Óbudai Egyetem

Doktori (PhD) értekezés tézisfüzete

Biometriaalapú beléptető rendszerek alkalmazhatósága tömegtartózkodású helyeken

Otti Csaba

Prof. Dr. Kovács Tibor, egyetemi docens

Biztonságtudományi Doktori Iskola

Budapest, 2019

Tartalomjegyzék

1 Summary

The subject of my research was the classification, scaling, and defining user attitudes of personal identification access control systems based on biometric data. With the help of Hungarian and international literature, as well as with professional interviews, I identified those critical areas of biometric access control systems, where the success of the implementation is not trivial, these are the access control and time and attendance systems of mass-staying buildings. I also outlined the aspects that decision-makers must take into account from a business-security perspective to manage successful biometric implementation projects.

I introduced a well adaptable procedure for setting up a stochastic model of an access control system with Markov chain, and I also described a new method for analyzing it. Based on the results I concluded that the developed analytical procedure is suitable for quality assurance in the planning phase of the implementation of biometric access control systems, and the support of business decisions.

The third thesis is the most important part of the dissertation, containing qualitative research based on my professional experience, the results of which I also used for quantitative research in this section. First, with a focus group, I surveyed people's knowledge and attitudes about access control systems. Then, through online questionnaire research, I have proved that the operational uncertainty given by the device manufacturers, is basically several orders of magnitude lower than people's acceptance threshold, so it can be ignored in the design process. All elements of the access control process must be taken into account, and only generate a maximum of 3-5% of false rejection, therefore it is still useable for that function.

2 A kutatás előzményei

Magyarországon az 1990-es évek végén kezdett a biztonsági szakma megismerkedni a biometrikus technológiákkal. 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 tervezett a magyar piacon elterjeszteni. 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 megoldásokkal, mint projekttámogató mérnök.

A kezdetben forgalmazott 5 gyártó mintegy 10 megoldása közül a gyakorlatban mindössze 2 működött – tudtuk, mert leteszteltük -, az egyik a Crossmatch által felvásárolt Digital Persona, Magyarországról nem

elérhető számitógépes beléptetést megvalósító ujjnyomat azonosítója, a másik a Recognition Systems kézgeometria felismerője volt.

A klasszikusan kiemelt biztonságúnak gondolt körülmények között (banki, IT, Telekom szektorok) nem volt komoly érdeklődés a biometrikus megoldásokra, azonban nagy létszámot foglalkoztató termelő vállalatok előszeretettel alkalmazták beléptetési és munkaidő nyilvántartási célokra.

Ezeken a tendereken rendszeres volt az a felállás, hogy az egyik ajánlatadó ujjnyomat olvasókkal indult, mi pedig a kézgeometria azonosítókkal. A tesztjeink alapján pontosan tudtuk, hogy tömegtartózkodású helyeken (pl. ipari, termelői környezetben) nem fog működni az ujjnyomat olvasó, de ez a döntéshozóknak nem volt nyilvánvaló. Adatlapok, szállító elmondása alapján, legjobb esetben is kis létszámú tesztek után döntöttek a bevezetésről. Ennek az lett az eredménye, hogy számos sikertelen rendszerbevezetés történt, ahol az üzleti döntéshozók csalódtak a biometriában, függetlenül attól, hogy csak a kiválasztott eszköz volt alkalmatlan az adott körülmények között.

A 2000-es évek elején kezdtem el együtt dolgozni és gondolkodni Prof. Dr. Kovács Tiborral, jelenlegi témavezetőmmel, hogyan lehetne a biometrikus rendszerek káoszában rendet vágni és megfelelő, hiteles tájékoztatást adni a biztonsági szakembereknek, hogy melyik technológia és eszköz mire alkalmazható a gyakorlatban. Ennek eredményeképpen jött létre 2011-ben az Óbudai Egyetem kereteiben az Applied Biometrics Institute, röviden ABI, amely felvállalta ezt a tevékenységet.

A közel 20 éves tapasztalat és 8 éves tudományos kutatás során sikerült létrehozni egy olyan metodikát, ami egyértelműen eldönthetővé teszi egy biometrikus rendszerről, hogy sikerrel bevezethető-e az adott alkalmazásban, figyelembe véve a biztonsági, üzleti igényeket, valamint az ott dolgozó, szolgálatot tevő emberek hozzáállását.

3 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 hiteles személyazonosítás egyre nagyobb jelentőséggel bír, azonban az alkalmazhatósági aspektusok területe kevéssé kidolgozott, sem a megrendelők, sem a biztonsági szakemberek számára nem áll rendelkezésre olyan, a gyakorlatban is hasznosítható eszköztár, melynek felhasználásával mérhető és előre jelezhető módon értékelhető 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 rengeteg teszt eredménye

alapján kívánom elérni. A biztonsági rendszerek egyik elsődleges tulajdonsága, hogy milyen mértékben képes kizárni 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 használni.**

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

Stratégiai célként határoztam meg feltérképezni a tömegtartózkodású munkahelyek biztonsági beléptetésének sajátosságait, valamint feltárni az ott dolgozók biometrikus beléptetéshez kapcsolódó szubjektív tényezőit.

Kihangsúlyozott figyelmet fordítottam és pontos, matematikai leírását adtam meg az egyik legnagyobb problémára, a dolgozók és felhasználók sorbanállására 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 hipotéziseket.

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.**

4 Vizsgálati 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.

5 Új tudományos eredmények

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.*

6 Az eredmények hasznosítási lehetősége

20 éve foglalkozom biometrikus beléptetőrendszerekkel és azzal a problémával, hogyan lehet egy üzleti, biztonsági döntéshozót a tender előtt vagy a tender során döntési helyzetbe hozni. A biometrikus gyártók által az adatlapra leírt tulajdonságai az eszközöknek – elsősorban a téves elutasítási arány – egy teljesen felesleges információ, ami a valós működésre még csak indikációt sem ad. A kutatásaim során elkészült

elemzések, amelyeket jelen dolgozatomban a 3 tézisben fogalmaztam meg választ ad, hogy mely alkalmazásoknál és milyen típusú elemzéseket elvégezni ahhoz, hogy a kivitelezés előtt el lehessen dönteni, hogy az adott rendszer alkalmas-e a célt kielégíteni.

A felhasználók attitűdjének kutatásával és elfogadási intervalluma létezésének bebizonyításával egzakt módszert adok bármely tömegtartózkodású hely biometrikus beléptetésének az ott megjelenő felhasználók elfogadási szintjének megfelelő rendszert választani.

További kutatásaimban tervezem szociometriai modellekkel a felhasználók között azonosítani a véleményvezéreket, ezután pedig a teljes populáció befolyásolására keresek módszereket, amellyel a bevezetés és betanulási idők lerövidíthetők, az attitűd és felhasználói hozzáállás pedig javítható.

7 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 azonositó 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.

8 Publikációk

8.1 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.

8.2 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.