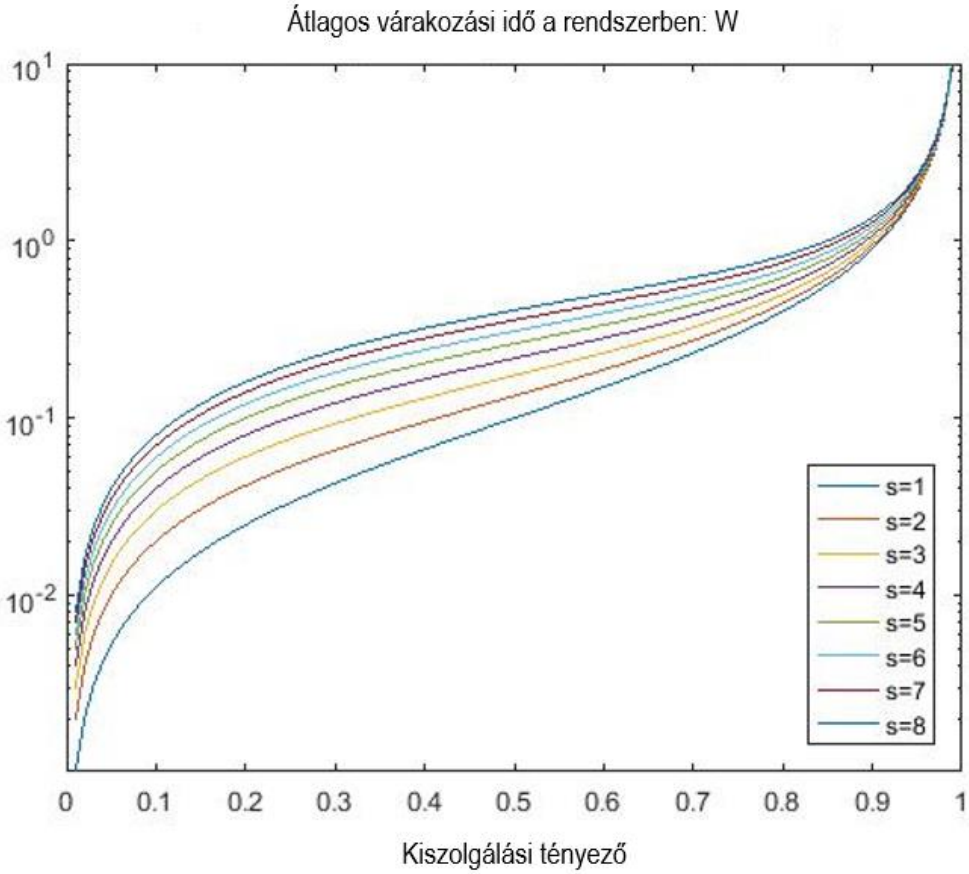
	W		W_q	
csatornák	végtelen	véges	végtelen	véges
1	0.050000000000000	0.050000000000000	0.035714285714286	0.035714285714286
2	0.016374269005848	0.016374269005848	0.002088554720134	0.002088554720134
3	0.014528867102397	0.014528867102397	0.000243152816682	0.000243152816682
4	0.014313810019793	0.014313810019793	0.000028095734079	0.000028095734079
5	0.014288664017100	0.014288664017100	0.000002949731386	0.000002949731386
6	0.014285991320228	0.014285991320228	0.000000277034513	0.000000277034513
7	0.014285737607056	0.014285737607056	0.000000023321342	0.000000023321342

Ezek alapján, amikor a populáció eléri a néhány százat, a véges és végtelen modellek megegyeznek egymással.

Ezért **a végtelen populációjú sorbanállási modell alkalmazható a tömegtartózkodású objektumok beléptető rendszereinek elemzéséhez**. Egy tömegkiszolgálási rendszer jellemző értékei függenek a kiszolgálási tényezőtől is (ρ). Felhasználva az L_q egyenleteket és a Little-formulákat az összefüggés ábrázolható. A következő ábrákon az L és W függése látható a kiszolgálási tényező függvényében különböző csatornaszámok esetén. Az ábrákon az y tengely logaritmikus skálájú, az átlagos beérkezési ráta $\lambda = 10$.



14. ábra: A felhasználók várható értéke; [82]



15. ábra: Az átlagos várakozási idő várható értéke; forrás: [82]

A Little-formuláknak köszönhetően $\lambda W = L$ a kapcsolat W és L között egy konstans, ezért a fenti görbék hasonlóak. Ezek a képletek és kapcsolatok felhasználhatók a beléptető rendszerek tervezésénél. Ha előírás van a várakozási időkre, egyértelműen meghatározható a szükséges csatornák száma.

2.5 Egy példa az alkalmazásra

Egy valós példán keresztül vizsgálom meg az előző fejezetekben részletezett matematikai modelleket. Tegyük fel, hogy egy beléptető rendszerben az átlagos kiszolgálási idő 13 másodperc. A beérkező felhasználók száma reggel 6 és 7 óra között ismeretes. A megfigyelések alapján az alábbi adatok állnak rendelkezésre:

7. táblázat: Alkalmazási példa; forrás: [82]

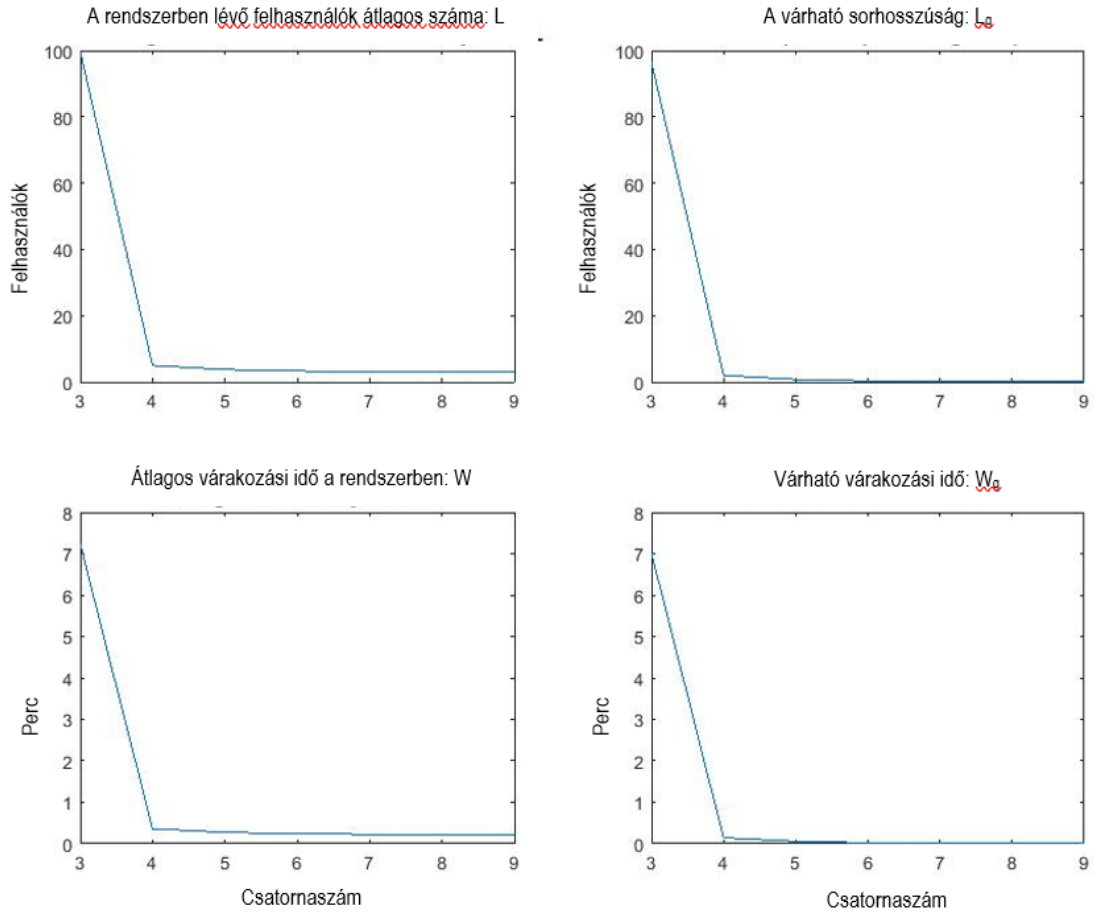
Időintervallum	A beérkező átlagos felhasználószám
6:00 – 6:20	185
6:20 – 6:40	275
6:40 – 7:00	202

Fontos megjegyezni, hogy ebben az esetben az időegység 20 perc, ezért minden számítást erre az intervallumra kell elvégezni. Mivel az átlagos kiszolgálási idő 13 s, az átlagos kiszolgálási intenzitás $\mu = \frac{1200}{13} = 92{,}3$. Mivel a rendszer csak akkor biztosít állandó valószínűségeloszlást, ha a kiszolgálási tényező kisebb mint 1, valamint figyelembe véve a maximális beérkező felhasználószámot, a kiszolgáló csatornaszámnak (3) alapján ki kell elégíteni a következő egyenlőtlenséget:

$$\rho = \frac{\lambda}{s\mu} = \frac{275}{s \cdot 92{,}3} < 1 \rightarrow s \geq 3$$

Ezek alapján legalább háromcsatornásra kell tervezni a rendszert.

Elvárás, hogy az átlagos várakozási idő kevesebb mint 1 perc legyen. Az adatokat felhasználva, a legalább háromcsatornás rendszerben kiszámíthatók a *L, L_q, W és W_q* értékei. A számítások eredményei a következő ábrán láthatók:



16. ábra: A λ = 275, μ = 92,3, T = 20 perc rendszer jellemző értékei; forrás: [82]

Fenti ábrákból az látható, hogy ha minimális csatornaszámot (*s = 3*) állítunk be a rendszerbe, akkor az átlagos várakozási idő körülbelül 7 perc, ami nem elfogadható a munkavállalók számára. Amikor

a csatornaszámot $s = 4$-re változtatjuk, a várakozási idő 1 perc alá csökken. Nyilvánvaló továbbá, hogy $s = 4$ csatornaválasztásnál az idő és várakozási függvények közel konstanssá válnak, ezért ez az optimális választás. A csatornaszám növelése nem fogja javítani a jellemzők értékeit, minden várható érték gyakorlatilag ugyanaz marad, ezért nincs értelme további csatornákat beállítani a rendszerbe.

A következő táblázat tartalmazza a kiszámított jellemző értékeket az egyes esetekre:

8. táblázat: A $\lambda = 275$, $\mu = 92{,}3$, $T = 20$ perc rendszer jellemző értéke különböző csatornaszámokra; forrás: [82]

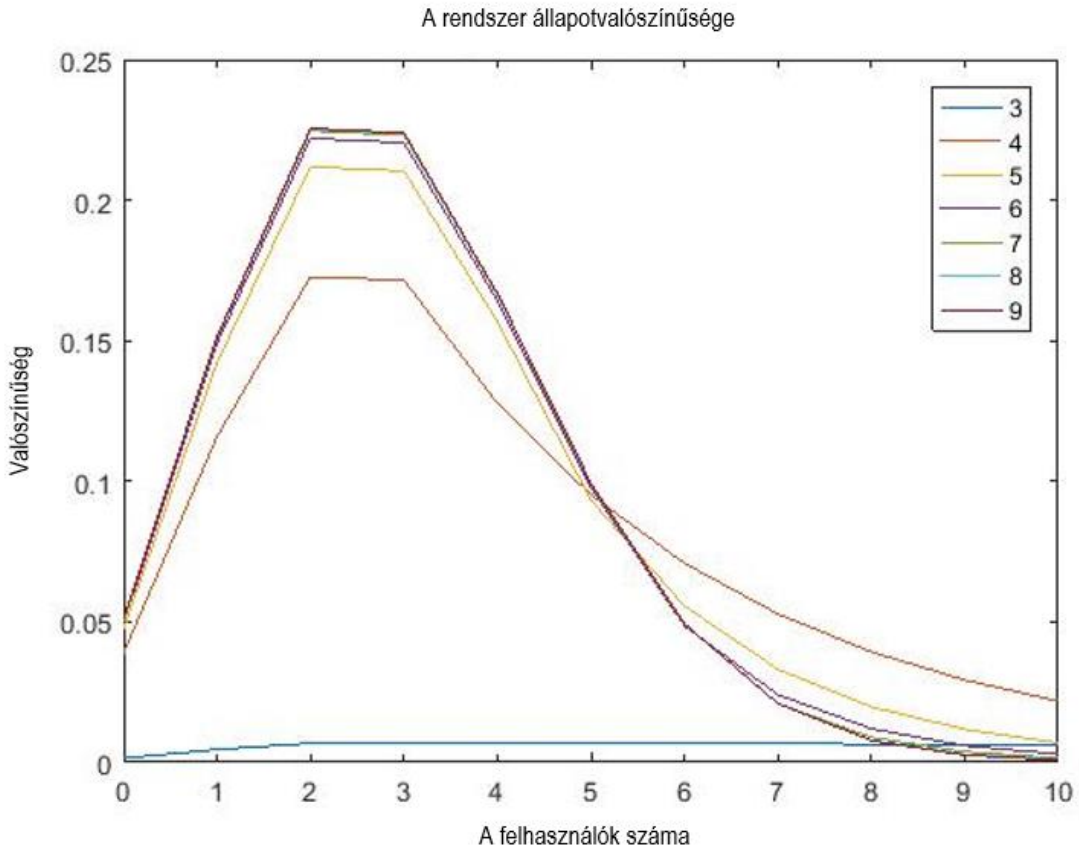
csatornák	L (felhasználók)	L_q (felhasználók)	W (perc)	W_q (perc)
3	99.5432	96.5638	7.2395	7.0228
4	4.9559	1.9765	0.3604	0.1437
5	3.7471	0.7677	0.2725	0.0558
6	3.3011	0.3217	0.2401	0.0234
7	3.1072	0.1278	0.2260	0.0093
8	3.0261	0.0466	0.2201	0.0034
9	2.9950	0.0155	0.2178	0.0011

A valós felhasználói létszám véletlenül alakul, ezért valószínűség eloszlással írható le. Az előzőekben átlagos várható felhasználószámról beszéltem, azonban ezek az értékek „csak" várható értékei egy valószínűség eloszlásnak. Az utolsó feltehető kérdés az, hogy mi a valószínűsége annak az esemény bekövetkezésének, hogy pontosan egy meghatározott számú felhasználó van a rendszerben. A következő táblázat tartalmazza ezeket a valószínűségeket.

9. táblázat: A valószínűsége annak az eseménynek, hogy pontosan n felhasználó van az s csatornás rendszerben; forrás: [82]

	n = 0	n = 1	n = 2	n = 3	n = 4	n = 5	n = 6	n = 7	n = 8	n = 9	n = 10
s = 3	0.0015	0.0046	0.0068	0.0068	0.0067	0.0067	0.0066	0.0066	0.0065	0.0065	0.0065
s = 4	0.0389	0.1160	0.1727	0.1716	0.1278	0.0952	0.0709	0.0528	0.0393	0.0293	0.0218
s = 5	0.0477	0.1422	0.2119	0.2104	0.1567	0.0934	0.0556	0.0332	0.0198	0.0118	0.0070
s = 6	0.0500	0.1490	0.2220	0.2205	0.1642	0.0978	0.0486	0.0241	0.0120	0.0059	0.0030
s = 7	0.0506	0.1508	0.2247	0.2231	0.1662	0.0990	0.0492	0.0209	0.0089	0.0038	0.0016
s = 8	0.0508	0.1513	0.2253	0.2238	0.1667	0.0993	0.0493	0.0210	0.0078	0.0029	0.0011
s = 9	0.0508	0.1514	0.2255	0.2240	0.1668	0.0994	0.0494	0.0210	0.0078	0.0026	0.0009

Az alábbi ábra szemlélteti a valószínűségeket grafikusan.



17. ábra: A rendszer különböző állapotainak valószínűsége; forrás: saját szerkesztés

2.6 A fejezet összefoglalása

A vonatkozó szakirodalom feldolgozásával definiáltam a beléptetési folyamatot, amely alapot szolgáltatott arra, hogy megtaláljam a megfelelő matematikai modellt az elemzésére.

Bemutattam a beléptető rendszerek Markov-lánccal történő sztochasztikus modell felállításának egy jól alkalmazható eljárását, valamint az erre épülő elemzésének egy új módszerét. Az eredmények alapján megállapítható, hogy a kidolgozott elemzési eljárás alkalmas a biometrikus beléptető rendszerek bevezetésének tervezési fázisban történő minőségbiztosítására, az üzleti döntések támogatására. Arra biztatom a biztonsági szakember kollégáimat, hogy egy megbízás során tegyék fel azokat a kérdéseket, amelyekkel biztosítható a projekt sikeressége. Sokszor találkozom olyan felhívással, amikor a pályázat kiírója definiálja, hogy két forgókaput kíván telepíteni. Általában más méretezési megfontolás nem áll ezek mögött, csupán egy tűzvédelmi-menekülési terv vagy a rendelkezésre álló terület mérete. Ezek egyike sem biztosítja azt, hogy normál működésben a tömeg megfelelően gyorsan át tud jutni az áthaladási pontokon.

Célom volt a tömegtartózkodású objektumok üzleti és biztonsági szempontok alapján történő projektbevezetés sikertelenségének elkerüléséhez létrehozott matematikai szimuláción alapuló

folyamat- és rendszerelemzési eljárások kidolgozása, valamint gyakorlati alkalmazási lehetőségeinek bemutatása esettanulmányok felhasználásával.

Az elemzéseket követően világossá vált, hogy rendkívül fontos szempont a felhasználók hozzáállásának megismerése, melyet szükségesnek tartok a továbbiakban részletesen tanulmányozni. Ezért a következő fejezetben primer kutatás segítségével megvizsgálom a felhasználók elfogadási küszöbét, amelyet közvetlenül összefüggésbe hozok a beléptető rendszerek tervezésével amennyiben ez a küszöb létezik.

3 AZ EMBEREK TÉVES ELUTASÍTÁSSAL SZEMBENI ELFOGADÁSI KÜSZÖBÉNEK VIZSGÁLATA

A biztonsági beruházások egyik sarkalatos szempontja, hogy a felhasználók hajlandók és képesek-e megfelelően használni a védelmi rendszert. A biometrikus beléptető rendszerekre ez méginkább jellemző, mivel az algoritmusok valószínűségekkel dolgoznak, így a felhasználók soha nem lehetnek biztosak abban, hogy a rendszer 100%-os pontossággal felismeri őket. Ugyanakkor a biometrikus rendszerek gyártói által megadott értékek nem érhetőek el a valós alkalmazásokban, sőt, a legtöbb esetben több nagyságrendű eltérés van köztük. Ebben a fejezetben elemzem a felhasználók beléptető rendszerek hibáival szemben mutatott egyéni, szubjektív elfogadási küszöbét, mely során a biometrikus rendszerek felhasználói oldalról is értékelhetővé válnak. [83]

3.1 Háttér

Ma már egyre több szakcikk és kutatás foglalkozik a biztonságmenedzsment kérdéskörével, Somroo és szerzőtársai kiemelik, a műszaki és menedzsmenttudományok interdiszciplináris összefüggéseit. [84] Ezt a gyakorlat is megerősíti, hiszen elengedhetetlen, hogy a biztonságtechnikai kérdésekben a döntéshozók felkészültek és járatosak legyenek a műszaki tudományokban is. [85] Kutatásomban ötvöznöm kellett a mérnöki és társadalomtudományokat így szemléltetve, hogy a mérnökök számára sem elhanyagolható az emberi viselkedés társadalomtudományi megközelítése. [86]

A biztonságmenedzsment egyik jelentős területe az IT-biztonság mellett a fizikai biztonság megteremtése. Általános részei: a mechanikai védelem, az elektronikai védelem és az élőerős védelem (1. és 2. ábra). A biztonság megteremtésének egyik alapvető feladata, hogy egy objektumhoz, értékhez, személyhez vagy információhoz történő hozzáférést csak az arra jogosultak vehessék igénybe. A biztonságtechnikai rendszerek jelentős része erre a feladatra fókuszál. Az automatikus személyazonosítás (beléptető rendszerek) területén három alaptechnológia létezik: a tudásalapú (PIN-kód, jelszó), birtokalapú (kártya, telefon) vagy biometrikus azonosítású (valamely testi jellemző).

Egy biometrikus beléptető rendszer kiválasztása és bevezetése a felsővezetői döntés hatásköre, ahol a döntés-előkészítést mérnökök végzik, de a legtöbb esetben nekik sem állnak rendelkezésre az erőforrások, hogy hitelesen leteszteljék a szóba jöhető technológiákat. Jelen fejezetben arra vállalkozok, hogy társadalomtudományi alapfogalmak megismertetésével közelebb kerüljünk ehhez a témakörhöz, ugyanakkor rá fogok világítani arra, hogy a felhasználók sokkal elfogadóbbak

a hibákat tekintve, és ez az elfogadási küszöb nagyságrendekkel eltér a rendszerek műszaki hibamutatóitól. [87]

Az automatizált, elektronikus biometrikus személyazonosítás hatalmas fejlődésen ment keresztül az elmúlt ötven évben. A rendészeti szerveknek egyre nagyobb az igénye arra, hogy személyeket hitelesen és gyorsan, gyakorlatilag bárhol képesek legyenek azonosítani. Ezzel párhuzamosan az élet minden területén egyre inkább szükséges a felhasználók, belépők azonosítása, a hozzáférés hitelesítése. Másrészről megfigyelhető, hogy a felhasználói elfogadottság az egyes technológiák vagy berendezések irányába döntő szerepet játszik ezek sikerességében, mindennapos használhatóságában. [23] [88] Természtesen azt sem lehet figyelmen kívül hagyni, hogy az adatvédelemmel foglalkozó szervek és hatóságok minden ilyen fejlesztésnél véleményezik a jog- és célszerűséget, illetve az arányosságot. [89]

Az első fejezetben azonosítottam azokat az elsősorban civil biometrikus alkalmazásokat, ahol a biometrikus azonosítás kritikus működésű. Ezek a tömegtartózkodású objektumok, elsősorban a nagy munkavállalói létszámú vállalatoknál és tömegtartózkodású objektumoknál használt beléptető és munkaidő-nyilvántartó rendszerek. A rendszer kritikus tulajdonságát az adja, hogy a nagy létszám miatt gyorsnak és alacsony hibás elutasítási (FRR – False Rejection Rate) értékűnek kell lennie.

Szakértői mélyinterjúk és empírikus módszerrel megszerzett információk alapján Magyarországon az elmúlt 20 évben megvizsgált mintegy 100 biometrikus rendszer bevezetésének jelentős része sikertelen volt.[23] Ezt a jelenséget elemezve jutottunk el az ABI-ban (Alkalmazott Biometria Intézet) 2010-ben a biometrikus eszközök teszteléséhez. A tesztekkel bármely gyártó bármely eszközét vizsgálva arra jutottunk, hogy a megadott FRR-adatok több nagyságrenddel eltérnek a valós értékektől. Ennek elsődleges oka, hogy a gyártók algoritmikus vagy más néven technológiai tesztek eredményeit adják meg és nem számolnak a felhasználókkal, a telepítési és környezeti körülményekkel.

Ekkor merült fel bennem, egyáltalán hogyan létezhetnek sikeres biometrikus projektek. Másképpen megközelítve, el lehet-e dönteni egy biometrikus eszközről egy tender során, hogy az jól fog-e működni vagy sem?

[23] Az 1. fejezet bekezdéseiben ismertettem néhány tipikus példát.

Ezért a mindennapi felhasználók irányából kezdtem el vizsgálódni, mivel kíváncsi voltam a nézőpontukra. A feltevésem az volt, hogy az emberek legalább 2-3 nagyságrenddel nagyobb hibás elutasítási arányt is még használhatónak tartanak.

A kutatás kihívása volt a mindenki számára érthető, releváns és egységes fogalmak felkutatása, melyek statisztikailag is érvényes eredményeket hozhatnak. A probléma kiküszöbölésére kvalitatív, azon belül is fókuszcsoportos vizsgálatot használtam. A fókuszcsoport résztvevőinek meglátásait elemezve hozzájutottam azokhoz a kifejezésekhez, melyek leginkább leírják a beléptető rendszerekről alkotott véleményeiket. A kapott fogalmakat pedig felhasználhattam a későbbi kvantitatív kutatásomhoz is.[24]

3.2 A témához kapcsolódó kutatások

A beléptető rendszerek és ezen belül is, a biometrikus eljárás, relatív új terület a biztonság megteremtésében. A nemzetközi szakirodalomban felhasználói elfogadottsággal (User Acceptance) kapcsolatos kutatásokat végeznek a különböző biometrikus adatokon alapuló azonosítási technológiák emberi tényezőkön alapuló vizsgálatához. A legtöbb ilyen kutatás Andrew Dillon és Michael G. Morris 1996-ban megjelent *User acceptance of new information technology: theories and models* című tanulmányára hivatkozik, mely összefoglalja az információs technológiák felhasználói elfogadásának modelljeit, valamint pszichológiai hátterét. [23] Eszerint a felhasználói elfogadottság definíciója, az az igazolt hajlandóság a felhasználói csoportban, hogy arra alkalmazzák az információs technológiát, amire azt tervezték. A biometrikus rendszerek felhasználói elfogadottsági kutatásait Marek Rejman-Greene értekezése foglalja össze az *Encyclopedia of Biometrics* című könyvben. [26, p. 1554–1561]

Magyarországon az első vonatkozó tudományos igényű kutatást 2006-ban végezték el a Budapesti Műszaki Főiskola Bánki Donát Gépész- és Biztonságtechnikai Mérnöki Karán, egy Panasonic gyártmányú BM-ET 330 típusú íriszfelismerő beléptető rendszerről, *„a beléptető rendszer keltette attitűdök és averzív reakciók vizsgálatát”* elvégezve. [24] Ezt követően 2014-ben Földesi Kriszta és Kovács Tibor lefolytattak egy hiánypótló, nagyszabású kérdőíves kutatást (*n = 333* fő) a magyar rendőrök és az Óbudai Egyetem diákjai megkérdezésével. [25] [88]

Ezek a kutatások a biometrikus eszközökre, a biometrikus technológiára, azok minőségére és elfogadottságára fókuszálnak. Kutatásom során nem találtam olyan tanulmányokat, amelyek a

[24] Legalábbis ez volt a tervem, mivel később kiderült, hogy nincs közös fogalmi tér.

beléptető rendszer áthaladási pontját egészében értékelnék, pedig ez az a környezet, amellyel a felhasználó találkozik.

3.3 A kvalitatív kutatás módszertana

A kutatás kihívása volt a mindenki számára érthető, releváns és egységes fogalmak felkutatása, melyek statisztikailag is érvényes eredményeket hoznak. A probléma kiküszöbölésére kvalitatív, azon belül is fókuszcsoportos vizsgálatot használtam. A fókuszcsoport résztvevőinek véleményét és meglátásait elemezve hozzájutottam azokhoz a kifejezésekhez, melyek leginkább leírják a beléptető rendszerekről alkotott véleményeiket. A fókuszcsoport egyértelmű célja a felhasználók tapasztalatainak és hozzáállásának megismerése volt. A kvalitatív technika teret enged, hogy a felhasználók gondolatait, logikáit, érzelmeit is feltérképezzük. Az introspekció során betekintés nyerhető a beléptető rendszerek használata során vélt hozzáállásukra. Így leképezhető, milyen gondolatok merülhetnek fel bennük, ha a rendszer hibáival szembesülnek, mik a tapasztalataik a rendszerről, összességében a korábban megfogalmazott felhasználói hozzáállást vizsgálom. A fókuszcsoport vezérfonalába kidolgozott kérdések főképp a rendszerről kialakított tapasztalataikra, azok hibás működéséről alkotott véleményükre, vagy a rendszer irányába megjelenő attítűdjükről kérdezett. Amikor a válaszadók nem értették pontosan a kérdést, nem fűztem hozzá további magyarázatot, tettem ezt azért, hogy a spontán válaszokat kapjam meg, ezért sok kérdésnél kevesebb választ kaptam, mint az összes résztvevő.

Mindemellett ez a technika kevésbé alkalmas a kvantitatív operacionalizálásra. Az elemzés tartalomelemző technikával, gondolati térképpel vagy leíró statisztikai elemzéssel végezhető el. Azonban a kutatás segíti a probléma mélyebb megértését, és a kapott eredmények kiváló alapot nyújtanak a későbbi kvantitatív kutatáshoz. [90]

3.4 A kvalitatív kutatás eredményei

A kutatás az Óbudai Egyetem Keleti Károly Gazdasági Kar MSc-s levelezős diákjainak tantermi keretek közötti megkérdezésével történt. Fontos szempont volt, hogy a résztvevők ne rendelkezzenek szakirányú előképzettséggel. Olyan felhasználókat szerettem volna elérni, akik nem rendelkeznek műszaki vagy mérnöki ismeretekkel a rendszerekről, így a prekoncepcióik saját tapasztalatikból fakadtak. A kérdéseket korábbi kutatásaim, szakirodalmi kutatás, szakemberekkel történő konzultációk és brainstorming alapján állítottam össze. A fókuszcsoport vezérfonalába kidolgozott kérdések főképp a rendszerről kialakított tapasztalataikra, azok hibás működéséről alkotott véleményükre, vagy a rendszer irányába megjelenő attitűdjükről kérdezett. Más kutatásokból vett kérdéseket a szükséges korrektúrákon felül igyekeztem változatlanul hagyni.

Minden kérdés nyitottan került megadásra és a moderátorok semmilyen módon nem befolyásolták a válaszadókat a kérdések értelmezésével.

A résztvevők száma és demográfiai adatai a következő táblázatban találhatóak:

10. táblázat: Válaszadók statisztikája (N = 13); forrás: saját szerkesztés

Jellemzők	Értékek
Résztvevők	13
Nemek eloszlása	Nő: 6, Férfi: 7
Életkori csoportosítás	Minimum: 25, Maximum: 49, Átlag: 37

A fókuszcsoportos kutatás az egyetemen tartott statisztika óra keretében valósult meg 2017. szeptemberében, a csoport tagjai heterogén összetételű 25 és 49 év közötti nők és férfiak voltak. A kutatás adatfelvétele személyes beszélgetés volt, mely később a moderátorok jegyzetei alapján kerültek kielemzésre. A beszélgetés során két moderátor volt jelen. A válaszokat széljegyzetek módszerével vizsgáltam a résztvevők rögzített válaszai alapján. Szemantikai tartalomelemzéssel, azon belül is megnevezéses analízissel értékeltem a szöveget. [90]

A kérdések a következők voltak:

1. *„Találkozott-e már beléptető rendszerrel?”*

Erre a kérdésre a válaszadók 100%-a igennel válaszolt, ami nem meglepő, hiszen egyrészt napjainkban már elterjedt rendszerről van szó, másrészről a résztvevők életkora alapján feltételezhető volt, hogy a döntő többségük dolgozott már fő- vagy mellékállásban, ahol gyakran találkozhattak beléptető rendszerrel.

2. *„Mi az első benyomása a beléptető rendszerekről?”*

Ennél a kérdésnél arra voltam kíváncsi, hogyan viszonyulnak a résztvevők a beléptető rendszerekhez. A válaszkategóriákat induktív következtetéssel alkottam meg.

11. táblázat: Mi az első benyomása a beléptető rendszerekről? (N = 11); forrás: saját szerkesztés

Ssz.	Válasz	Hasznosság	Általános hozzáállás
1.	Működőképes.	Pozitív.	pozitív

2.	Lassúnak találom, gyakori a meghibásodás lehetősége, ami fennakadást okoz.	Lassú.	negatív
3.	Hátráltat, lelassít, akadályoz.	Lassú.	negatív
5.	Pozitív, ki lehet szűrni azokat az embereket akiknek nincs jogosultságuk belépni.	Biztonságos.	pozitív
6.	Sok a hiba benne, ha telített a „háló”, nem enged belépni.	Lassú.	negatív
8.	Jó dolognak tartom biztonsági szempontból.	Biztonságos.	pozitív
9.	Lassú az áthaladás, zavarok esetén késések. Forgóvilla beragadás esetén balesetveszély.	Lassú.	negatív
10.	Nem mindig indokoltak, olykor problémásak.	Negatív.	negatív
11.	Hasznos, nincs rossz tapasztalatom.	Pozitív.	pozitív
12.	Mint vezető jónak tartom, mert munkaügyi vita esetén használható. Mint minőségbiztositó tűzvédelemmel foglalkozó jó, mert pontosan tudjuk ki, hol tartózkodik. Mint labdarúgás-szurkoló, utálom.	Biztonságos.	pozitív
13.	Talán egy szükséges rossz. A munkahelyemen utálom.	Negatív.	negatív

A kategóriák elhelyezhetők három dimenzió mentén. Az általános hozzáállás lehet negatív/pozitív, ezt követi a rendszer hasznossága, melyről a legtöbb esetben a résztvevők úgy vélekedtek, hogy biztonságos, végül a használat sebességét is kiemelték még a válaszadók, amelyről úgy gondolták, hogy lassú. Az elemzés során feltűnt, hogy vagy a felhasználó (belépő), vagy az üzemeltető szemszögéből ítélik-e meg a kérdést.

A következő ábrán szemléltetem a válaszadók által leggyakrabban használt kifejezéseket. A fogalmakat szófelhőprogram segítségével hoztam létre. Összesen 11 válaszadó válaszolt, ez 85%-os arány. A pozitív és negatív kategóriákat általános válaszok kódolására használtam.

18. ábra: Az első benyomások szófelhője; forrás: saját szerkesztés

A válaszok több mint **fele negatívan nyilatkozott** a beléptető rendszerekről, egyharmaduk egyértelműen megjelölte az okát, miszerint **lassú a beléptetés.**

3. *„Hol találkozott beléptető rendszerrel?"*

A résztvevők közül öten válaszoltak, közülük négyen a munkahelyüket jelölték meg válaszként, vagyis a beléptető rendszerekkel többnyire a biztonsági beléptetés és munkavállalóként munkaidő-nyilvántartással találkozhattak. Egy válaszadó több helyszínt adott meg válaszként, vélhetően ebbe beletartozik a munkahelye is, azonban az elemzésbe ezt a feltételezést nem építettem be.

12. táblázat: Hol találkozott beléptető rendszerrel? (N=5); forrás: saját szerkesztés

Ssz.	Válasz	Helyszín 1.	Helyszín 2.
1.	Több rendszer.	Több	
4.	Munkahelyemen gyakorlatilag minden ez alapján működik. Ha nem jól működik az nagy galibát okozhat.	Munkahely	
7.	Vendégként érkeztem egy nagyvállalathoz megbeszélésre így külön regisztrálni kellett a portán és kaptunk egy kártyát.	Munkahely	
12.	Munkahely.	Munkahely	Stadion
13.	Munkahely.	Munkahely	Stadion

4. *„Milyen rendszereket ismer?”*

A legtöbben forgóvillás beléptető rendszerekkel találkoztak, nagyon fontos eredmény, hogy a felhasználók egyben látják a fizikai korlátot az azonosítási eljárással.

13. táblázat: Milyen rendszereket ismer? (N=13); forrás: saját szerkesztés

Ssz.	Válasz
1.	Forgóvillás Detektorkapu Automata ajtó PIN-kódos Kártyás
2.	Beléptető rendszer Átvilágítási funkcióval rendelkező kapu Forgókapu
3.	Forgókeresztes Fémdetektoros
4.	Forgókapus Ajtót nyitja az irodámban
5.	Forgóvillás Fémdetektoros
6.	Forgóvillás
7.	Kártya, amit a portán kaptunk nyitotta az ajtót (érintést követően)
8.	Nem tudja a típust

9.	Honeywell Forgóvillás Teljes emberméretű rudas Fotocellás ajtó Fémdetektoros kapu
10.	Polipkarú Fémdetektoros kapu Kapu nélküli proxy kulcsos Forgóvillás
11.	Kártyás Forgóvillás
12.	Forgóvillás Forgókapus Ajtó
13.	Forgóvillás Detektoros kapu

19. ábra: Az ismert rendszerek szófelhője; forrás: saját szerkesztés

5. *„Milyen problémák lehetnek a beléptető rendszerrel?”*

A hibák is, az előző kérdésre adott válaszokhoz hasonlóan magához a fizikai eszköz problémáihoz köthetőek, mint például a „beragad” vagy „fennakad”, a beléptető rendszer hibája vagy maga a jogosultság kérdése – „fáziskésés” vagy „nem enged be” – csak két esetben merült fel. Ez az eredmény azért fontos, mivel alátámasztja azt, hogy a felhasználók az egész rendszert és folyamatot értékelik, nem pedig az egyes részlépéseket.

14. táblázat: Milyen problémák lehetnek a beléptető rendszerrel? (N=5); forrás: saját szerkesztés

Ssz.	Válasz
3.	Beragad. Megakad.
4.	Megakad. Fáziskésés. Blokkol.
6.	Nem enged be.
9.	Beragad. Stokked.
11.	Fennakadás. Torlasz.

6. *„Hogy érezné magát ilyenkor?"*

A sikertelen beléptetés esetén az emberek zavarba jönnek, és segítséget várnak a probléma megoldásához jellemzően valamilyen emberi kezelőtől.

15. táblázat: Hogy érezné magát ilyenkor? (N=7); forrás: saját szerkesztés

Ssz.	Válasz	Kategória	Megjegyzés
1.	Türelmetlen.		A türelmetlen válasz káromkodás volt.
5.	Türelmetlen.		A türelmetlen válasz káromkodás volt.
7.	Zavarba jövök és kérdően nézek a kezelőre. Most miért nem nyílik?		
8.	Kiszűrt ez a nyomorult kapu. Becsipogtam.		
10.	Időrabló.		
12.	Mi történt? Miért nem működik?		
13.	Ócska.		

A kvalitatív kutatással az volt a célom, hogy megismerjem, milyen szavakat, mondatokat és kifejezéseket használjak a kvantitatív felmérésben amit a legtöbben alkalmaznak. Ezzel szemben teljesen egyértelművé vált, hogy **nincs egységes fogalmi kör** még egy viszonylag homogén célcsoportban sem. Ez a probléma nemcsak a biometriát érintette, hanem a beléptető rendszert is. Határozott célom volt, hogy a lehető legegyszerűbb kérdéseket tegyem fel, és még véletlenül se

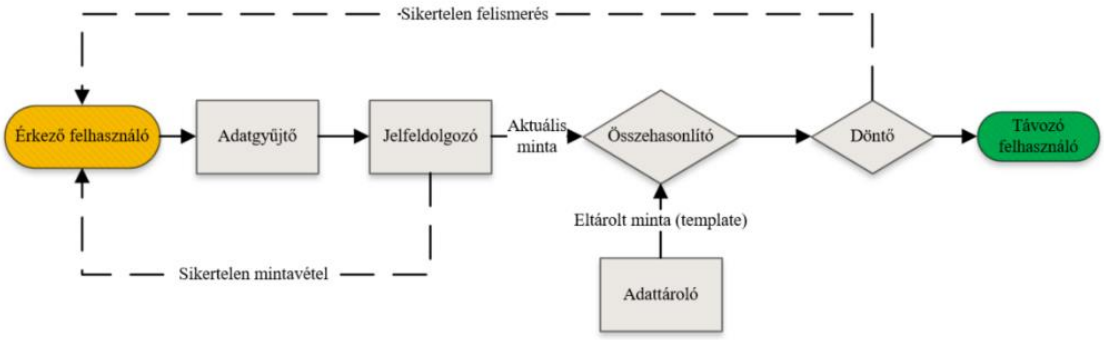
befolyásoljam a válaszadókat, ezért azt az irányt elvetettem, hogy a kérdőív elején vagy a kérdéseknél részletesen magyarázzak el egy szakmai fogalmat vagy a szituációt, mivel még ekkor sem lehettem volna abban biztos, hogy megértették vagy ugyanúgy értelmezték a kérdést a válaszadók. A másik lehetőség az volt, hogy olyan kérdést fogalmazzak meg, amely egyértelmű a válaszadóknak, mindenki ismeri és egyértelműen párhuzamba állítható azzal a mutatóval, melyet a biometrikus rendszereknél vizsgálok (FRR). A második lehetőséget választottam, és a szituáció, amit feltételezésem szerint mindenki ismer, egy ajtó meghibásodásáról szólt, ezért a kérdőívben feltett alapkérdés a következő: *„Képzelje el, hogy heti 5 napon keresztül, napi négyszer kell átmennie egy ajtón a munkahelyén/iskolájában. Ez az ajtó általában jól működik, ám naponta egyszer megakad, és csak egy újabb próbálkozással tudja kinyitni. Mennyire tartja használhatónak ezt az ajtót?”*

A következő pontban levezetem, hogy pontosan melyik az a hibatípus, amit az értekezésemben célszerű vizsgálni.

3.5 A biometrikus rendszerek jellemzése, hibamutatók

A biometrikus rendszerek jellemzésére és a hibamutatók elemzésére azért itt van szükség, mert ezzel fogok kapcsolatot teremteni a biometrikus rendszerek és a meghibásodott ajtókra kapott válaszok között.

A vonatkozó ISO-szabvány (ISO 19795-1:2006) és Shimon Modi *Biometrics in Identity Management: Concepts to Applications* cikke alapján a biometrikus berendezések alapvetően mintafelismerő rendszerek, általánosságban a következő ábrán látható alrendszerekből állnak össze, melyeket alább részletesen jellemzek: [19] [91]



20. ábra: Általános biometrikus eszköz alrendszerei; forrás: [19]

- **Adatgyűjtő alrendszer:** Felelős a felhasználó biometrikus mintájának levételéért. Ez jellemzően valamilyen szenzor, amely fizikai kontaktust igényelhet a felhasználótól. Ez az

egyetlen interfész a biometrikus rendszer és a felhasználó között, így az összes mintavételezéssel kapcsolatos hiba egyedüli forrása is. A rendszerbe ezen a ponton bekerült hibák végig futnak a teljes azonosítási folyamaton.

- **Jelfeldolgozó alrendszer:** Feladata a mintákból kinyerni azokat a tulajdonságokat, amelyek egyedivé teszik azt. Ez az alrendszer vizsgálja meg a levett minta minőségét, különíti el a tárolandó tulajdonságokat, majd előállítja azt a sablont, amelyet később tárolásra vagy összehasonlításra használ a biometrikus azonosító rendszer. A minőségellenőrző rendszer rendkívül fontos része a jelfeldolgozásnak, ugyanis ez határozza meg, hogy az adott mintát újra kell-e vételezni. A kialakult sablon az esetek jelentős többségében nem visszaállítható, tehát nem lehet a mentett sablon alapján újraalkotni az eredeti mintát.
- **Adattároló:** Tárolja a levett és kódolt biometrikus adatokat a későbbi összehasonlításhoz. Ezeket az adatokat a biometria területén sablonnak is nevezik. A tárolás lehet központi (egy számítógépen vagy szerveren), illetve lokalizált (pl. smart cardon vagy egyéni adathordozó eszközön). 2018. május 25. után az EU 2016/679-es rendeletével gyakorlatilag betiltja a felhasználók biometrikus adatának gazdasági célokból történő központi tárolását. [92]
- **Összehasonlító alrendszer:** Összehasonlít két mintát és létrehoz egy hasonlósági pontszámot. Ez a pontszám annak a bizonyosságát mutatja meg, hogy a tárolt sablon és a levett minta egy és ugyanazon személytől származik. A biometrikus azonosító rendszerek mindig valószínűség-alapúak, így sosem jöhet létre 100%-os egyezés. Ezzel szemben például egy kriptografikus vagy jelszóalapú rendszernél mindig 100%-os egyezés szükséges a sikeres azonosításhoz. Mivel az ember és a szenzor találkozása sosem lehet kétszer pontosan ugyanolyan, ezért a rendszer egy egyszerű „igen” vagy „nem” válasz helyett egy hasonlósági pontszámot generál.
- **Döntéshozó alrendszer:** Összeveti a generált hasonlósági pontszámot egy előre meghatározott határértékkel, hogy eldöntse az azonosítás sikerességét vagy sikertelenségét. Ez a határérték azt mutatja meg, hogy két biometrikus minta közt mekkora különbség esetén lehet még azt mondani, hogy egy és ugyanazon személytől származnak. Ez az érték rendkívül fontos a biometrikus rendszer működésében, ugyanis helytelen beállítása a rendszer működési hatékonyságát erősen (és negatívan) befolyásolja.

A biometrikus rendszerek az alábbi funkciókat végzik el:

- **Regisztráció:** A regisztrációs folyamatban egy felhasználó biometrikus mintája kerül rögzítésre. Folyamata: mintavétel; szegmentáció és jellemzők azonosítása; minőségellenőrzés; template létrehozása; ellenőrzés.
- **Ellenőrzés vagy igazolás (verification):** Ellenőrzés esetén a rendszer a felhasználó tranzakcióját pozitív egyezés megtalálásának érdekében vizsgálja, más szavakkal megnézi, hogy a személy XY-ként regisztrálva van-e a rendszerben. Ez a folyamat vagy elfogadja, vagy elutasítja a felhasználót. A döntési folyamat hibás, ha egy hamis tranzakciót igazinak vél (téves elfogadás) vagy egy valós tranzakciót hamisnak vél (téves elutasítás). Figyelembe kell venni, hogy egyes biometrikus rendszerek egy végfelhasználónak több, különböző minta felvételét is engedélyezik (pl. egy íriszazonosító rendszer esetében mindkét írisz, vagy egy ujjnyomat-azonosító rendszer esetén kettő vagy több ujj). Az ellenőrzés folyamata: mintavétel; szegmentáció és jellemzők azonosítása; minőségellenőrzés (amely a mintát/jellemzőt eldobhatja, ha az használhatatlan, és további minták begyűjtése válik szükségessé); a tárolt sablon összehasonlítása a begyűjtött mintával, hogy meghatározza a hasonlósági pontszámot; eldönti, hogy a pontszám alapján egyezőnek minősíthető-e a két minta, vagy átlépi azt a határt, ahonnan már a két minta nem egyezik. [93]
- **Azonosítás vagy felismerés (identification):** Azonosítás esetén a rendszer a tranzakció során megkeresi azokat a személyeket, akik a prezentált mintához leginkább hasonló sablonokkal rendelkeznek. Az azonosítás sikeres, ha az azonosítandó személy rendelkezik sablonnal a rendszerben, valamint csakis a helyes sablon került kiválasztásra. Az azonosítás sikertelen, ha van a jogosultnak sablonja az adatbázisban, de nem kerül kiválasztásra (téves negatív hiba), vagy egy, a rendszerben nem szereplő személy kiválasztásra kerül (téves pozitív hiba). Az azonosítás tipikusan ezekből a lépésekből áll: mintavétel; szegmentáció és jellemzők azonosítása; minőségellenőrzés (amely a mintát/jellemzőt eldobhatja, ha az használhatatlan, és további minták begyűjtése válik szükségessé); az adatbázisban található néhány, vagy összes sablonnal való összehasonlítás, ahol minden összehasonlítás egy-egy hasonlósági pontszámot eredményez; a hasonlósági pontszám értékének alapján (átlép egy határt, vagy a legmagasabb pontszámok között van) annak eldöntése, hogy az adott sablon azonosságra jelölt lehet-e; a jelöltlista felépítése; azonosítás a jelöltlista alapján egy vagy több vizsgálat alapján, amit a döntési policy ír elő.

3.5.1 A hibák

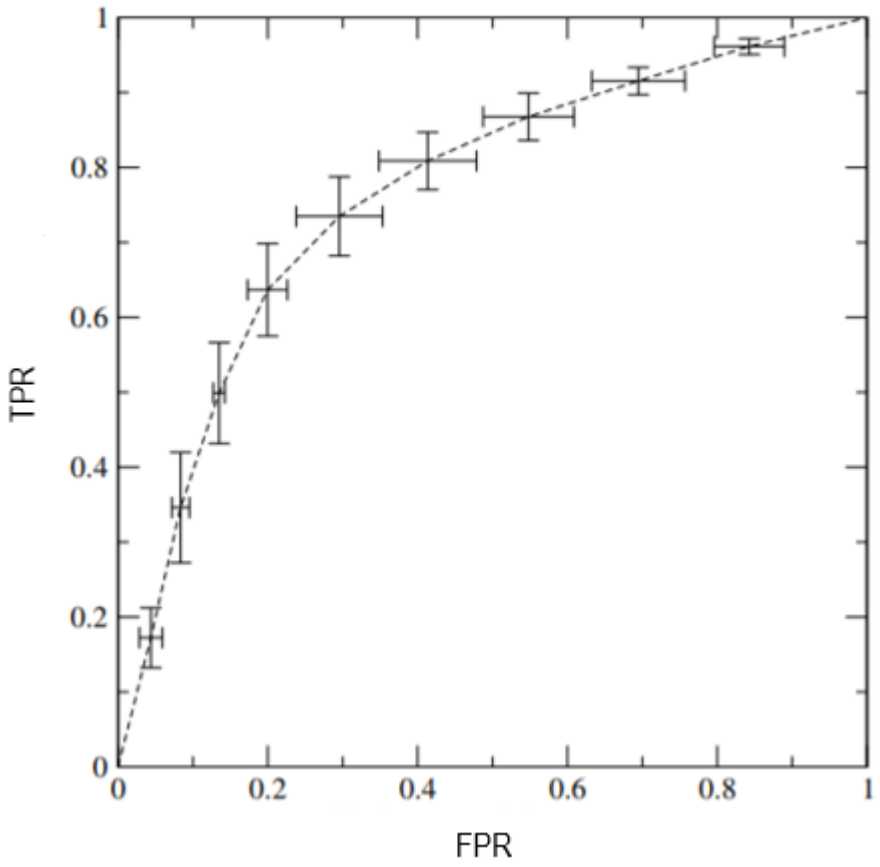
Az ellenőrzési és azonosítási hibák vagy megfeleltetési (téves egyezési, illetve téves nem egyezési hibák), vagy mintavételi hibákra (sikertelen mintavétel, sikertelen rendszerbe való felvétel) vezethetők vissza. Az, hogy ezek az alapvető hibák miként vezetnek döntési hibához, több tényezőn múlik, mint például az előírt összehasonlítások számán, a döntési policyn, vagy éppen azon, hogy pozitív vagy negatív-e az azonosítás. [15]

Egy biometrikus azonosító rendszer két hibatípust képes generálni.

- Két különböző személy biometrikus mintájának téves mérését és egyezőként azonosítani (Téves megfeleltetés – false match, szakirodalmi mutatószáma False Match Rate – FMR vagy False Acceptance Rate – FAR).
- Ugyanattól a személytől két mérést különböző személyként azonosítani (Téves meg nem feleltetés – false nonmatch, szakirodalmi mutatószáma False Non Match Rate – FNMR vagy False Rejection Rate – FRR). [94]

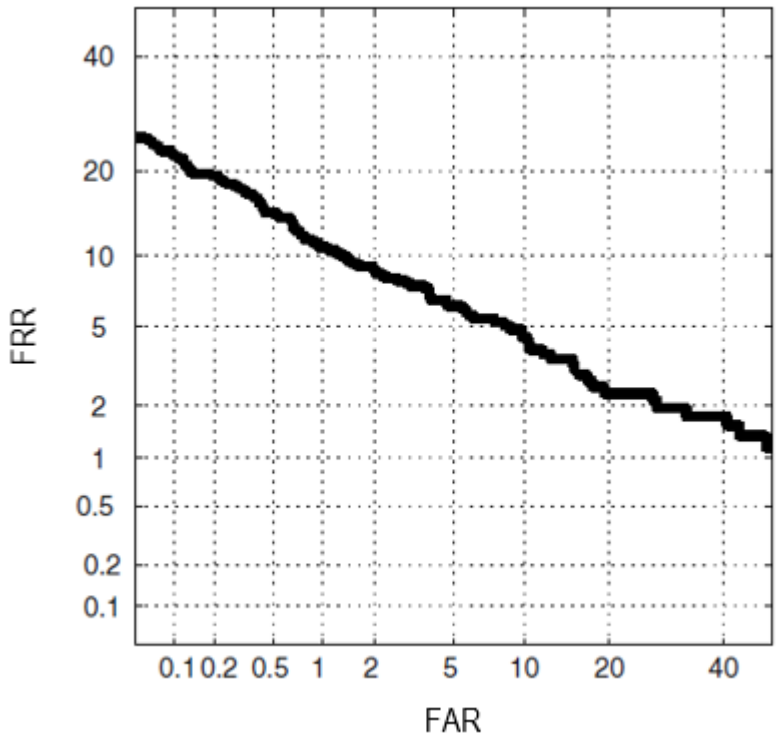
Minden rendszerben létezik egy tradeoff görbe a hibás egyezési ráta (FMR – False Match Rate) és a hibás nem-egyezési ráta (FNMR – False Non Match Rate) között. Ha úgy konfigurálják a rendszert, hogy kevésbé legyen érzékeny a zavaró tényezőkre, és jobban fogadja el a felhasználók mintáit, akkor az FMR nő meg, ha biztonságosabb beállításokat hoznak létre, akkor pedig az FNMR. A biometrikus rendszerek teljesítményének ábrázolására általánosan ROC (Receiver Operating Characteristic) és DET (Detection Error Tradeoff) görbéket használnak. ROC-görbéket először a II. világháborúban használtak a radarjelzések kielemzésére. Más területeken az ’50-es évektől kezdték alkalmazni: orvostudományban, osztályozási algoritmusoknál. Napjainkban biometrikus rendszereknél, adatbányászatban és mesterségesintelligencia-algoritmusok osztályozására is használják. [95]

Az ROC a mérések és modellek megkülönböztető képességének grafikus megjelenítése. Két dimenzióját a következő ábra mutatja meg, ahol az FPR (false positive rate) a téves riasztási arány és a TPR (true positive rate) a találati arány.



21. ábra: Átlagolt ROC-görbe; forrás: [96]

A következő ábra egy tipikus DET-görbét ábrázol, amelyen a hibás elutasítási arány (FRR) került ábrázolásra a hibás elfogadási arány függvényében (FAR).



22. ábra: DET-görbe; forrás: [15]

3.5.2 Mutatószámok

A szakirodalomban nincs (vagy különbözőképpen hivatkozzák) egységesen használt és elfogadott definíciója a biometrikus rendszereket jellemző mutatószámoknak, ezért ebben a fejezetben ismertetem az általánosan használt elnevezéseket. Az alábbiakban összefoglalom a biometrikus beléptető rendszerek műszaki paramétereit jellemző ismérveket.

1. **Sikertelen regisztrációs arány – Failure To Enroll rate (FTE)**
   Ez a mutató azt jelzi, hogy egy rendszerbe milyen valószínűséggel nem lehet beregisztrálni a felhasználókat. Általában a felhasználó biometrikus mintája alkalmatlan a feladatra, de ide tartoznak azok az esetek is, amikor valamilyen más ok miatt sikertelen a regisztráció, mondjuk rosszul tette rá a szenzorra a mintát. Az arány a regisztrálandó populációra és az adott berendezésre ad előjelzést.
2. **Sikertelen mintabeviteli arány – Failure To Acquire rate (FTA)**
   A sikertelen mintabevitel azt jelenti, hogy az eszköz valamilyen okból képtelen levenni a mintát, és abból előállítani azt a kódot, amit összehasonlítana az adatbázisával. Az ebből képzett arány pedig az összes sikeres mintabevitelre vetíti a sikertelen eseteket.
3. **Téves meg nem feleltetés – False None-Match Rate (FNMR)**

Az FNMR jelenti azt a várható értéket, hogy két minta ugyanattól a személytől hibásan különbözőnek lett felismerve az algoritmus által.

4. **Téves megfeleltetés – False Match Rate (FMR)**

   Az FMR jelenti azt a várható értéket, hogy két különböző minta hibásan egyezőnek lett felismerve az algoritmus által.

5. **Téves elutasítási arány – False Reject Rate (FRR)**

   Az FRR-t számos szakirodalom [97] alkalmazza az FNMR szinonimájaként, azonban én, a céloknak jobban megfelelő és a szabványban is így definált verziót alkalmazom:

$$FRR = FTA + FNMR * (1 - FTA) \tag{20}$$

6. **Téves elfogadási arány – False Accept Rate (FAR)**

   A téves elfogadási arány megmutatja annak a valószínűségét, hogy egy – szándékosságot mellőző – jogosulatlan személy mintáját tévesen elfogadja a rendszer.

   Kiszámítására alkalmazható képlet:

$$FAR = FMR * (1 - FTA) \tag{21}$$

7. **Általánosított téves elfogadási és elutasítási arány – Generalized False Reject Rate (GFRR), Generalized False Accept Rate (GFAR)**

   A különböző biometrikus rendszerek eltérő Sikertelen Regisztárciós Aránnyal (FTE) rendelkeznek, ezek az esetek azonban kiesnek az előző mutatószámokból, mivel jellemzően a továbbiakban nem vizsgálják azokat. Ezért került bevezetésre az általánosított téves elfogadási és elutasítási arány, amely mutatók egyesítik a regisztrációs, a mintavételi és az algoritmikus hibákat is.

   A GFRR és GFAR kiszámítására alkalmazható képletek:

$$GFRR = FTE + (1 - FTE) * FTA + (1 - FTE) * (1 - FTA) * FMR \tag{22}$$

$$GFAR = (1 - FTE) * (1 - FTA) * FMR \tag{23}$$

3.5.3 A hibás elutasítási arány jelentősége a gyakorlatban

Az FRR – hibás elutasítási arány látszólag másodlagos mutatószám a biometrikus azonosítás területén. Ez azért történhet meg, mert a FAR – téves elfogadási arány, sokkal inkább „félelmetes” a biztonság tervezésénél. A védett területre be tud menni olyan személy, aki arra nem jogosult (impostor). Ez számos alkalmazásban igaz is, azonban a fizikai biztonság területén,

tömegtartózkodású objektumokban, Magyarországon az elmúlt 20 évben nem találkoztunk olyan alkalmazással, ahol ez a tényező dominált volna. Matematikai kockázatelemzési módszerek használathatók, amennyiben a felhasználók beléptetésének ideje és sikeressége is szempont. [98]

Az FRR becslése, mérése és megadása a gyakorlatban kivétel nélkül technológiai eredményekre szorítkozik – ami nem meglepő, mert ez az egyetlen olyan teszttípus, amelyik jól kontrollálható, nagy tömegű mintán futtatható és egyértelmű sorrendet képes felállítani az algoritmusok között. [91] A gyártók ezeket az FRR-értékeket tüntetik fel az eszközeik adatlapján, általában 0,00001–0,01% tartományban.

Az általam elvégzett forgatókönyvi, valamint éles körülmények közötti tesztek eredményeit megvizsgálva azt találtam, hogy a valóságban a felhasználók az 1–70% tartományban találkoznak a hibás elutasításokkal. Ez azt jelenti, hogy legalább 2, de akár 6 (!) nagyságrendi különbség is lehet az adatlapi ígéret és a valós eredmények között. Mivel az adatlapi értékek a gyakorlatban mérhetetlenek, ez két dolgot eredményez egy biztonsági beruházás döntésénél:

- Minden gyártó eszköze megfelel a kiírásnak.
- Eldönthetetlen, hogy melyik rendszer lesz a megfelelő az adott feladatra.

Ezek miatt a döntési pontok eltolódnak, és más szempontok kerülnek előtérbe, mint az ár. [99]

3.5.4 Forgatókönyvi FRR-mérések

A vonatkozó biometrikus rendszerek teszteléséről szóló ISO-szabványok és saját módszertani fejlesztések alapján a forgatókönyvi teszteknél olyan körülményeket alakítottam ki, amelyekkel a felhasználók a valós életben is találkozni fognak. Ilyen egy arcfelismerő berendezés fényviszonyfüggése, amely tesztelésével pontosan megmondható, hogy egy kültérre telepített eszköz a napfény megvilágításának változásával a különböző napszakokban hogyan fog viselkedni.

Ahogy az várható volt, a körülmények ideálistól való eltérésekor az FRR-értékek gyorsan romlanak. Az egyes eszközök között az tesz különbséget és dönti el a használhatóságot, hogy milyen mértékben és milyen gyorsan romlanak el az eredmények.

A valós körülményeket minél jobban megközelítő eljárásokat dolgoztam ki úgy, hogy a mérések feltételei, körülményei pontosan dokumentáltak legyenek a megismételhetőség miatt:

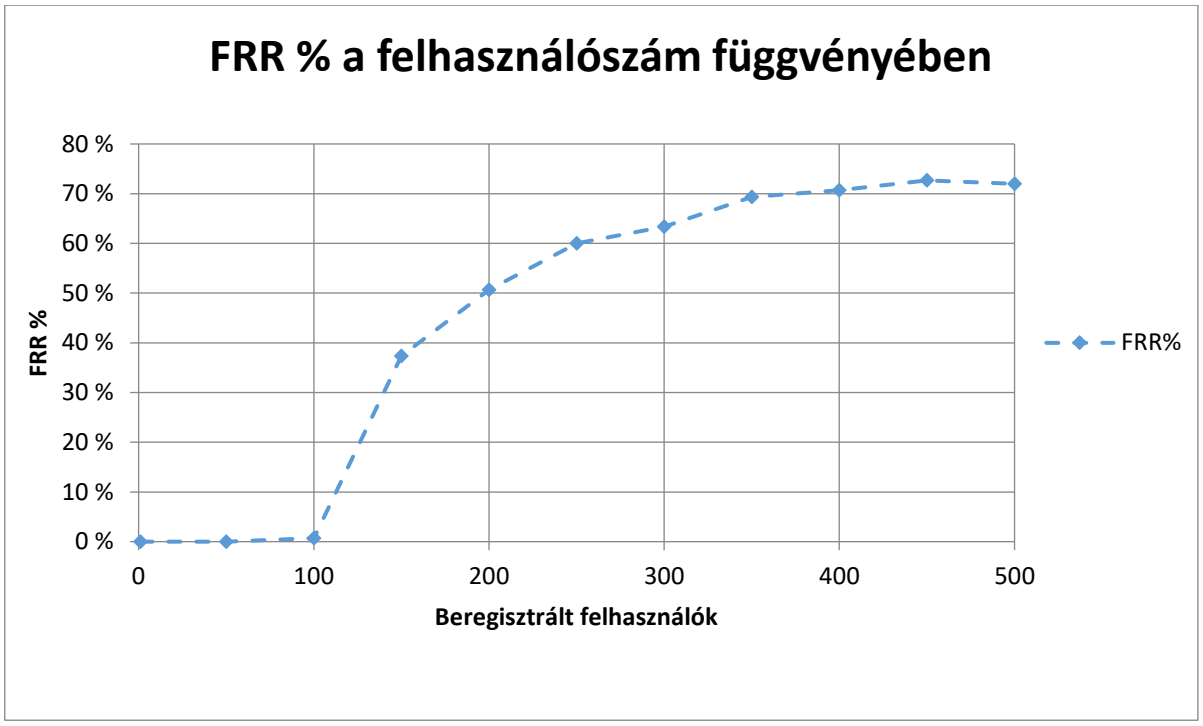
- **pozícionálási érzékenység:** a tökéletesen pozícionált minta elforgatásra és eltolásra kerül, és mérjük az FRR változását (6. és 7. ábra);

- **áteresztőképesség** mérése a regisztrált felhasználók és minták függvényében;
- **FRR** mérése a regisztrált felhasználók és minták függvényében;
- **minta szennyezése:** egy izzadt vagy nedves ujj;
- **minta torzítása:** egy felsértett ujj vagy gyűrű;
- **környezeti változások hatásai:** megvilágítás, hőmérséklet, páratartalom. [100]

Az FRR-mérések statisztikai hátterének elemzésére kiváló összefoglalást ad Hanka [101] publikációja. Ebben bebizonyítja és kiterjeszti a biometrikus ujjnyomat-azonosító rendszerekre Doddington 30-as szabályát, mely szerint: *„90%-os konfidenciaszint esetén, legalább 30 hibát kell észlelnünk, hogy a keresett p valószínűség a tapasztalat alapján számított relatív gyakoriság ± 30%-os környezetébe essen."* Jelen esetben a *p* valószínűség az FRR értéke és az elv értelmében adott FRR-szint elfogadásához 30 hibát kell mérni. Ez azt jelenti, hogy egy átlagos biometrikus eszköz FRR = 0,01% méréséhez **300.000** eseményt, azaz mérést kellene elvégeznünk. Ezt gyakorlatilag lehetetlen kivitelezni.

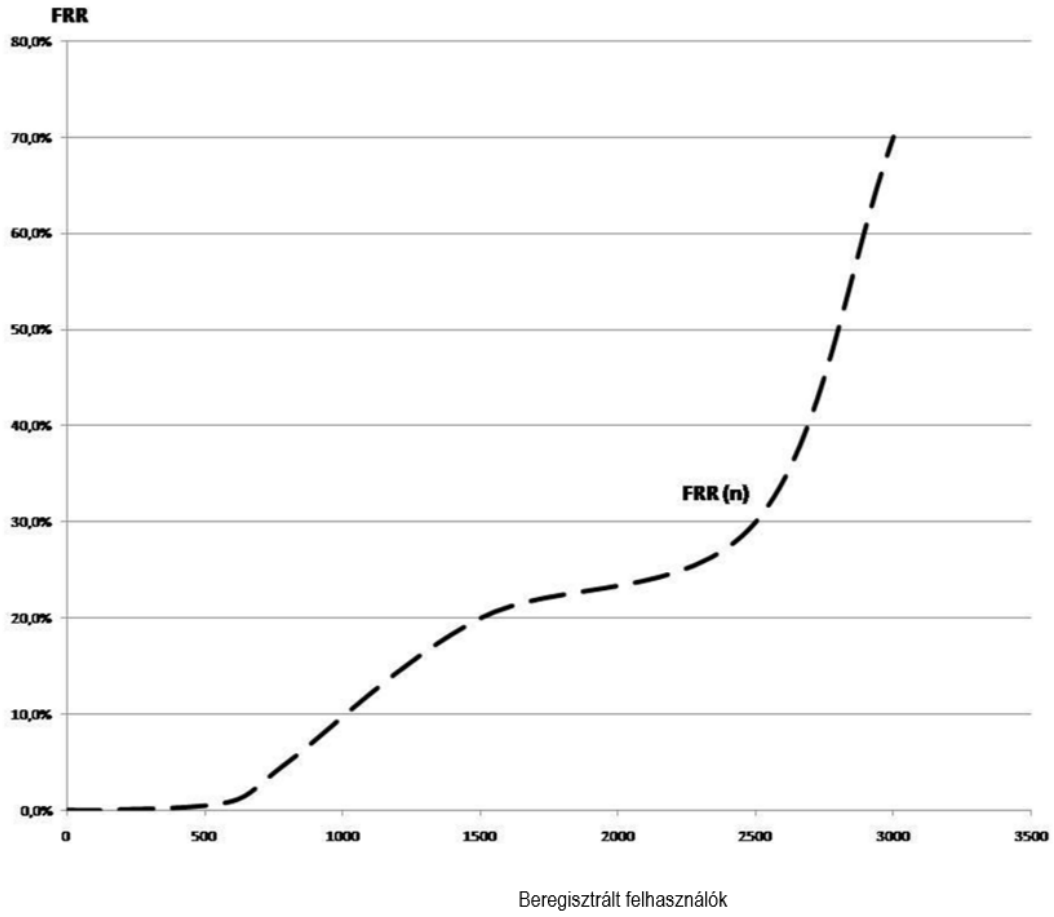
A valóságban ehhez képest mégis értelmezhető eredményeket kaptam, erre a legjobb példa egy ujjnyomat-azonosító berendezés FRR-függése a regisztrált minták számától.

A mérési metodika szerint a névleges felhasználói kapacitást (500 fő) 50 fős lépésközökkel töltöttem fel, és minden mérési pontban 300 mérést végeztem el. Az eredmények a következő ábrán láthatóak.



23. ábra: Arcfelismerő eszköz forgatókönyvi tesztjének eredménye. FRR% a regisztrált létszám függvényében; forrás: saját szerkesztés

Ezt az eredményt támasztotta alá az Óbudai Egyetem Bánki Donát Gépész- és Biztonságtechnikai Mérnöki Karán telepített Suprema ujjnyomatalapú biometrikus személyazonosító rendszere, amelynek éles körülmények között mért FRR-függése a létszámtól a következő ábrán látható:



24. ábra: Suprema Bioentry Plus ujjnyomat-azonosító eszköz FRR-függése a regisztrált létszám függvényében; forrás: [102]

3.6 A kvantitatív kutatás

A kvalitatív kutatás folytatásaként kvantitatív vizsgálatot végeztem. A kvalitatív kutatás során olyan fogalmakat igyekeztem felkutatni, melyeket a felhasználók egységesen használnak és értelmeznek. Az elemzés alapján arra jutottam, hogy a vizsgált csoportban nincs egységes megfogalmazás a beléptető rendszerre vonatkozóan, mely saját tapasztalataimat is alátámasztja.

Olyan általános modellt és megfogalmazást igyekeztem létrehozni, amely mindenki számára világos, érthető és egységes. A kutatásból elsősorban a biometria és a beléptető rendszerek fogalmát vettem ki, hiszen ez nem mindenki számára egyértelmű. Célom volt a lehető legegyszerűbb megfogalmazást adni kutatási kérdésként, amit mindenki ugyanúgy ért, és jó eséllyel már találkozott a jelenséggel, ezért releváns választ tud adni, mégis megfeleltethető legyen az FRR fogalmával. Hosszas egyeztetések után, azt a modellt választottam, amikor egy olyan ajtón kell áthaladni a felhasználónak, amely néha hibásan működik, ezért megszorul, és nem sikerül átmenni rajta. Ezzel a jelenséggel jó eséllyel már mindenki találkozott. Mivel az ajtó szempontjából a megszorulás eseménye valószínűségi változóval leírható, ezért megfeleltethető a biometrikus rendszereknél használatos valamelyik hibamutatónak.

A 3.5.2 fejezetben tárgyalt mutatószámok közül három hibamutató kerülhet szóba:

- **FNMR:** Téves meg nem feleltetés – algoritmikus hiba.
- **FRR:** Téves elutasítási arány – tartalmazza az algoritmikus hibákat (FNMR), valamint a sikertelen mintabeviteli arányt (FTA), amikor a jogosult felhasználó prezentálja a mintáját, a rendszer azonban nem képes azt beolvasni.
- **GFRR:** Általánosított téves elfogadási és elutasítási arány – tartalmazza az algoritmikus hibákat (FNMR), a sikertelen mintabeviteli arányt (FTA), valamint a sikertelen regisztrációs (FTE) arányt is.

Kutatásom ezen szakaszában azt gondoltam, hogy a GFRR definíciójának feleltethető meg a kvantitatív kérdőív eredménye, azonban később felismertem, hogy a populáció egy része szintén nem képes használni az ajtót, analóg módon a sikertelen regisztráció arány (FTE) elvéhez, ezért végül az **FRR – téves elutasítási arányt választottam.**

3.6.1 Hipotézisek és módszertan

Az előkészítés szakaszában gyakran gondoltam a kutatásom tárgyára mint emberi FRR-re. Ez alatt azt értettem, hogy vajon mi az a hibamutató, melyet a hétköznapi felhasználó érzékel és valójában mennyire érzékeny ő a hibákra. Másként fogalmazva hol találkozik a rendszer és az egyén hibamutatója.

Kutatásomban megfogalmazott harmadik hipotézis az, hogy *„biometrikus alkalmazásoknál meghatározható a felhasználók elfogadási intervalluma a téves elutasításokkal szemben, és ez alapján a biometrikus beléptető rendszerek értékelhetők”*. Ahhoz, hogy ezt igazolhassam, a kvantitatív felmérésben a hipotézist két alhipotézisre bontottam és ezeknek egyszerre kell teljesülniük ahhoz, hogy a hipotézis elfogadásra kerüljön.

AH1: A fennakadás gyakorisága negatívan befolyásolja a rendszer megítélt használhatóságát.

AH2: Az emberek elfogadási küszöbe legalább két nagyságrenddel magasabb, mint a gyártók által az eszközre megadott FRR – téves elutasítási értéke (0,01%).

Amennyiben a kutatás olyan eredményeket hoz, mely alapján elfogadom a hipotéziseket, úgy a forgatókönyvi tesztek alapján kapott értékek egyrészt a valóságban statisztikailag is validálhatók, másrészt ténylegesen prediktálni lehet a rendszer használhatóságát az adott alkalmazásban.

A kérdőívet úgy állítottam össze, hogy érvényes és megismételhető legyen, valamint a kitöltők érdeklődéssel olvassák a kérdéseket. A hagyományos kérdőíves platformok (Google-űrlap, Survey Monkey) helyett olyan felületet hoztam létre amely egyedi mind vizuálisan, mind a válaszlehetőségeket tekintve. A kérdőívben továbbá a négy tartalmi kérdés közé ékeltem olyan kérdéseket, amelyek elvonják a figyelmet a célról, végül a tartalmi kérdések sorrendjét minden kitöltőnél előre definiáltan más sorrendben tette fel a rendszer. A kérdőív az I. számú mellékletben található. [114]

A fókuszcsoportos kutatás eredményei alapján a beléptető rendszerekről vagy a biometrikus eszközökről nem volt célszerű újra megkérdezni a válaszadókat. A beléptetési folyamatban részt vevő elemek közül az ajtó volt az, amelyikről leginkább feltételezhető, hogy mindenki ismeri. Az ajtó használati folyamatára alkalmazva a hibás elutasítás modelljét, analóg módon alkalmazható, hogy az ajtó véletlenszerűen megszorul, nem nyílik és újra kell próbálkozni. [103]

Ezek alapján kutatáshoz releváns kérdés szövege így hangzott:

„Képzelje el, hogy heti 5 napon keresztül, napi négyszer kell átmennie egy ajtón a munkahelyén/iskolájában. Ez az ajtó általában jól működik, ám ……. (megakadási gyakoriság) egyszer megakad, és csak egy újabb próbálkozással tudja kinyitni. Mennyire tartja használhatónak ezt az ajtót?”

A megakadás gyakoriságát az áthaladások számának függvényében határoztam meg, ehhez a következő egységekkel dolgoztam:

- naponta egyszer (leggyakoribb);
- hetente egyszer;
- havonta egyszer;
- évente egyszer.

Amennyiben feltételezzük, hogy a válaszadó minden hétköznap legalább négyszer áthalad a kapun (2 belépés és 2 kilépés), akkor havi átlagos 20 munkanappal számolva az évente 960 áthaladást jelent, vagyis a fennakadások relatív gyakorisága (FRR) évente:

- napi egyszeri fennakadásnál 25%;
- heti egyszeri fennakadásnál 5,415%;
- havi egyszeri fennakadásnál 1,25%;
- éves egyszeri fennakadásnál 0,104%.

A megítélt használhatóságot négy fokozatú szemantikus differenciálskálán értékeltem a következő fokozatokat alkalmazva:

- használhatatlan – 1-es érték;
- kevésbé használható – 2-es érték;
- használható – 3-as érték;
- tökéletesen használható – 4-es érték.

Mindkét ismérv ordinális skálán mért adatokat jelent. Az elemzés során az alábbi statisztikai eljárásokat alkalmaztam: leíró statisztika, intervallumbecslés (90%-os konfidencia intervallummal, mely értéket a biometrikus rendszerek értékelésénél használatos Doddington-szabály indokol), kereszttábla elemzések (α = 0,05 szignifikanciateszttel) és nemparametrikus hipotézis próbák (ugyancsak p = 0,95), valamint regresszióanalízis.

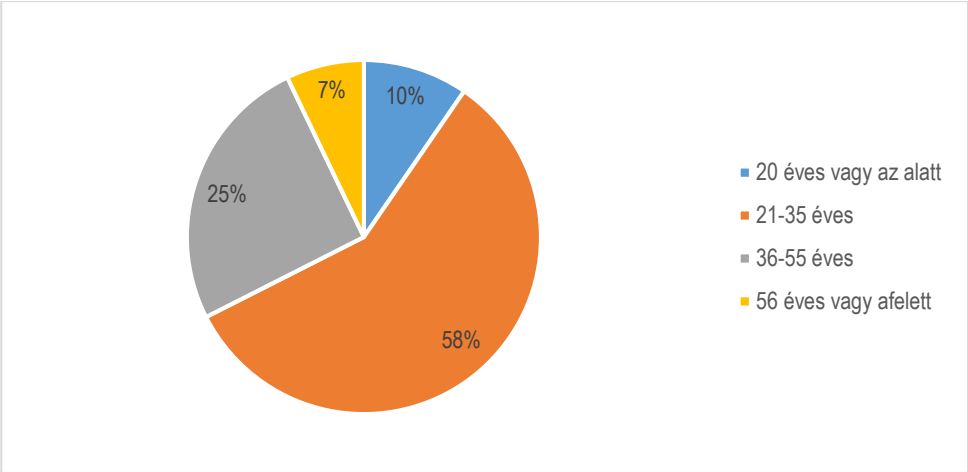
3.6.2 Eredmények

Az adatok felvétele 2017. márciusa és áprilisa között történt az Óbudai Egyetem hallgatóinak (446 fő, a kitöltők 60,8%-a) és a MENSA HungarIQ tagjainak (197 fő, a kitöltők 26,8%-a), valamint más egyetemek hallgatói körében (91 fő, a kitöltők 12,4%-a) körében. Az adatok tisztítása után *n = 734* kitöltő válaszaival dolgoztam, ezt az elemszámot további 653-ra csökkentettem, ami azon válaszadókat fedi le, akik minden válaszra feleltek. A mintaválasztás két szempont alapján történt, egyfelől az Óbudai Egyetem Campusain a hallgatók már találkoznak és naponta használnak beléptető kapukat, másfelől ők képezik majd a munkaerőpiac szerves részét, ahol a tapasztalataim alapján a vállalatok döntő többségénél, ezen belül a nagyvállalatok mindegyikénél találkoznak ilyen beléptető rendszerekkel. Az Óbudai Egyetem hallgatói közül 390 fő a Bánki Donát Gépész- és Biztonságtechnikai Mérnöki Kar hallgatója, ők nemcsak találkoznak ilyen rendszerekkel, de tanulmányaikban is megjelenik az. A kitöltők egy része – 497 fő – jellemzően olyan területen dolgozik, ahol találkozhat ilyen rendszerekkel.

Minta elemzése

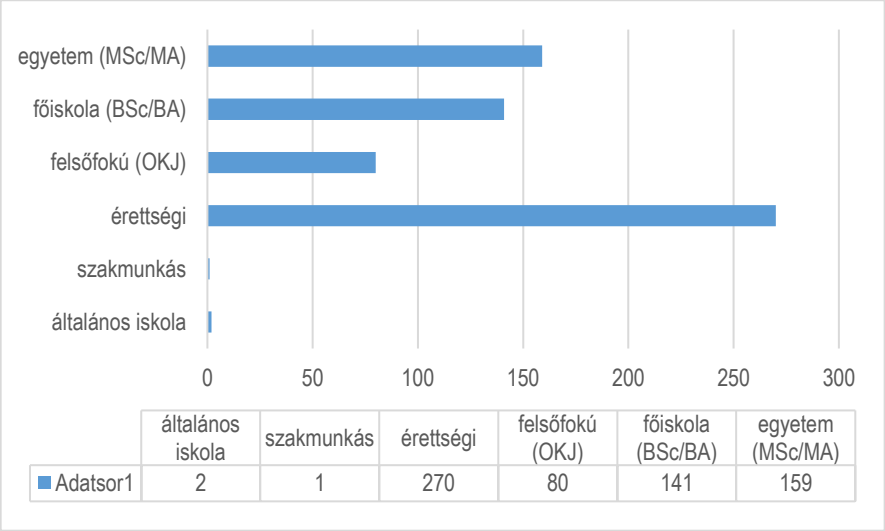
A válaszadók megoszlása a következőképpen alakult.

Nemek szerint a kitöltők 74,4%-a (486 fő) férfi és 25,6%-a (167 fő) nő. A kor szerinti megoszlás a következő ábrán látható, melyből kitűnik, hogy a kitöltők nagy része 21–35 év közötti::



25. ábra: A kitöltők kor szerinti megoszlása (n = 653); forrás: saját szerkesztés

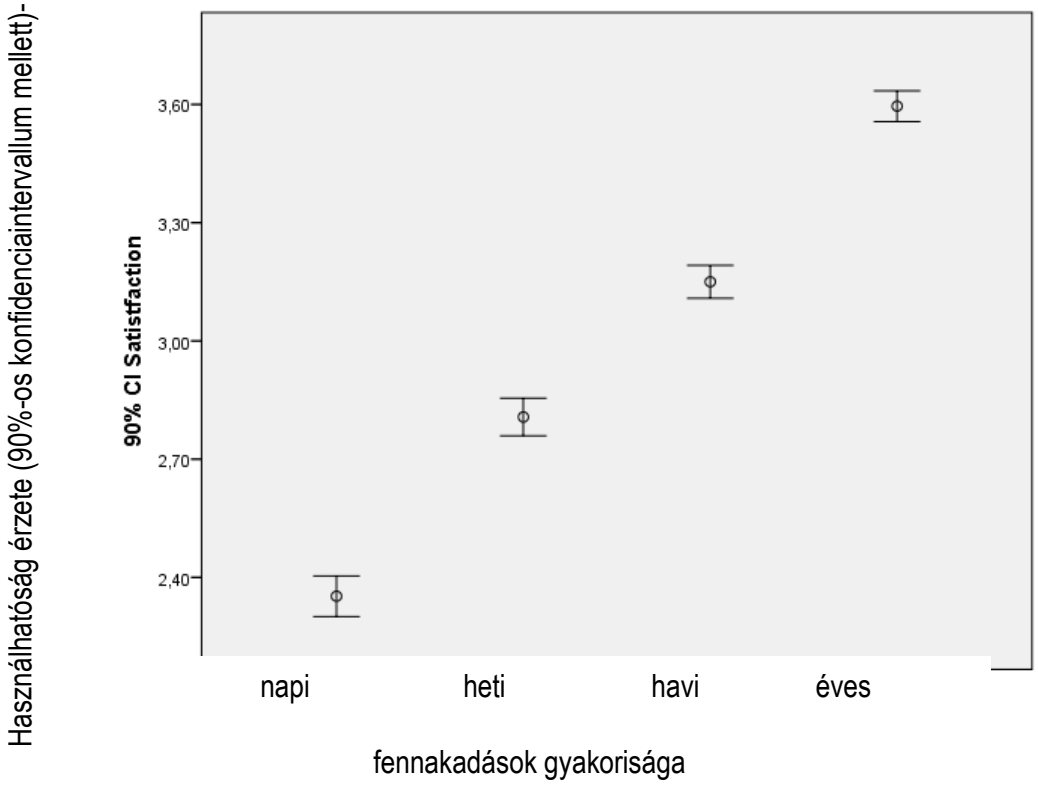
A végzettség szerinti megoszlást a következő ábra tartalmaza, melyből kitűnik, hogy a kitöltők nagy része BSc-tanulmányait folytató, még nem végzett hallgató:



26. ábra: A kitöltők végzettség szerinti megoszlása (n = 653); forrás: saját szerkesztés

A mintaválasztás önkényes kiválasztáson alapult, a minta nagy elemszámú. Kutatásom során nem törekedtem reprezentativitásra, mivel az alapsokaság nehezen jellemezhető, így nem tekinthető reprezentatívnak, azonban az eredmények alapján következtetni lehet az alapsokaságra. A nagy elemszám miatt a beléptető kapukat használók sokaságához külön súlyokat nem használtam. A kapott válaszok kitűnő iránymutatást adnak, hiszen ilyen magas kitöltői számnál a centrális határeloszlás által a normális eloszlással számolhatok. Az egyes vizsgált ismérvek esetén normalitás (illeszkedés)-vizsgálat is történt. [104]

A fennakadások gyakorisága és a használhatóság megítélésében szembetűnő (szignifikáns sig.p = 0 < 0,05) összefüggés van. **A fennakadások gyakoriságának csökkenésével nő az elégedettség.** Az összefüggés Pearson-féle korrelációval R = 0,543, közepesen erős kapcsolatot mutat.

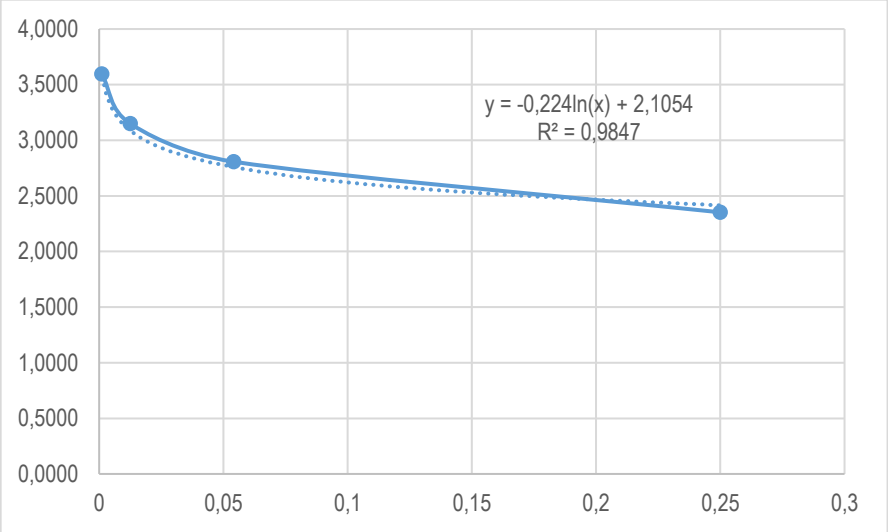


27. ábra: A válaszadók átlagos elégedettsége a fennakadások gyakoriságának függvényében 90%-os konfidenciaintervallum mellett n = 653; forrás: saját szerkesztés

Amennyiben az időegységet nem ordinális, hanem arányskálán ábrázolom, azaz a fennakadások gyakoriságát a fentebb leírt százalékos (relatív) megoszlásban vizsgálom, az érték nagyon hasonló lesz (R = –0,479 – a negatív értéket indokolja, hogy ahogyan csökken a fennakadások gyakorisága, úgy nő a felhasználó elégedettsége).

Ez a közepesen erős szignifikáns együttjárás lehetővé teszi, hogy regressziós függvényt illesszek az adatokra. Az illesztés során már a fennakadások gyakoriságát az időegység százalékában vizsgáltam. A legjobb illeszkedés a logaritmikus függvény esetén mutatkozik, melyet a következő ábra szemléltet. A konstans értéke 2,1054, vagyis semleges a beállítódás az ajtó fennakadására, amely a fennakadás gyakoriságának a növekedésével csökkenti az eszköz használhatóságának az értékét. Ebben az esetben a fennakadás gyakoriságának egy százalékos (itt a 960 darab éves áthaladási alkalomból, napi négyszeri áthaladásnál vett egy százalékról van szó) emelkedése a

felhasználó 0,224 egységnyi használhatósági érzet csökkenésével jár (az előzőekben definiált leírt 4 fokozatú skálán tekintve).



28. ábra: A válaszadó átlagos elégedettségi szintjére illesztett regressziós függvény a fennakadások gyakoriságának függvényében (n = 653) (X tengelyen: fennakadás éves relatív gyakorisága, Y tengelyen: használhatósági/elégedettségi szint mértéke); forrás: saját szerkesztés

Az eredmények alapján elfogadom az AH1 alhipotézisemet, mely szerint a fennakadás gyakorisága és a rendszer megítélt használhatósága között összefüggés van.

A kapcsolat erőssége miatt az adatokra logaritmikus regressziós függvényt is illesztettem. Szükséges megemlítenem azonban, hogy a magyarázó erő (R négyzete) 0,295, azaz a fennakadások gyakorisága csak közel 30%-ban magyarázza a felhasználó megelégedettségét. A továbbiakban felmerül a kérdés, hogy még vajon mi lehet hatással a felhasználó megelégedettségére. A kérdőívben megkérdeztem a kitöltőket a(z) munkahelyi/iskolai megelégedettségről, a munkájukhoz/tanulmányukhoz kapott információk teljességéről, és arról, hogyan érzik magukat. A kérdőív kérdései közzé ékeltem olyan kérdéseket, melyek nem kapcsolódnak szorosan a kutatás tárgyához, azonban kiküszöbölik, hogy a sorrendben feltett kérdéseknek mi a célja, ezzel minimalizáltam a sugalmazás lehetőségét. A kérdésekben főleg a kitöltők érzelmi/elégedettségi állapotára voltam kíváncsi. A kérdések így hangzottak:

- Hogyan érzi magát most?
- Mennyire elégedett a munkájához/tanulmányaihoz kapott információkkal?
- Mennyire ajánlaná másnak a jelenlegi munkahelyét/iskoláját?

A válaszokat itt is szemantikus differenciál skálán értékelhették a válaszadók. Érdekes lehet, de a kutatásomban nem térek ki ezen kérdésekre adott válaszok egyenkénti elemzésére. Ezen eredmények esetében csak azokat az együttjárásokat vizsgálom, ahol a felhasználó aktuális

hangulata és munkája iránti attitűdje hatással van az általam vizsgált használhatósági értékre. Az összehasonlítás során az általános eszköz megelégedettségi szintet vizsgáltam, ahol szignifikáns összefüggéseket találtam (sig. $p < 0,05$), azok a következő jellemzők voltak:

1. Aki jobban érezte magát, vagyis magasabb értéket jelölt meg ezen a skálán az általánosan az eszközt is használhatóbbnak értékelte (Cramer-értéke: 0,179).
2. Minél több információt kap a válaszadó, annál elégedettebb az eszközzel is (Cramer-értéke: 0,197).
3. Ez esetben a kapcsolat iránya nem került azonosításra (az ok-okozati összefüggés), de szignifikáns kapcsolat mutatkozott az eszköz iránti elégedettség és az ajánlás mértékével (Cramer-értéke: 0,161).

A legerősebb kapcsolat az információ esetén mutatkozik. Egy másik kérdésben az előreláthatóság mértékét jelölték meg a legtöbben legfőbb munkahelyi stresszforrásként. **Ez rámutat arra, hogy az oktatás, megfelelő tájékoztatás és információátadás csökkenti a bizonytalanságot és ezáltal javítja az eszköz használata iránti attitűdöt, annak elfogadását.** [105] Ezeket a tényezőket mindenképpen érdemes tovább vizsgálni. [106]
Látható, hogy mindenhol szignifikáns, de nagyon gyenge kapcsolat mutatható ki, ezért a fenti modell magyarázó erejét csak gyengítenék ezen faktorok egy többtényezős regressziós modell alkalmazásának esetén, ezért elfogadom a kéttényezős modellt.

Az AH2 alhipotézis szerint a felhasználók elfogadási küszöbe több nagyságrenddel magasabb, mint az adatlapokon általában megadásra kerülő hibás elutasítási arány (FRR = 0,01%). Ahogyan látható a 28. ábrán a 3.00 „Használható” értékhez körülbelül 3%-os FRR tartozik. **Az eredmények alapján az AH2 alhipotézist is elfogadom.**

A harmadik hipotézisemet két alhipotézis elfogadásához kötöttem, mivel mindkettő igazolást nyert az eredmények alapján, ezért ezt ahipotézist is **elfogadom**.

3.7 Összefoglalás és következtetések

Primer kutatásomban első körben összegyűjtöttem azokat a kutatásokat, amelyek a felhasználók attitűdjét vizsgálják és rámutattam a kutatások hiányosságaira. Fókuszcsoportos vizsgálatot alkalmaztam annak érdekében, hogy jobban megértsem a felhasználók gondolatait, érzéseit a beléptető rendszereket illetően. Ennek legfontosabb eredménye az, hogy szinte még egy homogén csoportban sincs azonos fogalmi kör.

Ezek alapján ki kellett dolgozni egy olyan kérdéssorozatot, amelyet az emberek sokkal inkább azonosan értenek, így jutottam el az ajtó megszorulása, mint a hiba analógiájához. Ezzel a megközelítéssel jóval általánosabb és széleskörűen használható eredményekhez jutottam a kvantitatív kutatásban.

Az ajtó megszorulási problémáját meg kellett feleltetnem a biometrikus rendszereknél használatos hibamutatók egyikének, ezért összegyűjtöttem a szakirodalomban szereplő mutatókat és levezettem, hogy az FRR-mutató felel meg legjobban a kutatási céloknak.

A tömegtartózkodású objektumok tulajdonsága, hogy sok felhasználó használja, kötelező jelleggel, nincs alternatív azonosítási lehetőség és a kiválasztás negatív jellegű. Ezeknél az alkalmazásoknál a hibás elutasítási arány (FRR) a legfontosabb tényező, mivel ez befolyásolja azt, hogy mindenki tudja-e használni a rendszert, elég gyorsan és kevés téves elutasítással.

A biometrikus rendszerek gyártói algoritmikus FRR-értékeket adnak meg (0,001–0,01%), amelyek több nagyságrenddel jobbak, mint amit a gyakorlatban el lehet érni.

Ezek alapján elvégeztem a kvantitatív kutatást. Az adatok felvétele 2017. márciusa és áprilisa között történt az Óbudai Egyetem hallgatóinak (446 fő, a kitöltők 60,8%-a) és a MENSA HungarIQ tagjainak (197 fő, a kitöltők 26,8%-a), valamint egyéb egyetemi hallgatók körében (91 fő, a kitöltők 12,4%-a) körében.

Az eredmények nem általánosíthatók, azonban pilotkutatásként megállja a helyét, ugyanis a későbbi kutatások során a felhasználók által értett és használt kifejezéseket tudom használni, biztosítva ezzel a kutatás érvényességét.

A beléptető rendszerek általánosan ismertek a felhasználók előtt, mindenki találkozott már velük valahol. Teljesen másként ítéli meg egy szakember a rendszert, mint egy általános felhasználó, ezért a további kutatásokban célszerű ezeket kiszűrni.

A fókuszcsoportos felmérésemben a válaszadók több mint fele negatívan vélekedett a beléptető rendszerekről, 37% a lassúságot nevezve meg hátrányként, és mindössze 27% nevezte biztonságosnak. További kutatásban érdemesnek tartom pontosítani a fogalmak jelentését, hiszen a résztvevők akár rokon fogalmakként is használhatták ezeket (egyszerre biztonságos és lassú).

A fókuszcsoport válaszadói legtöbbször forgókapus, forgóvillás és fémdetektoros kaput említettek, azaz jellemzően teljes belépési pontokkal találkoztak. Ebből az következik, hogy a biometrikus gyártók által megadott algoritmikus hibás elutasítási aránnyal a felhasználó gyakorlatilag nem találkozik. A megadott algoritmikus FRR-értékek 0,01–0,001% tartományban mozognak, azaz a

felhasználók 10.000–100.000 áthaladásonként egy alkalommal találkoznának velük, napi 4 áthaladással számolva hozzávetőlegesen 15–150 évente egyszer(!) történne egy sikertelen azonosítás, ez az arány nyilvánvalóan fel sem tűnne az embereknek, és triviális, hogy a népesség döntő többsége nem is találkozott volna ilyen jelenséggel.

Érdemes viszont megkeresni azt a gyakorlati értéket, ahol a felhasználók rendszeresen sikertelenül mennek át különböző belépési pontokon mechanikai vagy felhasználói hiba folytán, de még elfogadhatónak értékelik a rendszer működését.

Ennek azért van jelentősége, mert ekkor a különböző biometrikus beléptető rendszereket nem lehet algoritmikus értékek alapján rangsorolni. Ezzel szemben a gyakorlati hibás áthaladási értékeket tesztelve biometrikus beléptető rendszereknél – amelyek 1–20% között mozognak – már van értelme tesztelni és ezeket statisztikailag is lehet értékelni.

Peltier rendszerezi azokat a jellemzőket, melyek a biztonságot segítendő rendszerek bevezetése előtt megfontolandók. [85] Ezek közül a felhasználók véleményére fókuszáltam összevetve az általuk adott elfogadást (jóság mutatót) a rendszerek műszaki paramétereivel. Ennek oka, hogy a kutatásom célcsoportja a végfelhasználó, akit nem műszaki paraméterein keresztül, hanem társadalomtudományi módszerekkel hipotetikus helyzetben elképzelt szituációkra adott introspektív válaszai által teszteltem.

A biztonságérzet csökkenésével egyre több biztonsági és biometrikus rendszert vezetnek be a világon. A felhasználók általi elfogadottság szorosan együttjár azzal, hogy tudják-e használni a rendszert. Kutatásomban ezért két alhipotézist teszteltem, amelyek ha elfogadásra kerülnek az eredmények alapján, igazolják az eredeti hipotézisemet. [107]

AH1: A fennakadás gyakorisága és a rendszer megítélt használhatósága között összefüggés van.

AH2: Az emberek elfogadási küszöbe több nagyságrenddel magasabb, mint a gyártók által az eszközre megadott FRR – téves elutasítási értéke.

Mindkét hipotézist az eredmények alapján elfogadtam, ezzel bizonyításra került, hogy a forgatókönyvi teszteknél mért valós FRR-értékek ebben a tartományban értékelhetők. Habár a műszaki paraméterek fontosak a döntésben, mégsem mindig a műszaki adatok (paraméterek) a legfontosabb tényezők, ahogyan a kutatás mutatja is, az egyéni felhasználók kevésbé érzékenyek, mint a hitelesített FRR tartománya.

Az adott biztonsági körülmények között meg kell határozni, hogy a felhasználók milyen elfogadási értéke felel meg az üzleti döntéshozóknak, és erre az értékre lenne szükséges a biometrikus

beléptető rendszereket igazítani. Az is kiderült, hogy oktatással és az információk átadásával az elfogadottság szignifikánsan javítható. A szakirodalomban is legfontosabbnak egy ilyen rendszer bevezetése során a megfelelő képzést és tréninget, a későbbiekben pedig a körültekintő kontrollt tartották a legfontosabbnak. [108] [112]

A kvantitatív kutatás eredménye, hogy az emberek **mintegy 3-5%-os kényelmetlenséget még jellemzően elfogadnak**. Ez azt jelenti, hogy tréning és az adott rendszerhez való elköteleződés javítása nélkül ilyen mértékű kényelmetlenséget még különösebb elégedettségcsökkenés nélkül fogadnak a felhasználók. [109]

ÖSSZEGZETT KÖVETKEZTETÉSEK

A kutatási céljaim elérése érdekében átfogó vizsgálatot végeztem a biometrikus személyazonosító eszközök használata tekintetében. A műszaki ismereteimen felül jelentősen bővítettem tudásomat a matematikai, statisztikai és társadalomtudományi területekről is. Téziseimet és az ajánlásokat a tudományos közösségben megvalósult publikációk és viták alapján fogalmaztam meg.

A kutatómunka összegzése

Napjainkban egyre nagyobb az igény az emberek egyértelmű azonosítására – tekintve, hogy a globális biztonsági helyzet egyre romlik. Az elmúlt időszakban nyilvánosságra került hackertámadások, felhasználó-, jelszó- és identitáslopások pedig jobb megoldások alkalmazását igénylik. A biztonsági és egyéb kereskedelmi és marketingigények miatt a biometrikus azonosításra egyre nagyobb szükség van, azonban nem mindegy, hogy melyik alkalmazáshoz milyen technológiát és eszközt választanak ki a szakemberek. Értekezésemben azt tűztem ki célul, hogy ezt a kiválasztási folyamatot támogassam olyan megközelítésben, amelyet még a szakirodalom ebben a formában nem tárgyalt.

Az első fejezetben a biometria alapjainak bemutatása után feltérképeztem a biometrikus megoldások alkalmazási területeit, majd azonosítottam, hogy mely területek és miért kritikusak a bevezetés sikerességének szempontjából.

A második fejezetben teljeskörűen levezettem a tömegtartózkodású objektumokra jellemző beléptetési folyamat matematikai modelljét. Ezt a sorbanállási modellt a gyakorlatban alkalmazva megmutattam, hogyan lehet méretezni egy beléptető rendszert.

Az utolsó, harmadik fejezet az értekezés legfontosabb része, mely tartalmazza a szakmai tapasztalataimra alapozott kvalitatív, és ennek eredményeire épülő kvantitatív kutatást. Először fókuszcsoporttal felmértem az emberek ismereteit, attitűdjét a beléptető rendszerekről. Majd online kérdőíves kutatással bebizonyítottam, hogy az eszközök gyártói által megadott működési bizonytalanság alapvetően több nagyságrenddel alacsonyabb, mint az emberek elfogadási küszöbe, ily módon ez a tervezésnél figyelmen kívül hagyható. A beléptetési folyamat minden elemét figyelembe kell venni, és annak kell összességében maximum 3-5%-os téves elutasítást produkálni ahhoz, hogy még használható legyen. Az első három fejezet eredményei alapján végeztem el a hipotézisek vizsgálatát, majd megalkottam a téziseket, a kutatási eredményeket, valamint az ajánlásokat.

Új tudományos eredmények – tézisek

1. *A gyakorlatban kiépített biometrikus beléptető rendszerek elemzése alapján* ***elsőként alkottam meg a biometrikus alkalmazások osztályozási rendszerét és kimutattam, melyek a kritikus alkalmazások.***
2. *A beléptetés folyamatának megismerésével és elemző modelljének felállításával* ***megalkottam a biometrikus beléptetés sorbanállási modell hatékony elemezhetőségének eszközét.***
3. *Kvalitatív és kvantitatív kutatással* ***bebizonyítottam, hogy létezik az elfogadási intervallum, amely alapján a biometrikus beléptető rendszerek minősíthetők.***

Ajánlások

A biztonsági szakembereknek a biometrikus projektek elemzése és tervezése során javaslom, hogy állapítsák meg az adott alkalmazásról, hogy kritikus-e vagy sem és ezt mint kiválasztási szempontot vegyék figyelembe a beruházásnál.

Javaslom, hogy a tömegtartózkodású objektumok beléptetési projektjeinél használják fel az általam megadott számítási módszereket és sikerkritériumként vessék össze a várható értékeket az üzleti, biztonsági igények alapján kapott elvárásokkal.

Végül javaslom, hogy végezzenek maguk vagy vegyenek igénybe más hiteles forrásokat a biometrikus rendszerek forgatókönyvi tesztjeiről, és állapítsák meg a rendszer várható hibás elutasítási (FRR) értékét. Célszerű megállapítani – ha meg lehet – egy felhasználó kör elfogadási küszöbét, és ezt érdemes felhasználni a rendszerek értékelésekor. Ha nem lehet megállapítani, bátran használják fel az általam felismert tartomány alsó értékét, ez mintegy 3% téves elutasítási küszöb, amit a felhasználók még el fognak fogadni.

Jövőbeni kutatási irányok

Doktori értekezésem egyik célja, hogy tudományos alapot szolgáltasson a téma további elemzéséhez és kutatásához. Indokoltnak és célszerűnek tartom a folytatást az alábbi területeken:

1. A kutatást érdemesnek tartom Magyarország viszonylatában reprezentatívan megvalósítani, ily módon pontosabb eredményeket lehetne kapni, amelyet az adott alkalmazásban fel lehet használni. A kutatást néhány évente meg kellene ismételni annak érdekében, hogy felmérhető legyen az attitűd időbeli változása.

2. Az EU 2016/679 rendeletének 29. cikke szerinti adatvédelmi csoport *„3/2012. sz. véleménye a biometrikus technológiák terén történt fejleményekről”* szerint *„A biometrikus rendszerekről már a bevezetésük kezdetétől fogva elismerték, hogy számos területen súlyos aggodalmakat vethetnek fel, ideértve a magánélet védelmét és az adatvédelmet.”*, továbbá: *„A leplezett technikák lehetővé teszik az egyének tudtukon kívüli azonosítását, ami a magánéletet érintő súlyos fenyegetést eredményez, és csökkenti a személyes adatok feletti ellenőrzést.”* [110] Célszerű lenne a témát feltérképezni jogi megközelítésben is.
3. Az emberek attitűdje megismerhető és befolyásolható: a szociálpszichológiai elemzések között a szociometria tekintélyes helyet foglal el. A módszer célja a csoportok személyközi kapcsolatainak feltárása és ez alapján a társas alakzat kidolgozása. [111] A felhasználói elfogadottság problémáinak megértése a biztonsági szakemberek számára véleményem szerint kulcsfontosságú. Ezt az irányt elkezdtem kidolgozni a *Hadmérnök* folyóiratban megjelent *A biztonsági rendszerek felhasználói attitűdje, értékelése és befolyásolásának lehetőségei* cikkemben. [112]
4. A felhasználók attitűdje megismerésének legfontosabb technikája a kérdőíves véleményfelmérés. Minden felmérés elemi érdeke, hogy a megcélzott csoport szükséges elemszámú résztvevője hitelesen töltse ki a kérdőívet. Az empirikus eredmények azt mutatják, hogy minél hosszabb egy kérdőív, annál nehezebb kitöltetni azt. Egy lehetséges módszer, hogy olyan kérdőíves szoftverfelületeket kell létrehozni, amelyeket szeretnek a felhasználók, továbbá matematikai módszerekkel kiszűrhetők a valótlan állítások. Ezeket a területeket két cikkemben kezdtem el feldolgozni: *Attitűd-kockázatfeltáró robot* és *Ergonómia és hasonlóságelemzés a biometrikus rendszerek felhasználóinak tükrében*. [113] [114]

BEFEJEZÉS

Amikor a kutatói munkát megkezdtem, a problémára adott válaszok, és a kutatás eredménye még ismeretlen volt a számomra. A probléma azonban ismert volt. Tapasztalataim azt mutatták, hogy túl sok a sikertelen biometrikus személyazonosítási projekt, pedig néhányuk következménye akár előre látható is volt.. Erre a problémára akartam egy olyan megoldási módszert kidolgozni, és a szakemberek rendelkezésére állítani, amely biztosítja, hogy a tervezésnél, tenderezésnél és bevezetésnél nagyobb legyen a siker.

Ehhez az kellett, hogy azonosítsam azokat a területeket, ahol várhatóan nagy kockázatú a biometria bevezetése, majd matematikai modellt kellett létrehoznom, amivel az üzleti-biztonsági kérdésekre adott egzakt mérnöki válasz előre jelzi, hogy egyáltalán meg lehet-e felelni ezeknek. Végül számszerűsítettem, hogy mi az a hibás működéssel szembeni elfogadási küszöb, amit az emberek még különösebb elégedetlenség nélkül el tudnak fogadni. Jelen értekezésemben ezt a három problémakört vázoltam fel, és célul tűztem ki azok felkutatását, megválaszolását, hogy gyakorlatban is alkalmazható eredményeket tudjak felmutatni.

A problémát kétoldalúan vizsgáltam, egyrészt magát a biometrikus rendszer hatékonyságát vizsgáltam, másrészt feltérképeztem a felhasználók elfogadottságát a biometrikus rendszerekkel szemben. Az eredményeim alapján elmondható, hogy létrehoztam a biometrikus alkalmazások osztályozási rendszerét, és azonosítottam azokat a területeket, melyek kritikusak egy biometrikus rendszer esetén, mint a beléptetés és a munkaidő-nyilvántartás. Ezt követően részletesebben megismertem a beléptetés folyamatát, melynek felállítottam az elemző modelljét. Megalkottam egy hatékony eszközt, mellyel elemezhető a biometrikus beléptetés sorbanállási modellje. A többlépcsős primer kutatás hozzájárult, azon elfogadási intervallum felkutatásához, amely alapján a biometrikus beléptető rendszer minősíthető.

A biometrikus beléptető rendszerek jelen vannak a mindennapi életünkben, és nem elhanyagolható azok biztonságos, kényelmes és lehetőleg a legalacsonyabb hibaküszöbbel való működésük. Bízom benne, hogy a kutatásom során kapott eredményeket a szakemberek megismerik és hasznosítják a munkájuk során, hiszen közös érdekünk a rendszerek hatékonyabbá tétele és a felhasználók elfogadottságának növelése.

KÖSZÖNETNYILVÁNÍTÁS

Köszönettel tartozok prof. dr. Kovács Tibornak, témavezetőmnek, a nyitott hozzáállásáért, az értékes gondolataiért és mindenkori támogatásáért azon az úton, amelynek eredményeit jelen értekezésben foglalom össze.

Ezúton köszönöm mindazok segítségét, akik végig támogatták a munkámat. Elsősorban prof. dr. Pokorádi László, prof. dr. Rajnai Zoltán és dr. Hanka László hozzájárulását, akik segítettek a matematika eszköztárának használatában és megértésében. A fókuszcsoportos és kvantitatív kutatás kidolgozásában és elemzésében dr. Kolnhofer-Derecskei Anita támogatott, aki nélkül nem jöhetett volna létre ilyen magas szintű elemzés, és köszönöm az inspiratív beszélgetéseket is. Amikor elakadtam a kutatásomban – és bizony sokszor volt ilyen –, a családom lendített tovább a mélypontokon. Ők biztosították azt az érzelmi biztonságot, amely nélkül már rég feladtam volna. Édesanyám mindig hitt bennem, amit őszintén csodálok. Drága Feleségem nélkül sosem tartanék itt, mindig mellettem állt, remek ötleteket adott, és sokszor hajnalonként hallgatta a gondolatmeneteimet. Köszönet illeti továbbá a gyermekeinket, mert látva a hihetetlen kitartást és örömmel tanulni vágyást, óriási erőt adtak, hogy ne adjam fel.

IRODALOMJEGYZÉK

[1] CHRISTIAN L., A magánbiztonság elméleti alapjai, Budapest: NKE, 2014.

[2] LUKÁCS G., Új vagyonvédelmi nagykönyv, Budapest: CEDIT 2000, 2002.

[3] TÓTH A. és TÓTH L., Biztonságtechnika, Budapest: Nemzeti Közszolgálati és Tankönyv Kiadó Kft., 2014.

[4] TÓTH L., , *Video menedzsment (VMS) rendszerek összehasonlítása, trendek és az élőerő szerepe, jelentősége a CCTV technológiában.* Magyarországi Fegyveres Biztonsági Örök, 2017.

[5] *2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.*

[6] *ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems. Requirements..*

[7] KOVÁCS T., OTTI Cs. és MILÁK I., „A biztonságtudomány biometriai aspektusai," in *A biztonság rendészettudományi dimenziói: Változások és hatások.*, Pécs, Magyarország, Magyar Rendészettudományi Társaság, 2012, pp. 485-496.

[8] A MAGYAR TUDOMÁNYOS AKADÉMIA NYELVTUDOMÁNYI INTÉZETE, „A magyar nyelv értelmező szótára," A Magyar tudományos Akadémia Nyelvtudományi Intézete, 2016. [Online].
Elérhető: http://mek.oszk.hu/adatbazis/magyar-nyelv-ertelmezo-szotara/elolap.php. [Hozzáférés dátuma: 2019. május 3.].

[9] *ISO/IEC 31010: 2019, Risk management - Risk assessment techniques.*

[10] CHUNLIN L., CHONG-KUAN T., YEA-SAEN F. és TAT-SENG L., „The Security Risk Assessment Methodology," in *Procedia Engineering*, International Symposium on Safety Science and Engineering in China, 2012, Elsevier Ltd., 2012, pp. 600-609.

[11] KOVÁCS T. és HORVÁTH T., „Kockázatértékelési módszerek, azok alkalmazási lehetőségei a fizikai védelem területén," in *TAVASZI BIZTONSÁGTECHNIKAI SZIMPÓZIUM 2013.*, Budapest, Óbudai Egyetem, 2013, pp. 1-10.

[12] JAIN A. K., NANDAKUMA K. és ROSS A., „50 years of Biometric Research: Accomplishments, Challenges and opportunities," *Pattern Recognition Letters,* pp. 1-26, 2016.

[13] OTTI Cs., „Biometrikus rendszerek felhasználói minta pozicionálásának kérdései," in *DOSZ, Tavaszi Szél 2016*, Budapest, 2016.

[14] OTTI Cs., „Comparison of biometric identification methods," in *2016 IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, Timisoara, 2016.

[15] JAIN A. K., NANDAKUMA K. és ROSS A., Introduction to Biometrics, New York: Springer, 2011.

[16] LIM M. H. ésTEOH A., „Biometric Template Binarization," in *Encyclopedia of Biometrics*, New York, Springer, 2015, pp. 257-263.

[17] EUROPEAN DATA PROTECTION SUPERVISOR, „The History of the General Data Protection Regulation," European Union, 2019. [Online]. Elérhető: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en. [Hozzáférés dátuma: 2019. február 14.].

[18] FÖLDESI K., *A biometrikus azonosítási eljárások alkalmazhatósága a rendőri munkában. Ph.D. értekezés,* Budapest: Óbudai Egyetem, Biztonságtudományi Doktori Iskola, 2017.

[19] MODI S. K., Biometrics in Identity Management: Concepts to Applications, Norwood: Artech House, 2011.

[20] FIALKA G., *A pénzintézeti biztonság fogalma, eredete, jelene, jövője, a paradigmaváltás feltételei és jelentősége. Doktori (PhD) értekezés,* Budapest: Óbudai Egyetem, Biztonságtudományi Doktori Iskola, 2016.

[21] OTTI Cs., „THE PAST, PRESENT AND FUTURE OF BIOMETRICS," in *Sixth International Scientific Videoconference of Scientists and PhD. students or candidates*, Obuda University and University of Economics in Bratislava, 2016.

[22] *58/2010. (OT 33.) ORFK utasítás Az Automatikus Arcképfelismerő és Azonosító Rendszer bevezetéséről,* 2010.

[23] DILLON A. és MORRIS M. G., „User acceptance of new information technology: theories and models.," *Annual Review of Information Science and Technology,* kötet 31, pp. 3-32., 1996..

[24] SUPLICZ S., FŐZI B. és HORVÁTH S., „Írisz felismerésen alapuló beléptető rendszer által keltett attitűdök és averzív reakciók vizsgálata," in *Budapesti Műszaki Főiskola*, Budapest, 2006.

[25] FÖLDESI K. és KOVÁCS T., *Összehasonlító kutatáselemzés a biometrikus személyazonosító-beléptető rendsze-rek, eljárások 2006. és 2014. évi társadalmi averzív reakcióinak vizsgálatára,* Budapest: Securinfo, 2015.

[26] LI S. Z. és JAIN A. K., Encyclopedia of Biometrics - Second Edition, New York: Springer; 2nd ed. 2015 edition , 2015.

[27] KATONA G., „A rendészet fogalma és tagozódása.,” *Magyar Rendészet ,* kötet 4, pp. 11-19, 2003.

[28] KOMARINSKI P., Automated fingerprint identification systems (AFIS), USA: Academic Press, 2005.

[29] SZÁZADVÉG POLITIKAI ISKOLA ALAPÍTVÁNY, „Szakpolitikai tanulmány – Rendvédelem és Közbiztonság,” Századvég Politikai Iskola Alapítvány, Budapest, 2019..

[30] BALLA J., *A biometrikus adatokat tartalmazó úti és személyazonosító okmányok biztonságnövelő hatása a határ- es közbiztonság alakulására. Doktori (PhD) értekezés,* Budapest: Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, 2013.

[31] KSH, „Magyarországi regionális nemzetközi repülőterek utasforgalma,” KTI, 2016. [Online]. Elérhető: http://www.kti.hu/trendek/magyarorszagi-regionalis-nemzetkozi-repuloterek-utasforgalma-2004-2015/. [Hozzáférés dátuma: 2019. február 16.].

[32] VARGA J. és BORSZÉKI J., „Intelligens határok,” *Hadtudományi Szemle,* kötet 7, szám 1, pp. 278-288., 2014..

[33] GÖRBE ATTILÁNÉ K. Z., *A magyarországi migráció helyzete, kezelésének feltételei és lehetıségei, doktori (PhD) értekezés,* Budapest: Zrinyi Miklós Nemzetvédelmi Egyetem, 2010.

[34] BÖRÖCZ M., *Az illegális migráció és a terrorizmus közti összefüggések vizsgálata,* Budapest: Terrorelhárítási Központ, 2015.

[35] KOVÁCS T., Biometrikus Azonosítás, Budapest: Óbudai Egyetem, 2015.

[36] LÁSZLÓ C., A magánbiztonság elméleti alapjai, NKE RTK: NKE, 2014.

[37] OTTI Cs., „Termelő cégeknél használt kézgeometria azonosítóval megvalósított munkaidő elszámoló rendszerek gyakorlati tapasztalatai és megtérülés-számítása,” in *Óbudai Egyetem, Nemzetközi Gépész, Mechatronikai és Biztonságtechnikai Szimpózium*, Budapest, 2011.

[38] OTTI Cs., „Integrált munkaidő nyilvántartó rendszerek a gyakorlatban,” in *Gépész, Mechatronikai és Biztonságtechnikai Szimpozium*, Budapest: Budapesti Műszaki Főiskola Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, 2009.

[39] *2012. évi I. törvény a munka törvénykönyvéről.*

[40] BEREK L., Biztonságtechnika, Budapest: Nemzeti Közszolgálati Egyetem, 2014.

[41] OTTI Cs., „Arcfelismerő rendszerek gyakorlati problémái,” in *Óbudai Egyetem, KGK, Vállalkozásfejlesztés a XXI. században*, Budapest, 2014.

[42] TÓTH L., CCTV Magyarul, Budapest: BM Nyomda Kft., 2004.

[43] MICHELBERGER P., Információbiztonság, Budapest: Óbudai Egyetem, Keleti Károly Gazdasági Kar, 2013.

[44] OTTI Cs. és RÓNASZÉKI P., „Információbiztonság: az ISO 27001 információbiztonsági irányítási rendszer 2. rész," *DETEKTOR Plusz,* 2. kötet, pp. 18-19, 2013.

[45] OTTI Cs. és RÓNASZÉKI P., „Információbiztonság: az ISO 27001 információbiztonsági irányítási rendszer 1. rész," *DETEKTOR Plusz,* 1. kötet, pp. 10-11, 2013.

[46] VALERO G., „Banks secure customer access with fingerprint and fingervein," *Biometric Technology Today,* 10. kötet, pp. 2, November-December 2011.

[47] RING T., „First biometric ATMs roll out in Poland," *Biometric Technology Today,* 6. kötet, pp. 5-12, June 2010.

[48] OTTI Cs. és MILÁK I., „The security and vulnerability of biometry," in *A MAGYAR TUDOMÁNY ÜNNEPE 2012 KONFERENCIA AZ ÓBUDAI EGYETEMEN: BIZTONSÁGTECHNIKAI SZEKCIÓ.*, Budapest, 2012.

[49] OTTI Cs., , *A biometria biztonsága és sérülékenysége.* . HACKTIVITY IT SECURITY FESTIVAL - HACKTIVITY KFT., 2012.

[50] OTTI Cs., *Ujjnyomat azonosító biztonsági beléptető rendszerek tesztelésének szükségessége és metodikája (Diplomamunka),* Budapest: Óbudai Egyetem, 2014.

[51] BUNYITAI Á., „A ma és a holnap beléptető rendszereinek automatikus személyazonosító eljárásai biztonságtechnikai szempontból," *Hadmérnök,* 1. kötet, pp. 22-35, 2011.

[52] OTTI Cs., „Classification of biometric access control systems based on real-time throughput," in *Proceedings of Fifth International Scientific Videoconference of Scientists and PhD. students or candidates*, Bratislava, 2015.

[53] OTTI Cs., „Térfigyelő rendszerek arcfelismerési lehetőségeinek gyakorlati problémái," in *Tanulmányok a "Biztonsági kockázatok - rendészeti válaszok" című tudományos konferenciáról*, Pécs, Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, 2014, pp. 67-75.

[54] TURK M. és PETLAND A., „Eigenfaces for Recognition," *Journal of Cognitive Neuroscience,* kötet 3, 1. szám, pp. 71-86, 1991.

[55] *Állásfoglalás a biometrikus azonosítón alapuló, munkahelyi beléptető rendszerekről,* 2007.

[56] CAMPISI P., Security and Privacy in Biometrics, New York: Springer Publishing Company, 2013.

[57] SROKA W., CYGLER J. and GAJDZIK B., "The Transfer of Knowledge in Intra-Organizational Networks: A Case Study Analysis," *Organizacija,* pp. 24-34, 2014.

[58] *MSZ EN 50133-1:2006: Riasztórendszerek. Beléptetőrendszerek biztonságtechnikai alkalmazásokhoz. 1. rész: Rendszerkövetelmények*

[59] *54/2014. (XII. 5.) BM rendelet az Országos Tűzvédelmi Szabályzatról,* 2014.

[60] *MSZ EN 60839-11-2:2015. Riasztórendszerek és elektronikus biztonsági rendszerek. 11-2. rész: Elektronikus beléptető rendszerek. Alkalmazási irányelvek*

[61] POKORÁDI L., Rendszerek és folyamatok modellezése, Debrecen: Campus, 2008.

[62] BUNYITAI Á., „A beléptető rendszerek helye és szerepe a vagyonvédelemben," *Hadmérnök,* VI. kötet, 4. szám , pp. 17-25, 2011.

[63] OTTI Cs. és ŐSZI A., „Sérülékenységi vizsgálatok az arcazonosítás terén," *Detektor plusz szakmai szakfolyóirat,* pp. 10-11, 2013.

[64] MASHAGBA E., „Human Identification Based on Geometric Feature," *Computer and Information Science,* 9. kötet, 2. szám, pp. 140-155, 2016.

[65] KUMAR A., DAVID W. C., HELEN S. C. és ANIL J. K., „Personal verification using palmprint and hand geometry biometric," *Proceedings of Fourth International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA),* pp. 668-675, 2003.

[66] STYLIOS I., THANOU O., ANDROULIDAKIS I. és ZAITSEVA E., „A Review of Continuous Authentication Using Behavioral Biometrics," in *ACM 2016*, Kastoria, Greece, 2016.

[67] HANKA L., „A BINOMIÁLIS ELOSZLÁS ALKALMAZÁSI LEHETOSÉGEI UJJNYOMAT AZONOSÍTÓ RENDSZEREK VIZSGÁLATÁBAN, A MAXIMUM LIKELIHOOD ELV ALKALMAZÁSA," in *TAVASZI BIZTONSÁGTECHNIKAI SZIMPÓZIUM 2013, ÓBUDAI EGYETEM*, Budapest, 2013.

[68] HANKA L. és WERNER G., „Using the Beta-Binomial Distribution for the Analysis of Biometric Identification," in *SISY 2015 : IEEE 13th nternational Symposium on Intelligent Systems and Informatics: Proceedings*, Subotica, Szerbia, International Symposium on Intelligent Systems and Informatics, 2015, pp. 209-216.

[69] KLEINROCK L., Queueing Systems Volume 1: Theory, New Yor: Wiley - Interscience, 1975.

[70] LOVÁSZ L., Algoritmusok Bonyolultsága, Budapest: ELTE, Matematikai Intézet, 2009.

[71] SZEIDL L., Tömegkiszolgálás, Budapest: Óbudai Egyetem, Neumann János Informatikai Kar, 2009.

[72] PAP G. és SZŰCS G., Sztochasztikus folyamatok, Szeged: Szegedi Tudományegyetem, Bolyai Intézet, Sztochasztika Tanszék, 2014.

[73] KENDALL D. G., „Stochastic processes occurring in the theory of queues and their analysis by the method of imbedded Markov chain," *Annals of Mathematical Statistics,* pp. 338-354, 1953.

[74] SZTRIK J., A sorbanállási elmélet alapjai, Debrecen: Debreceni egyetem, Informatikai Kar, 2011.

[75] LAW A. M., Simulation Modeling and Analysis. 5th edition., Tucson, Arizona, USA: McGrow-Hill , 2015.

[76] FISHWICK P. A. és PARK H., „Queue Modeling and Simulation," in *Principles of Modeling and Simulation: A Multidisciplinary Approach*, Canada, John Wiley & Sons, Inc, 2008, pp. 71-90.

[77] LUKÁCS J., *Beléptető kapu elhelyezési stratégia fejlesztése és bemutatása néhány kiválasztott metróállomáson keresztül,* Budapest: Budapesti Műszaki és Gazdaságtudományi Egyetem, 2014.

[78] LITTLE J. D. C., „A proof of the queuing formula: l = λw," *Operations research,* pp. 383-387., 1961.

[79] SENNEWALD C. A. és BAILLIE C., Effective Security Management, Elsevier: Butterworth-Heinemann, 2015.

[80] OTTI Cs., „Belépési pontok meghatározása markovi modellel, nagy létszámú üzemek biometrikus beléptetésénél," *Hadmérnök,* kötet 12, szám 2, pp. 22-33., 2017.

[81] HILLIER F. S. és LIEBERMAN G. J., INTRODUCTION TO OPERATIONS RESEARCH, USA: McGraw-Hill Higher Education, 2014.

[82] OTTI, Cs., HANKA, L.: Analysis of access points with the queue model, *Revista Academiei Fortelor Terestre / Land Forces Academy Review 94 (2),* pp. 164-174., 2019.

[83] OTTI Cs., „Why does it fail to operate?," in *Thinking Together: The economy in practice*, Budapest, Óbudai Egyetem, 2017., pp. 45-66.

[84] SOOMRO Z. A., SHAH M. H. és AHMED J., „Information security management needs more holistic approach: A," *International Journal of Information Management,* pp. 215-225, 2016.

[85] PELTIER T. R., Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management, Washington: CRC Press LLC , 2016.

[86] BARABÁSI A. L., A hálózatok tudománya, Budapest: Libri, 2016.

[87] SAFA S. N. és VON SOLMS R., „An information security knowledge sharing model in organizations," *Computers in Human Behavior,* pp. 442-451, 2016.

[88] FÖLDESI K. és KOVÁCS T., „Biometriával kapcsolatos averziók vizsgálata hivatásos rendőrök és egyetemisták körében," in *Óbudai Egyetem Biztonságtudományi Doktori Iskola*, Budapest, 2014.

[89] *NAIH észrevételek az automatikus arcképelemző rendszerről,* 2015.

[90] VICSEK L., Fókuszcsoport, Budapest: Osiris, 2006.

[91] *ISO/IEC 19795-6:2012(E). Information technology — Biometric performance testing and reporting — Part 6: Testing methodologies for operational evaluation.*

[92] *EU 2016/679 RENDELETE a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet - GDPR),* 2016.

[93] S. B. Kalyani Mali, „Comparative Study of Different Biometric Features," *International Journal of Advanced Research in Computer and Communication Engineering,* kötet 2, szám 7, pp. 2776-2784, 2013.

[94] International Organization for Standardization, *ISO/IEC 19795-1 Information technology — Biometric performance testing and reporting — Part 1: Principles and framework.*

[95] KRISTÓF T., „Többváltozós statisztikai szeparáció - módszertani áttekintés," *Statisztikai Szemle,* 9. kötet, pp. 841-863, 2005.

[96] FAWCETT T., „HP Laboratories Palo Alto," 7. Január 2003. [Online]. Elérhető: http://www.hpl.hp.com/techreports/2003/HPL-2003-4.pdf. [Hozzáférés dátuma: 1. április 2018.].

[97] ŐSZI A., „Az e-kereskedelem elvárásai a biometriával szemben," in *Vállalkozásfejlesztés a XXI. században IV.*, Óbuda University, Keleti Faculty of Business and Management, 2014, pp. 427-440.

[98] MICHELBERGER P. és HORVÁTH Z., „Security aspects of process resource planning," *Polish Journal of Management Studie,* pp. 142-153, 2017.

[99] SZIKORA P., *Párosítás elméleti problémák megoldási lehetőségei egyetemi környezetben. Doktori (PhD) értekezés,* Budapest: Óbudai Egyetem, Biztonságtudományi Doktori Iskola, 2016.

[100] OTTI Cs., „Biztonságtechnikai eszközök vizsgálata és minősítési módszertana," in *Tavaszi Biztonságtechnikai Szimpózium*, Budapest, 2012.

[101] HANKA L., „A Doddington-féle 30-as szabály, biometrikus rendszerek megbízhatóságának statisztikai elemzése," in *Tavaszi Biztonságtechnikai Szimpózium 2013, Óbudai Egyetem*, Budapest, 2013.

[102] FIALKA G. és KOVÁCS T., „THE CORRELATION AMONG TECHNICAL PARAMETERS, CONDITIONS OF APPLICATION AND BIOMETRICAL IDENTIFICATION," *Hadmérnök,* XI. kötet, 2. szám, pp. 5-13, 2016.

[103] OTTI Cs. és KOLNHOFER-DERECSKEI A., „Introduction to the biometric access control systems for managers: which error indicator matters in the selection?," *POLISH JOURNAL OF MANAGEMENT STUDIES,* 17. kötet , 2. szám, pp. 197-210, 2018.

[104] SAJTOS L. és MITEV A., SPSS Kutatási és adatelemzési kézikönyv, Budapest: Aliena kiadó, 2007.

[105] LYUBOMIRSKY S., KING L. és DIENER E., „The Benefits of Frequent Positive Affect: Does Happines Leads to Success?," *Psychological Bulletin,* 131 kötet, 6. szám, pp. 803-855, 2005.

[106] OTTI Cs. és RÁCZ E., „Hogyan érezzük magunkat a munkahelyen?," in *Vállalkozásfejlesztés a XXI. században*, Budapest, Óbudai Egyetem, 2017, pp. 453-463.

[107] NAGY A. Z., „A KIBER-HÁBORÚ ÚJ DIMENZIÓ – A VESZÉLYEZTETETT ÁLLAMBIZTONSÁG," in *Magyar Hadtudományi Társaság*, Pécs, 2012.

[108] Cavusoglu H., SON J. Y. és BENBASAT I., „Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources," *Information & Management,* pp. 385-400, 2015.

[109] OTTI Cs. és KOLNHOFER-DERECSKEI A., „Az emberek elfogadási küszöbe a biometrikus rendszerek megbízhatóságával szemben," *Szakmai Szemle,* XVI. kötet, 3. szám, pp. 133-147, 2018..

[110] *A 29. cikk szerinti adatvédelmi munkacsoport 3/2012. sz. vélemény a biometrikus technológiák terén történt fejleményekről,* 2012..

[111] SZÁNTÓ Z., „A társadalmi kapcsolatháló-elemzés szociometriai gyökerei," in *A társadalmi kapcsolatháló-elemzés*, Budapest, BCE Szociológia és Társadalompolitika Intézet, 2011, pp. 649-662.

[112] OTTI Cs. és VALOCIKOVÁ C., „A biztonsági rendszerek felhasználói attitűdje, értékelése és befolyásolásának lehetőségei," *Hadmérnök,* 14. kötet, pp. 31-40, 2019.

[113] OTTI Cs., PITLIK L., PITLIK M., PITLIK M. és PITLIK L. I., „Attitiűd-kockázatfeltáró robot," *Magyar Internetes Agrárinformatikai Újság,* 21. kötet, 244. szám, pp. 1-13, 2019.

[114] OTTI Cs. és PITLIK L., „Ergonómia és hasonlóságelemzés a biometrikus rendszerek felhasználóinak tükrében," *Bánki Közlemények,* %1. kötetII., 2019..

[115] TRAURING M., „Automatic Comparison of Finger-Ridge Patterns," *Nature,* 197. kötet, pp. 938-940, 1963.

[116] OTTI Cs., ŐSZI A. és NAGY A. L., *iEvo ujjnyomat olvasó gyorstesztje,* Budapest, 2012..

[117] OTTI Cs. és ŐSZI A., „Fingerprint security," in *IESB 2011 - International Engineering Symposium at Bánki - Bánki Kari Tudományos Konferencia*, Budapest, 2011.

[118] OTTI Cs., A. Fehér és A. Őszi, *Face recognition systems,* 2013..

[119] OTTI Cs., „A felhasználók véleménye, amikor egy beléptető rendszer nem működik megfelelően," in *XX. Tavaszi Biztonságtechnikai Szimpózium*, Budapest, 2017.

[120] NAZARETH D. L. és CHOI J., „A system dynamics model for information security management," *Information & Management,* pp. 123-134, 2015.

PUBLIKÁCIÓS LISTA

Tézisekhez kapcsolódó publikációk

I. KOVÁCS T.; OTTI Cs.; MILÁK I.: A biztonságtudomány biometriai aspektusai, in *A biztonság rendészettudományi dimenziói: Változások és hatások,* Pécs, Magyar Rendészettudományi Társaság, pp. 485–496., 2012.

II. OTTI, Cs.; MILÁK, I.: The security and vulnerability of biometry, in *A Magyar Tudomány Ünnepe 2012 Konferencia az Óbudai Egyetemen: Biztonságtechnikai szekció*, Budapest, 2012.

III. OTTI Cs.: Térfigyelő rendszerek arcfelismerési lehetőségeinek gyakorlati problémái, in *Tanulmányok a "Biztonsági kockázatok - rendészeti válaszok" című tudományos konferenciáról*, Pécs, pp. 67–75., 2014.

IV. OTTI Cs.: Biometrikus rendszerek felhasználói minta pozicionálásának kérdései, in *DOSZ, Tavaszi Szél 2016*, Budapest, 2016.

V. OTTI, Cs.: Comparison of biometric identification methods, in *2016 IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, Timisoara, 2016.

VI. OTTI, Cs.: The Past, Present and Future of Biometrics, in *Sixth International Scientific Videoconference of Scientists and PhD. students or candidates*, Obuda University and University of Economics in Bratislava, 2016.

VII. OTTI Cs.: Classification of biometric access control systems based on real-time throughput, in *Proceedings of Fifth International Scientific Videoconference of Scientists and PhD. students or candidates*, Bratislava, 2015.

VIII. OTTI Cs.: Belépési pontok meghatározása markovi modellel, nagy létszámú üzemek biometrikus beléptetésénél, *Hadmérnök,* 12. évf. 2. szám, pp. 22–33., 2017.

IX. OTTI, Cs.: Why does it fail to operate?, in *Thinking Together: The economy in practice,* Budapest, Óbudai Egyetem, pp. 45–66., 2017.

X. OTTI Cs.; RÁCZ E.: Hogyan érezzük magunkat a munkahelyen?, in *Vállalkozásfejlesztés a XXI. században,* Budapest, Óbudai Egyetem, pp. 453–463., 2017.

XI. OTTI Cs.: A felhasználók véleménye, amikor egy beléptető rendszer nem működik megfelelően, in *XX. Tavaszi Biztonságtechnikai Szimpózium,* Budapest, 2017.

XII. OTTI, Cs.; KOLNHOFER-DERECSKEI, A.: Introduction to the biometric access control systems for managers: which error indicator matters in the selection?, *Polish Journal Of Management Studies,* Vol. 17, No. 2, pp. 197–210., 2018.

XIII. OTTI Cs., KOLNHOFER-DERECSKEI, A.: Az emberek elfogadási küszöbe a biometrikus rendszerek megbízhatóságával szemben, *Szakmai Szemle,* 16. évf. 3. szám, pp. 133–147., 2018.

XIV. OTTI, Cs., HANKA, L.: Analysis of access points with the queue model, *Revista Academiei Fortelor Terestre / Land Forces Academy Review 94 (2),* pp. 164-174., 2019.

További publikációk

XV. OTTI Cs.: Integrált munkaidő nyilvántartó rendszerek a gyakorlatban, in *Gépész, Mechatronikai és Biztonságtechnikai Szimpózium*, Budapest, Budapesti Műszaki Főiskola Bánki Donát Gépész- és Biztonságtechnikai Mérnöki Kar, 2009.

XVI. OTTI Cs.: Termelő cégeknél használt kézgeometria azonosítóval megvalósított munkaidő elszámoló rendszerek gyakorlati tapasztalatai és megtérülés-számítása, in *Óbudai Egyetem, Nemzetközi Gépész, Mechatronikai és Biztonságtechnikai Szimpózium,* Budapest, 2011.

XVII. OTTI Cs.; ŐSZI A.: Fingerprint security, in *IESB 2011 – International Engineering Symposium at Bánki – Bánki Kari Tudományos Konferencia*, Budapest, 2011.

XVIII. OTTI Cs.; FEHÉR A.; ŐSZI A.; MILÁK I.: *A biometria biztonsága és sérülékenysége,* Hacktivity, 2012.

XIX. OTTI Cs.: Biztonságtechnikai eszközök vizsgálata és minősítési módszertana, in *Tavaszi Biztonságtechnikai Szimpózium*, Budapest, 2012.

XX. OTTI Cs.; FEHÉR A.; ŐSZI A.: *Face recognition systems,* 2013.

XXI. OTTI Cs.; ŐSZI A.; NAGY A. L.: *iEvo ujjnyomat olvasó gyorstesztje,* Budapest, 2012.

XXII. OTTI Cs.; RÓNASZÉKI P.: *Információbiztonság: az ISO 27001 információbiztonsági irányítási rendszer 1. rész*, Budapest, 2013.

XXIII. OTTI Cs.; RÓNASZÉKI P.: *Információbiztonság: az ISO 27001 információbiztonsági irányítási rendszer 2 rész,* Budapest, 2013.

XXIV. OTTI Cs.; ŐSZI A.: *Sérülékenységi vizsgálatok az arcazonosítás terén,* Budapest, 2013.

XXV. OTTI Cs.; VALOCIKOVÁ C.: A biztonsági rendszere felhasználói attitűdje, értékelése és befolyásolásának lehetőségei, *Hadmérnök,* 2019.

XXVI. OTTI Cs.; PITLIK L.; PITLIK M.; PITLIK M.; PITLIK L.: Attitiűd-kockázatfeltáró robot, *Alkalmazott Informatikai Újság,* 244. szám, 2019.

XXVII. OTTI Cs.; PITLIK L.: Ergonómia és hasonlóságelemzés a biometrikus rendszerek felhasználóinak tükrében, *Bánki Közlemények,* 2. évf., 2019.

RÖVIDÍTÉSJEGYZÉK

ABI	Applied Biometrics Institute – Alkalmazott Biometria Intézet; www.abibiometrics.org; az Óbudai Egyetem, Bánki Donát Gépész- és Biztonságtechnikai Mérnöki Karon belül 2011-ben létrejött szakmai csoport.
AFIS	Automated Fingerprint Identification System – Automatikus ujjnyomat-felismerő rendszer. Biometrikus személyazonosító rendszer, amely digitális képalkotó technikával begyűjti, tárolja és analizálja az ujjlenyomatokat. Eredetileg az FBI számára fejlesztették ki.
APAS	Access Point Actuators and Sensors – Beléptetőpont átengedő szerkezetei és érzékelői. Az átengedő szerkezetekre példák az elektromos ajtónyitók, elektromos zárak, forgóajtók és egyéb feltartóztató eszközök. Az érzékelőkre példák az érintkezők, kapcsolók, nyomás- és ajtónyitás érzékelők.
ART	Average Recognition Time – Átlagos azonosítási idő.
CCTV	Closed Circuit TeleVision – Zártláncú televízió.
DET	Detection Error Tradeoff – tipikusan FAR és FRR értékeket ábrázoló módosított ROC-grafikon, ahol a függvények paramétere az eszköz érzékenységi beállítása.
EER	Equal Error Rate – Egyesített hibaarány: az az arány, ahol a téves elfogadás (FAR) és a téves elutasítás (FRR) közel megegyezik egymással. Ez a pont a berendezés és algoritmus optimális beállítása, a két görbe itt metszi egymást, innen biztonságosabb vagy kényelmesebb irányba elmozdulni csak a másik rovására történhet. Kényelmesebb a rendszer, ha kevesebbszer utasítja el a jogosult felhasználókat tévesen, biztonságosabb, ha alacsonyabb a hibás elfogadási aránya.
FAR	False Acceptance Rate – Hibás elfogadási arány: a hibás vagy téves elfogadási arány annak a valószínűségét írja le, hogy a rendszer hibásan elfogad egy olyan személyt, aki nincs benne az adatbázisban vagy hibásan azonosít valaki mást az adatbázisból.
FIFO	First In First Out - A folyamatba vagy tárolóba először megérkező igénynek, eseménynek vagy terméknek először is kell elhagynia azt.
FNMR	False Non Match Rate – Hibás nem-egyezési ráta: Az FNMR jelenti azt a várható értéket, hogy két minta ugyanattól a személytől hibásan különbözőnek lett felismerve az algoritmus által.
FMR	False Match Rate – Téves megfeleltetés: Az FMR jelenti azt a várható értéket, hogy két különböző minta hibásan egyezőnek lett felismerve az algoritmus által.
FPR	False Positive Rate – Hibás pozitív arány
FRR	False Rejection Rate – Hibás elutasítási arány: megmutatja annak a valószínűségét, hogy egy rendszer elutasít egy érvényes mintát, amely benne van az adatbázisában. A téves elutasítási arány a téves elutasítások számának és az összes azonosítási kísérletnek a hányadosa. A gyakorlati tapasztalatok szerint ez a mutató az egyik legfontosabb, nagyban meghatározza a biometrikus rendszer használhatóságát. A létszám növekedésével értelemszerűen statisztikailag egyre nagyobb a valószínűsége, hogy a felhasználóknál problémát fog jelenteni a téves elutasítás.

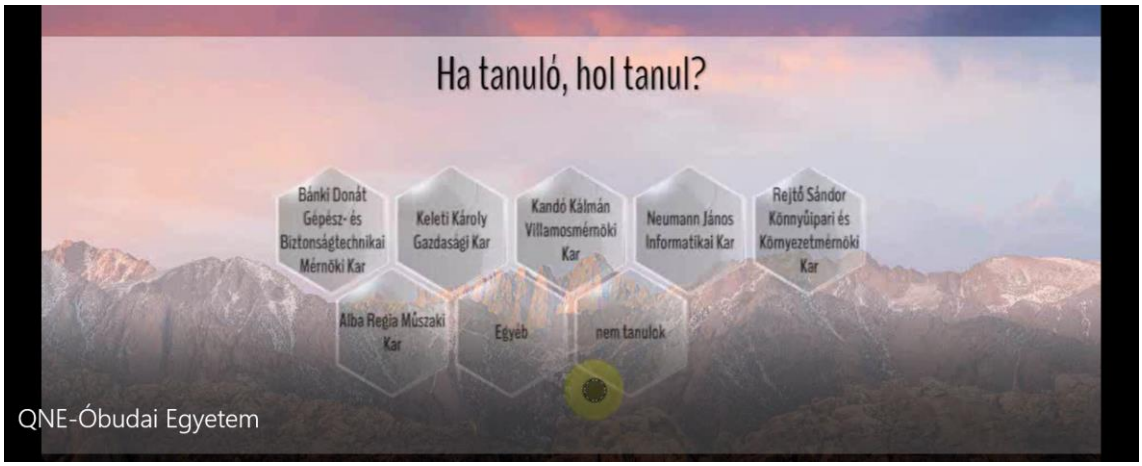
FTA	Failure To Acquire – Sikertelen mintabeviteli arány: A sikertelen mintabevitel azt jelenti, hogy az eszköz valamilyen okból képtelen levenni a mintát, és abból előállítani azt a kódot, amit összehasonlítana az adatbázisával. Az ebből képzett arány pedig az összes sikeres mintabevitelre vetíti a sikertelen eseteket.
FTE	Failure To Enroll – Sikertelen regisztrációs arány: Ez a mutató azt jelzi, hogy egy rendszerbe milyen valószínűséggel nem lehet beregisztrálni a felhasználókat.
GDPR	General Data Protection Regulation – EU rendelet a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról.
GFAR	Generalized False Accept Rate - Általánosított téves elfogadási arány
GFRR	Generalized False Reject Rate - Általánosított téves elutasítási arány
ICAO	International Civil Aviation Organization – Nemzetközi Polgári Repülési Szervezet
LIFO	Last In First Out - A folyamatba vagy tárolóba utoljára érkező igénynek, eseménynek vagy terméknek először kell elhagynia azt.
MOA	Mission Oriented Application - feladatorientált alkalmazás, mely, mint mutató arra vonatkozik, hogy az adott eszközt milyen biztonsági igényű feladatokra lehet alkalmazni.
PIN	Personal Identity Number – Személyi azonosító szám
ROC	Receiving Operating Characteristic – tipikusan a FAR és TPR függvényét ábrázoló grafikon
RFID	Radio Frequency Identification Device – Rádiófrekvenciás azonosító eszköz
TPR	True Positive Rate – Valós pozitív arány

TÁBLÁZATJEGYZÉK

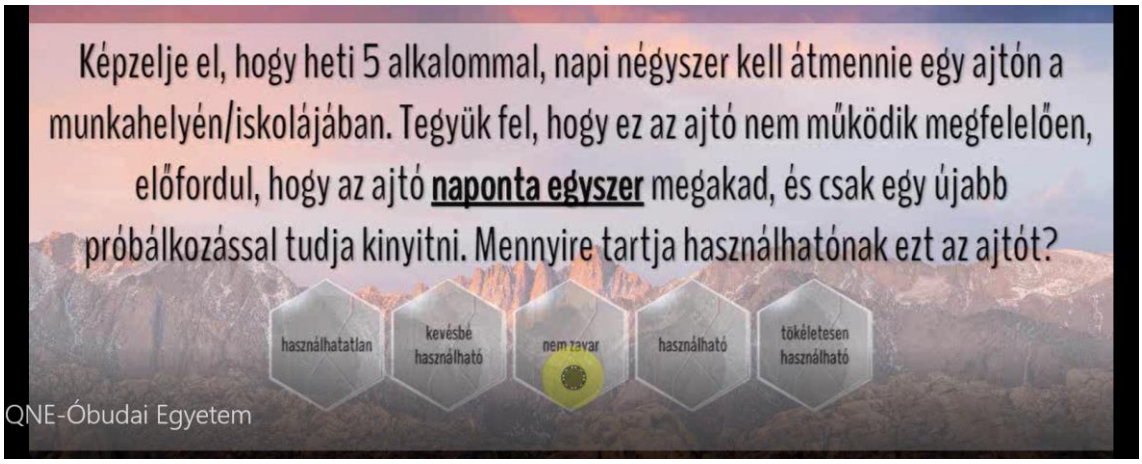
ÁBRAJEGYZÉK

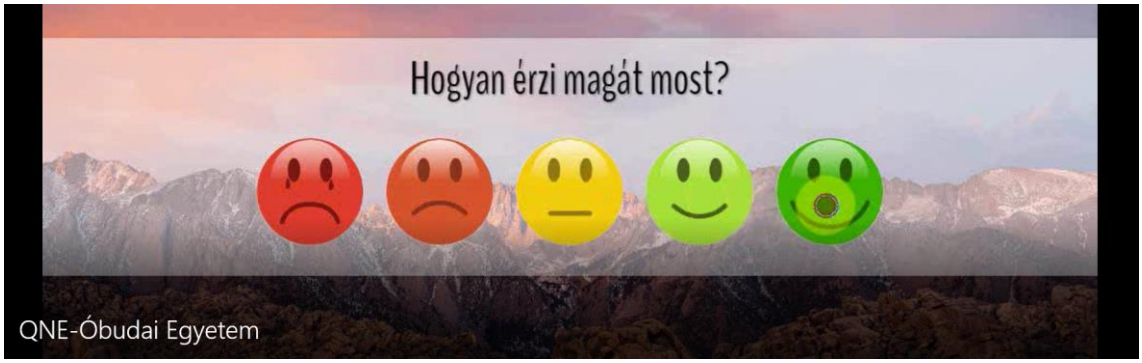
MELLÉKLETEK

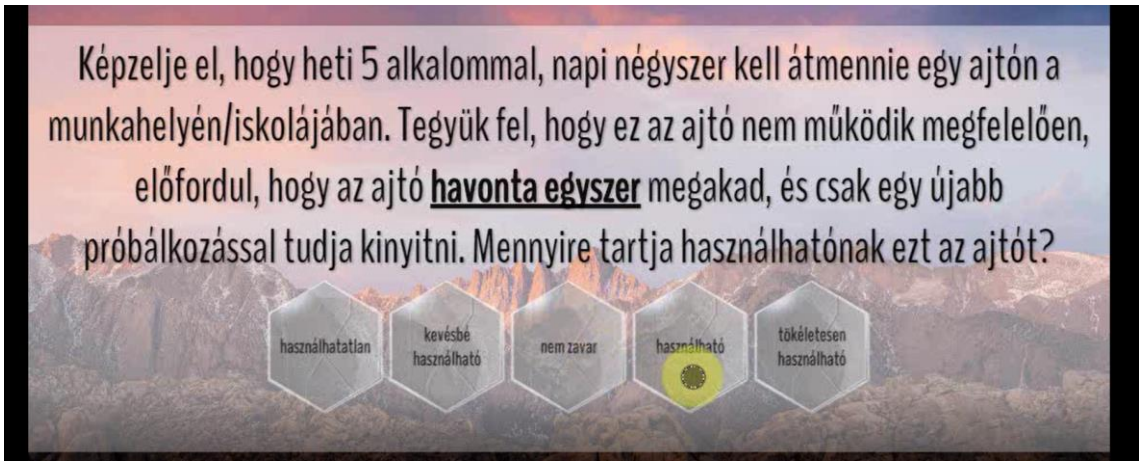
Kvantitatív kérdőív


Ha tanuló, hol tanul?
Bánki Donát Gépész- és Biztonságtechnikai Mérnöki Kar
Keleti Károly Gazdasági Kar
Kandó Kálmán Villamosmérnöki Kar
Neumann János Informatikai Kar
Rejtő Sándor Könnyűipari és Környezetmérnöki Kar
Alba Regia Műszaki Kar
Egyéb
nem tanulok
QNE-Óbudai Egyetem

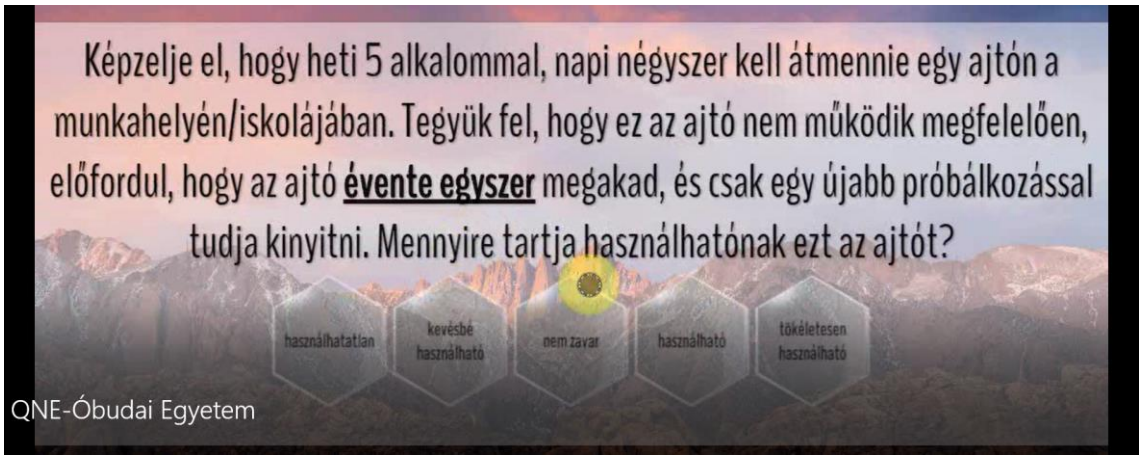

Ha dolgozó, milyen területen dolgozik?
adminisztráció, asszisztens, irodai munka
bank, biztosítás
cégvezetés, menedzsment
egészségügy
építőipar
gyártás, termelés
HR
IT
jog
kereskedelem
közigazgatás
marketing, média
mezőgazdaság
oktatás, kutatás
pénzügy, könyvelés
vendéglátás, idegenforgalom
nem dolgozom
QNE-Óbudai Egyetem


Képzelje el, hogy heti 5 alkalommal, napi négyszer kell átmennie egy ajtón a munkahelyén/iskolájában. Tegyük fel, hogy ez az ajtó nem működik megfelelően, előfordul, hogy az ajtó naponta egyszer megakad, és csak egy újabb próbálkozással tudja kinyitni. Mennyire tartja használhatónak ezt az ajtót?
használhatatlan
kevésbé használható
nem zavar
használható
tökéletesen használható
QNE-Óbudai Egyetem

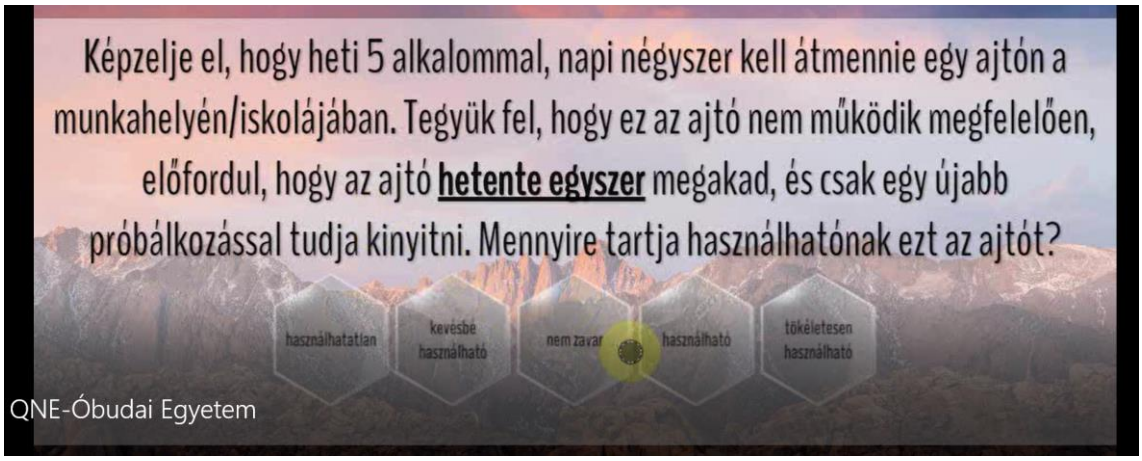

Hogyan érzi magát most?
QNE-Óbudai Egyetem


Képzelje el, hogy heti 5 alkalommal, napi négyszer kell átmennie egy ajtón a munkahelyén/iskolájában. Tegyük fel, hogy ez az ajtó nem működik megfelelően, előfordul, hogy az ajtó havonta egyszer megakad, és csak egy újabb próbálkozással tudja kinyitni. Mennyire tartja használhatónak ezt az ajtót?
használhatatlan
kevésbé használható
nem zavar
használható
tökéletesen használható

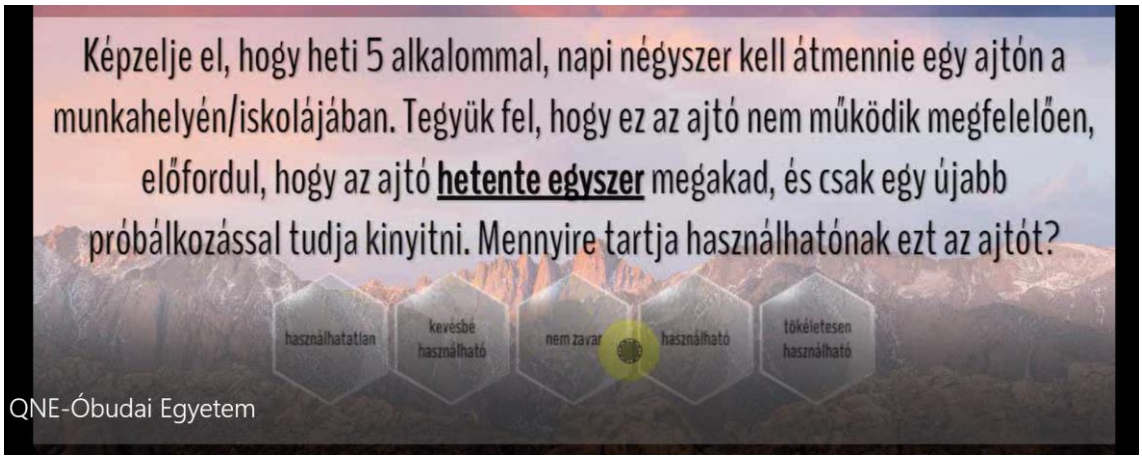

Mennyire elégedett a munkájához/tanulmányaihoz kapott információkkal?
QNE-Óbudai Egyetem

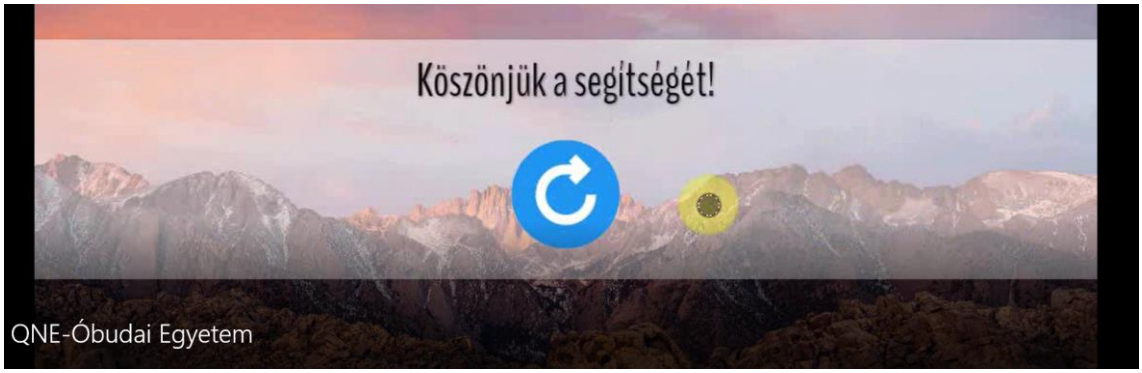

Képzelje el, hogy heti 5 alkalommal, napi négyszer kell átmennie egy ajtón a munkahelyén/iskolájában. Tegyük fel, hogy ez az ajtó nem működik megfelelően, előfordul, hogy az ajtó évente egyszer megakad, és csak egy újabb próbálkozással tudja kinyitni. Mennyire tartja használhatónak ezt az ajtót?
használhatatlan
kevésbé használható
nem zavar
használható
tökéletesen használható
QNE-Óbudai Egyetem


Mennyire ajánlaná másnak ezt a munkahelyet/iskolát?
QNE-Óbudai Egyetem


Képzelje el, hogy heti 5 alkalommal, napi négyszer kell átmennie egy ajtón a munkahelyén/iskolájában. Tegyük fel, hogy ez az ajtó nem működik megfelelően, előfordul, hogy az ajtó hetente egyszer megakad, és csak egy újabb próbálkozással tudja kinyitni. Mennyire tartja használhatónak ezt az ajtót?
használhatatlan
kevésbé használható
nem zavar
használható
tökéletesen használható
QNE-Óbudai Egyetem


Mi a legfőbb stresszforrás a munkahelyén?
munkahelyi követelmények
felettestől való támogatás hiánya
munka értelmetlensége
előreláthatóság hiánya
hatáskör/ kontroll hiánya
jutalmazási rendszer/ jutalmazás hiánya
QNE-Óbudai Egyetem


Képzelje el, hogy heti 5 alkalommal, napi négyszer kell átmennie egy ajtón a munkahelyén/iskolájában. Tegyük fel, hogy ez az ajtó nem működik megfelelően, előfordul, hogy az ajtó hetente egyszer megakad, és csak egy újabb próbálkozással tudja kinyitni. Mennyire tartja használhatónak ezt az ajtót?
használhatatlan
kevésbé használható
nem zavar
használható
tökéletesen használható
QNE-Óbudai Egyetem


Köszönjük a segítségét!
QNE-Óbudai Egyetem

Nyilatkozat a munka önállóságáról, irodalmi források megfelelő módon történt idézéséről

Alulírott Otti Csaba kijelentem, hogy a

„Biometriaalapú beléptető rendszerek alkalmazhatósága tömegtartózkodású helyeken”

című benyújtott doktori értekezést magam készítettem, és abban csak az irodalmi hivatkozások listáján megadott forrásokat használtam fel. Minden olyan részt, amelyet szó szerint, vagy azonos tartalomban, de átfogalmazva más forrásból átvettem, egyértelműen, a forrás megadásával megjelöltem.

Budapest, 2019. július 9.

……..

(aláírás)