Sisekaitseakadeemia

Politsei- ja piirivalvekolledž

Veronika Kiprejeva

BIOMEETRIA JA BIOMEETRILISED REISIDOKUMENDID

Lõputöö

Juhendaja:

Piret Teppan, MA

Muraste 2012

ANNOTATSIOON

SISEKAITSEAKADEEMIA

Kolledž: Politsei- ja Piirivalvekolledž	Kuu ja aasta: juuni 2012
Töö pealkiri eesti keeles: Biomeetria ja biomeetrilised reisidokumendid Töö pealkiri võõrkeeles: Биометрия и биометрические проездные документы	
Töö autor: Veronika Kiprejeva	Olen nõus oma lõputöö kättesaadavaks tegemisega elektroonilises keskkonnas. Allkiri:

Lühikokkuvõte: Töö on 37 lehel lisadeta, eesti keeles.

Biomeetriliste meetodite rakendamine aitab muuta riigi kaitse turvalisemaks, ja vähendada kuritegevuse arvu. Käesoleva lõputöö eesmärgiks oli uurida biomeetriliste reisidokumentide turvalisust.

Eesmärgi saavutamiseks viidi läbi ekspertintervjuud Tallinna, Narva, Koidula ja Luhamaa piiripunktides II astme kontrolli spetsialistide seas, analüüsiti ja võrreldi intervjuude tulemusi ja tehti järeldusi ja ettepanekuid biomeetria kasutamise kohta reisidokumentides. Intervjuu käigus saadi ülevaade biomeetria kasutamisest reisidokumentides ja sellega seotud positiivsed ja negatiivsed küljed. Antud lõputöö empiirilise osa tulemused näitasid, et biomeetriliste tehnoloogiate kasutamine kõikides reisidokumentides on efektiivne võimalus muuta EL liikmesriigid ja s.h. Eesti turvalisemaks ning vähenda illegaalide sisserändajate arvu.

Edaspidise perspektiivi mõttes, antud töö jätkamiseks pakub autor välja uurida täpsemate skaneerimise ja identifitseerimise süsteemide arengut, et võimalikult minimaliseerida isikute tuvastamise eksimuste protsenti.

Võtmesõnad: biomeetria, reisidokumendid, turvalisus, tuvastamine, identifitseerimine
Võõrkeelsed võtmesõnad: биометрия, проездные документы, безопасность, опознавание, идентификация
Säilitamise koht:
Kaitsmisele lubatud Kolledži direktor: Allkiri:
Vastab lõputöö nõuetele Juhendaja: Allkiri:

SISUKORD

MÕISTETE JA LÜHENDITE LOETELU

Välismaalane – isik, kes ei oma Eesti Vabariigi kodakondsust (Välismaalase seadus, 09.12.2009).

Illegaal – seadusliku aluseta riigis viibiv välismaalane (Välismaalase seadus, 09.12.2009).

E-pass – masinaga loetav pass, mis sisaldab kontaktivaba kiipi (Machine Readable Travel Documents 2006:5).

Dokumendiekspert – politseiametniku ametikoht, kes teostab piiripunktis II astme kontrolli (Ida prefektuuri piirivalvebüroo teenistujate ametijuhendite kinnitamine, prefekti 17.12.2010 käskkiri nr 102 Lisa 54).

AFIS – Automated Fingerprint Identification System, automaatne sõrmejälgede identifitseerimise süsteem.

IAFIS – Automated Fingerprint Identification System, integreeritud automaatne sõrmejälgede identifitseerimise süsteem.

FBI – Federal Bureau of Investigation, föderaalne juurdlusbüroo.

IKS – Isikuandmete kaitse seadus.

VMS – Välismaalaste seadus.

ABC süsteem – Automated Border Control system, automaatne piirikontrolli süsteem.

DNA – Deoxyribonucleic acid, desoksüribonukleiinhape.

ICAO – International Civil Aviation Organization, Rahvusvaheline Tsivillennunduse organisatsioon.

SISSEJUHATUS

Biomeetria, mis koosneb kreekakeelsetest sõnadest *„bios“* elu ja *„metron“* mõõtmine, on pakkunud teadlastele huvi mitmete aastasadade jooksul. Biomeetriliste uuringute tagamaad on olnud erinevatel aegadel erinevad – inimeste kujutamine kunstis, agressiivsuse-, kuritegevuse- ja terrorismi suurenenud kasv jne. Tõuke põhjalikemateks biomeetria uuringuteks andis aga 11. september 2001 aasta, kui toimus terroriakt Ameerika Ühendriikides Maailma Kaubenduskeskuse ja Pentagoni vastu. Sellest ajast alates on hoogustunud biomeetriliste andmete kasutamise võimaluste uurimine kogu maailmas, mille tulemusena oleks võimalik saavutada kontroll inimeste üle ning vähendada kuritegevust. Biomeetriliste andmete kasutamise vajadust tingis ka võltsitud dokumentide ja illegaalide arvu suurenemine, kes püüdsid eelkõige kasutada võõrast identiteeti.

Samuti nõuab biomeetriliste passide väljastamist Euroopa Nõukogu määrus, kus on välja toodud, et Euroopa Liidu (edaspidi EL) liikmesriigid peavad oma reisidokumendid muutma biomeetrilisteks dokumentideks kasutades selleks näo ja sõrmejälgede biomeetriat. (Nõukogu määrusega 13.12.2004)

Töö on aktuaalne kuna biomeetria areneb äärmiselt kiiresti ning järjest rohkem hakatakse kasutama biomeetrilisi dokumente ning selleteemalisi uuringuid ei ole autori teada viimasel ajal Sisekaitseakadeemias läbi viidud.

Käesoleva lõputöö eesmärgiks ongi uurida biomeetriliste reisidokumentide turvalisust.

Lõputöös on püstitatud järgmised uurimisküsimused:

1. Kas biomeetriliste tehnoloogiate kasutamine reisidokumentides on efektiivne meetod teha dokumendid turvalisemaks?
2. Kas biomeetria kasutamine reisidokumentides väheneb dokumentide võltsimist?

Eesmärgi saavutamiseks on püstitatud järgmised uurimisülesanded:

1. Anda ülevaade biomeetriast ning biomeetrilistest dokumentidest;
2. Koostada küsimused ja läbi viia ja analüüsida ekspertintervjuud Tallinna, Narva, Koidula ja Luhamaa piiripunktides II astme kontrolli spetsialistide seas;
3. Teha järeldusi ja ettepanekuid biomeetria kasutamise kohta reisidokumentides;

Töö koosneb kahest osast, millest esimeses annab autor ülevaate biomeetriast ja kirjeldab erinevaid biomeetrilisi metodoloogiaid. Teises osas autor selgitab, kuidas ja kus kasutatakse biomeetrilisi andmeid ning kirjeldab biomeetrilisi reisidokumente ja selliste dokumentide omanike võimalustest. Samuti teises osas analüüsitakse läbiviidud intervjuude tulemusi ja saadakse ülevaade biomeetria kasust riigi turvalisusele, mille põhjal autor teeb järeldusi ning ettepanekuid.

1. BIOMEETRIA JA BIOMEETRILISTE ANDMETE KASUTAMISE MEETODID

Biomeetria on tekkinud mitmeid aastatuhandeid tagasi, vanas Egiptuses, kus elanikud identifitseerisid isikuid läbi füüsiliste omaduste, näo kujutiste, naha värvi ja teiste tunnuste järgi, nagu näiteks armid. Biomeetria teaduslikud alused tekkisid aga üheksateistkümnenda sajandi lõpus, mis oli Francis Galtoni ja Karl Pearsoni töö tulemuseks. (Ashbourn 2000:1-4; Прохоров 1978)

Alles eelmise sajandi üheksakümnendate aastate keskel hakati biomeetriat uurima kui inimeste identifitseerimise vahendit. (Lion 2005-2006)

Biomeetriat on lahti mõtestatud erinevate definitsioonide abil, kuid kõige paremini iseloomustab biomeetriat järgmine selgitus:
biomeetria on matemaatilise statistika ja tõenäosusteooria meetodite rakendamine bioloogias. Seega väljendab biomeetria füsioloogilisi eriomadusi konkreetsete tunnuste alusel. Need on sõrmejäljed, käe ja näo geomeetria, silmaiiris, hääl. Biomeetria andmed on ka andmed, mis sisaldavad biomeetria näidist ükskõik millisest mehhanismist. Näiteks sõrmejäljed või häälesalvestus. Biomeetria süsteem võimaldab tuvastada isikuid nende anatoomia ja käitumise tunnuste järgi. Kogu biomeetriline identifitseerimise süsteem on protsess, mis loeb inimese füüsilisi andmeid, võrdleb neid andmeid biomeetrilise informatsiooniga, mis on saadud läbi skaneerimise ja identifitseerib tema isiksuse. (Лакин 1990:8; Naan 1985; Ashbourn 2000:12; Li, Jain 2009)

Eelpool väljatoodu põhjal saab öelda, et biomeetria tõestab iga isiku ainulaadsust. Iga inimese füsioloogilised ja käitumisomadused on kordumatud ja kuuluvad vaid ühele isikule. Biomeetriline tunnus on tavaliselt püsiv – reeglina inimese sünnist kuni tema surmani koosolev parameeter. Selline omadus vähendab märgatavalt

selle väärkasutamise võimalust. (Jain, Bolle, Pankanti 2006:4)

Vastavalt Isikuandmete kaitse seaduse (edaspidi IKS) § 4 loetakse biomeetrilised andmed isiku delikaatseteks andmeteks (Isikuandmete kaitse seadus, 15.02.2007).

Biomeetria tehnoloogia kasutamine on tekkitanud tihti diskussioone, et see võib rikkuda isiku konfidentsiaalsust ja kardatakse ka biomeetriliste andmete avalikustamist (Jain, Bolle, Pankanti 2006:35). IKS § 30 lg 2 ütleb, et delikaatsetete andmete kasutusele võtmine ja nende töötlemine peab olema täielikus sõltuvuses tegevuse eesmärgiga. See loob turvalisuse tunde, seaduse tasandil nendele inimestele, kes kardavad oma biomeetrilised andmete edastamist.

Milliseid biomeetrilisi andmeid kasutada – kas on turvalisem kasutada sõrmejälge või silmaiirist. On olemas mitu erinevat kasutusliiki ja kasutamise meetodit, kuid eelkõige sõltub kõik siiski olukorast. (Ashbourn 2000:45)

Biomeetriliste andmete kasutamise meetodid on jagatud kaheks põhiliseks rühmaks. Need on füsioloogilised meetodid ja käitumismeetodid (Modi 2011:4), mida autor kirjeldab järgmites peatükkides.

1.1. Füsioloogilised meetodid

Füsioloogilised meetodid on meetodid, mille aluseks on isikute füüsilised ehk anatoomilised omadused, mis on muutumatud. Need omadused on näiteks sõrmejäljed, iirise mustrid, võrrkesta kujud, peopesa kujutised, käe geomeetria, näo jooned. (Li, Jain 2009).

Kui viimati nimetatud omadust, ehk näo tuvastamist, võib kasutada nii inimeste tuvastamiseks kui ka igapäevases elus, näiteks kohtudes erinevate inimestega, siis teiste omadustega see nii lihtne ei ole. Selleks, et tuvastada isikut biomeetriliste omaduste kaudu, on olemas erinevad meetodid.

Kõige enamlevinum füsioloogiline meetod isiku tuvastamiseks on **sõrmejäljed**. Enamustes juhtumites ongi sõrmejälg esimene, mis assotsieerub biomeetriaga. Sõrmejälgede tuvastamine on õigusorganite peamine vahend, mille kaudu isikuid tuvastatakse. (Ashbourn 2000:45)

Biomeetria entsüklopeedia kirjutab, et sõrmejäljeks nimetatakse kuju, mis on jäänud pinnale pärast sõrme papilaarkurrustiku kokkupuudet (Li, Jain 2009).

Sõrmejälgede võtmist, uurimist ja nende kaudu isikute tuvastamist nimetatakse daktüloskoopiaks. Daktüloskoopia aluseks on kaks põhilist omadust, mis kuuluvad peopesa ja sõrmede papillaarnaha mustrile:

- stabiilne muster terve elu jooksul
- unikaalne muster, mis tähendab, et kahel isikul ei saa olla samasugust mustrit

Sõrmejälgede papillaarkurrud jagunevad, sõltuvalt iseloomulikust mustrist, kolmeks tüübiks, mis on välja toodud alloleval joonisel 1. (Lall 2010:9-10)

kaarkurrustik silmuskurrustik keerdkurrustik

Joonis 1. Sõrmejälgede papillaarkurrude tüübid (allikas Lall 2010:9-10)

Tänapäeval papillaarkurdude joonise identifitseerimise tehnoloogiat kasutatakse laialdaselt sõrmejälgede automaatse identifitseerimise süsteemis Automated Fingerprint Identification System (edaspidi AFIS), mis annab võimaluse luua ja

hoida daktüloskoopilised andmed elektrooniliselt. Praeguseks hetkeks on hoiul kümned miljonid sõrmejäljed, mida saavad kasutada erinevate riikide erinevad ametkonnad, sealhulgas ka piirivalve. (Ashbourn 2000:45; Modi 2011:46-47)

Integreeritud sõrmejälgede automaatne identifitseerimise süsteem Integrated Automated Fingerprint Identification System (edaspidi IAFIS) on maailmas kõige suurem biomeetriline andmebaas, mida haldab Föderaal Juurdlus Büroo ehk „Federal Bureau of Investigation“ (edaspidi FBI). IAFIS sisaldab nii sõrmejälgede kujusid, kui ka teisi inimeste füüsilisi omadusi ja tunnuseid nagu näiteks armid, tätoveeringute fotosid, inimese pikkus, kaal, juuste ja silmade värvid jne. (Modi 2011:52; Integrared...17.03.2012)

Teine füsioloogiline meetod on **käe geomeetria** ehk **käejäljed**. Käe geomeetria põhineb isiku identifitseerimiseks tema käe kuju ja mõõdu järgi (Li, Jain 2009). Käe geomeetria identifitseerimise meetod on sarnane sõrmejälgede identifitseerimisega. Suurim erinevus on selles, et kui sõrmejäljed püsivad muutumatutena, siis käe tunnused muutuvad vanusega. (Ворона, Тихонов 2010:76). Näiteks, käelaba ehk käe geomeetria aastatega muutub: esialgu nooruses inimesel käsi kasvab ja suureneb kuni isiku täisealiseks saamiseni ning seejärel hakkab seoses vanusega minema väiksemaks – „kokku kuivama“. Samuti käe geomeetria, mida saab matemaatiliselt ära mõõta, võib inimese elu jooksul muutuda haiguse, amputastsiooni või eluiviisi pärast.

Vastavalt käejäljendite tekkemehhanismist jagunevad need nelja rühma:

1) süvendjäljed– plastiline pind (või äkki siiski süvajäljed – süva st. sügavad, sügavamad);
2) pindjäljed – kõrvaliste aineosade kandumisel pinnale;
3) vähenähtavad – sile pind;
4) nähtamatud – poorne pind.

(Lall 2010:11)

Käe geomeetriat on võimalik kasutada füüsilise juurdepääsu või aja ning kohaloleku arvestamise kontrollimiseks (Ashbourn 2000:45). Näiteks lennujaamas, haiglas jne.

Järgmine tuntuim füsioloogiline meetod, mida loetakse samaväärseks kui sõrmejäljed on – **silmaiirise skaneerimine**.
Silmaiirise skaneerimise ja identifitseerimise valdkonna avastaja on doktor John Daugman ning ta patenteeris oma meetodit Amerika Ühendriigis 1994. aastal. Algoritmi mõte koosneb sellest, et inimese silmaiiris töödeldakse unikaalseks „iiris koodiks“, mis meenutab triipkoodi, mille alusel toimub andmebaasist kokkulangevuste otsing. Silmaiirise skaneerimine on mugav, kuna inimene ei pea visuaalselt keskenduma sihtmärgile ja seda saab teha vähem kui ühe meetri kauguselt. Suureks plussiks saab välja tuua, et silmaiirise skaneerimist erinevad häired ei sega, nii nagu sõrmejälgede puhul mustus, armid või käejälgede muutumine ajas. See tähendab, et läätsed, prillid ja ka päikeseprillid ei mõju süsteemi töövõimekusele. (Ворона, Тихонов 2010:68-69; Ashbourn 2000:52-53)

Silmaiirise skaneerimises kõige vajalikum tehnika on kaamera, mis loeb silmaiirise kujutist, füüsilist kontakti kasutaja ja seadme vahel ei toimu. (Jain, Bolle, Pankanti 2006:8-9)

Iga inimese silmaiiris on unikaalne nagu sõrmejälg. Õdesid, vendi ja ka kaksikud ei loeta eranditeks. Isegi ühe inimese vasaku ja parema silma iiris on erinev. Seega annab skaneeritud silmaiirise pilt rohkem informatsiooni kui sõrmejäljed. (Ashbourn 2000:52)

Isiku identifitseerimine läbi silma iirise skaneerimise on populaarne finantssektoris – näiteks on võimalik kasutada silma iirise skaneerimist sularahaautomaatides või kohtades, kus on kõrgendatud turvanõuded, ning John Daugmani loodud algoritme kasutatakse tänapäevani. (Ashbourn 2000:52-53; Ворона, Тихонов 2010:69)

Järgmine võimalus, mida saab kasutada isiku tuvastamisel on samuti seotud silmaga - **võrkkesta skaneerimine.** Igal inimesel on unikaalne silma võrkkest, mis tõestati juba 1935. aastal arstide poolt, kes uurisid silmahaiguseid ning avastasid, et võrkkesta mustrid olid keerulised ja stabiilsed (Ashbourn 2000:55).

Võrkkesta skaneerimise protsess näeb välja järgmiselt: isik peab vaatama kindlas suunas ja fokuseerima silma teatud punkti. Skanneeritakse väikese valgusega unikaalset võrkkesta mustrit ja suurendatakse teda optiliselt. Selline meetod võtab rohkem aega, kui mõni teine protsess aga on samas väga usaldusväärne. (Ashbourn 2000:55-56; Jain, Bolle, Pankanti 2006:14)

Kõige levinum füsioloogiline meetod, mida me kasutame igapäevaselt on isikute **näo tuvastamine**. Loomulikult kasutatakse seda meetodid kõige rohkem ka piirikontrolli süsteemis. Iga inimene, kes ületab piiri, läbib selle protsessi. Dokumendi kontrollija vaatab, kas passis olev pilt kuulub passi omanikule või mitte. Sama protsess toimub arvutis, aga erinevalt kontrollijast, kes lihtsalt visuaalselt võrdleb pilti kontrollitava inimese näoga, on arvuti süsteemis pilt juba olemas. (Ashbourn 2000:56-57)

Näo tuvastamise võib jagada kaheks rühmaks. Esimene on kontrollimine, mis tähendab kaameras oleva näo tuvastamist. Teine on identifitseerimine – on vaja leida vastavust „üks paljudest". (Ashbourn 2000:56; Ворона, Тихонов 2010:76)

Kui näo tuvastamist võrrelda mitmete teiste meetoditega, loetakse seda tunduvalt kliendisõbralikumaks. Selles protsessis puudub füüsiline kontakt inimese ja tehnika vahel. Ei ole vaja midagi puutuda ja ta säästab ka aega. Puudub vajadus seista ning oodata millal toimub tegevus. (Ворона, Тихонов 2010:72-73)

2003 aastal maikuus võttis Rahvusvaheline Tsivillennunduse Organisatsioon International Civil Aviation Organization (edaspidi ICAO (tegemist on organisatsiooniga, mis reguleerib reisidokumentides olevad turvaelementide standardid)) ametlikult vastu näo tuvastamise meetoodika masinaga loetavates reisidokumentides. Samas jäeti sõrmejälgede ja silmaiirise kasutamise

vabatahtlikuks, kuna Ameerika Ühendriikides sooviti pigem kasutada silmaiirist ja Euroopas sõrmejälgede tehnoloogiat. (Lion 2005-2006). Näiteks Eestis hakati kasutama masinaga loetavaid reisidokumente ehk biomeetrilisi reisidokumente alates 2007. aasta maist ning sõrmejäljekujutis lisati dokumendis olevale kiibile alates 2009. aasta juunist. Selline muudatus aitab kindlasti paremini isikuid tuvastada ning vähendab võltsitud dokumentide arvu. (Tabur, Koort 2010: 27-28)

Viimastel aastatel on biomeetrias suure populaarsuse võitnud **desoksüribonukleiinhape deoxyribonucleic acid** (edaspidi **DNA)** tehnoloogia, kuigi on võrreldes teistega tunduvalt kallim ja töömahukam. DNA testid on täpsed, kuigi see võib olla varieeruv just isikute sugulussidemete ilmnemisel, näiteks ühemunakaksikute DNA on identne. Suureks probleemiks on DNA määramisel aeg, mida soovitakse lühendada maksimaalselt ühele tunnile. (Modi 2011:149-150)

1.2. Käitumismeetodid

Käitumismeetodite järgi tuvastamisel vaadeldakse inimeste tegevusi, mis on samuti nagu füsioloogilisedki meetodidki igale ühele ainuomased (Li, Jain 2009). Tegevuste all mõeldakse näiteks rääkimist, laulamist, kirjutamist või trükkimist. Järgnevalt kirjeldab töö autor käitumismeetoditest hääle kontrollimist, allkirja kontrollimist, klahvivajutise dünaamikat ja kõnnakut.

Hääle kontrollimise põhimõte on see, et üksikisikute näo struktuur, häälekurrud, hammaste ja suu struktuur mõjutavad ja muudavad kõne dünaamikat. Näiteks kui võtta kaks inimest samast soost, sama kasvuga, kes on sündinud ja kasvanud samas linnas, räägivad samas keeles samasuguse dialektiga, ja paluda neil öelda mikrofoni üks ja sama sõna, siis leiame suuri erinevusi. (Ashbourn 2000:59)

Selle meetodi suureks miinuseks on madal identifitseerimise täpsus. Näiteks haige kurguga inimest ei saa kasutada hääle kontrollimisel. Selline biomeetriliste andmete kasutamise liik omab palju puudusi ning sõltub paljudest teguritest, näiteks on oluline, kas on müra või ei ole, kas mikrofonis on häired või ei.

Inimene, kui räägib, võib teha vigu, mis segab hääle kontrollimist. Samuti mõjutab häält isiku emotsionaalne seisund. (Воронв, Тихонов 2010:80)

Allkiri on isiku unikaalne omadus. Mille kontrollimine on rohkem arusaadavam, tuntum ja loomulikum kui näiteks sõrmejälgede identifitseerimine, mida enamus seostab kriminaal valdkonnaga. Allkirja kontrollimisel võrreldakse, mitte juba tehtud allkirja, vaid allkirja tegemise protsessi. (Ashbourn 2000:61; Ворона, Тихонов 2010:78)
Allkirja identifitseerimiseks on olemas kaks võimalust:

- tavaline võrdlemine näidisega
- dünaamiline kontroll

Esimest meetodit ei saa nimetada usaldusväärseks. Allkirja võrreldakse andmebaasis juba oleva graafilise kujutisega. Kuna allkiri ei ole iga kord samasugune (allkirja kuju sõltub näiteks kirjutamise positsioonist jne.) on vigade protsent väga suur.

Dünaamiline kontroll on raskem. See annab võimaluse fikseerida allkirja tegemise protsessi omadused reaalajas. Vaadatakse kui tugevalt vajutatakse pinnale, kui kiiresti tehakse kirjutusvahendiga esimene löök, kuidas muutub kirjutamise kiirus.Vaadatakse ka kui palju üldse võtab aega allkirja kirjutamise protsess. See garanteerib, et allkiri ei ole võltsitud, kuna keegi ei oska kopeerida allkirja omaniku käe käitumist. (Ворона, Тихонов 2010:78-79)

Klahvivajutise dünaamika identifitseerimine on aja pikkus klahvivajutuste vahel. Iga inimene, kui kasutab arvutit näitab oma unikaalse trükkimisviisi. Kasutaja unikaalsus on seotud trükkimiskiiruse ja trükkimisomadustega. (Ashbourn 2000:63)

Suhtelselt ainulaadne on inimese **kõnnak**. Unikaalseks teeb seda inimese skeletti anatoomiline iseärasus, inimese kasv ning inimese omandatud käitumisoskused. Kõnnaku plussiks on see, et seda saab jälgida vahemaa tagant, samuti on seda hea

kasutada järelevalve rakendamisel. Identifitseerimine kõnnaku jälgimisega on näidanud paljulubavaid tulemusi. On selge, et välised faktorid nagu kehakaalu muutus, jalatsite tüüp, väsimuse tase, riiete liik ja kokkupuute pind mõjutavad kõnnakut. Kõnnaku järgi isiku tuvastamine on praegusel hetkel veel algus järgus. Arvatavasti hakatakse kõnnakut kasutama koos teiste biomeetriliste tehnoloogiatega, et teha identifitseerimise tulemused paremaks ja usaldusväärsemaks. (Modi 2011:150)

2. BIOMEETRILISTE ANDMETE KASUTAMINE JA BIOMEETRILISED REISIDOKUMENDID

Väga tihti kui räägitakse biomeetriast kasutatakse sõna „identifitseerimine". Muidugi ei ole see vale, kuid siiski mittetäiuslik, sest biomeetrias teiseks oluliseks komponendiks on verifitseerimine või teiste sõnadega kontrollimine. Need kaks mõistet, mis iseloomustavad biomeetrilist süsteemi on erinevate tähendustega.

Kui tegemist on biometrilise identifitseerimisega, siis kasutatakse tuvastamiseks kõiki salvestusi, mis on olemas andmebaasis, et kontrollida kas on kokkulangemist, või ei ole. (Ashbourn 2000:66) Sellist meetodit kasutatakse näiteks kriminalistikas, et kontrollida leitud sõrmejälgi juba olemasolevate jälgedega läbi andmebaaside.
Biomeetriline verifitseerimine tähendab isiku eelnevalt skaneeritud tunnusjoonte võrdlemist uute samade skaneeritud tunnustega. Näiteks, kui isik tuleb esimest korda tööle, tema sõrmejäljed sisestatakse tööaja arvestamise andmebaasi süsteemi. Kui töötaja tuleb järgmine kord tööle, siis tema uuesti skaneeritud sõrmejälgi võrreldakse nendega, mis tal olid võetud esimesel päeval. Kui kokkulangevus on olemas, siis saab isik juurdepääsu. Verifitseerimine on kiirem protsess, kui identifitseerimine (Ashbourn 2000:65).

Väga efektiivselt võib biomeetriat kasutada läbipääsusüsteemis ja vanglasüsteemis. Näiteks vanglasüsteemis rakendatakse biomeetriat eelkõige külalistele, et tuvastada, kes pärast visiiti lahkub – kas külaline või keegi teine kes esineb külalisena. Sellistes situatsioonides on efektiivne kasutada käe biomeetriat. (Ashbourn 2000:27-29)

Biomeetria rakendamine kriminalistikas on äärmiselt levinud, näiteks daktüloskoopeerimine ja palmoskoopia, mis tegeleb inimese peopesa uurimisega.

Nende protsesside kasutamine annab võimaluse identifitseerida näiteks, kes pani toime kuriteo, ning selle isiku omadused nagu tema sugu vanus ja kasv. (Ashbourn 2000:5-6; Lall 2010:8-9)

Biomeetriaga puutuvad kokku erinevates tuvastamissituatsioonides ka tavainimesed (Ashbourn 2000:21). Nii Isikut tõendavate dokumentide seaduses kui ka Välismaalaste seaduses (edaspidi VMS) on ära reguleeritud biomeetriliste andmete võtmine, töötlemine, hoiustamine. Et vältida dubleerimist, toob autor välja näited Eesti Välismaalaste seadusest. VMS § 26 reguleerib, et välismaalaselt võib võtta ja töödelda nende biomeetrilisi andmeid, et isikut identifitseerida. Kui haldusorgan nõuab välismaalase isiku biomeetrilisi andmeid, siis on välismaalane kohustatud need andmed andma. (Välismaalase seadus, 09.12.2009)

Vastavalt VMS § 272 järgi võib biomeetrilistest andmetest töödelda näokujutist, sõrmejäljekujutisi, allkirja või allkirjakujutist ja silmaiirisekujutisi. Juhul kui välismaalane ise ei anna oma biomeetrilisi andmeid, siis võib tema vastu kasutada jõudu. (Välismaalase seadus, 09.12.2009) Viimast loomulikult ei kehtestata kui välismaalane soovib esitada viisataotlust.

VMS § 270 on välja toodud, et haldusorgan võib töödelda, üle anda välismaalase biomeetrilisi andmeid kolmandatele isikutele ja seda isiku nõusolekuta ning isikut teavitamata juhul, kui välismaalane esitab või pikendab taotlust, mis puudutab tema seaduslikku töötamist või elamist Eestis. Või kui haldusorganil on vajadus kontrollida selle omamise õiguspärasust. Samuti VMS § 271 tuleneb, et haldusorganil on õigus kogutud välismaalase biomeetrilisi andmeid üle anda välisriigile, rahvusvahelistele organisatsioonidele, EL institutsioonile ja EL ühtsesse andmekogusse, lähtudes nendega seotud õiguaktidest. Samuti võib haldusorgan töödelda saadud delikaatseid andmeid. (Välismaalase seadus, 09.12.2009)

Autori arvates on Eesti seadusandlus, VMS näitel, väga hästi reguleerinud võimaluse isikute tuvastamiseks biomeetriliste andmete kaudu ning samuti andmete töötlemise ja edastamise välisriikidesse, mis on üks kindel võimalus riikide turvalisuse tõstmiseks.

Samuti oleks mõistlik kasutada biomeetrilist tehnoloogiat turvalisuse eesmärgil spordiklubides, hasartmängudeklubides ja teistes kohtades, kus on tegemist erahuvidega. Tavaliselt klubiliikmetele väljastatakse tavaline plastikkaart. Pole välistatud, et kaardi kaotamisel võib selle oma huvides ära kasutada võõras isik. Sellist olukorda saab vältida biomeetrilise tehnoloogia kasutamisega ning loob klientidele personaalsema lähenemise. (Ashbourn 2000:39-40)

Biomeetria kasutamine tegi turvalisemaks ka tohutu kiirusega areneva infotehnoloogia valdkonna, sealhulgas personaalarvuti kasutamise. Näiteks saab arvutitesse sisselogida pärast sõrmejälje tuvastamist, või tuvastatakse arvutikasutaja kiipkaardil olevate andmete kaudu. (Ashbourn 2000:35)

Piiri kontrolli süsteemis kasutatakse biomeetrilisi tehnoloogiaid erinevatel juhtudel. Näiteks Eestis, nagu teistes EL liikmesriikides, on olemas biomeetrilised reisidokumendid, kus kasutatakse dokumentide turvalisemaks muutmiseks näobiomeetriat ja sõrmejäljebiomeetriat. Näobiomeetria ja sõrmejälje andmekandjaks on kontaktivaba kiip, mis on lisatud reisidokumenti. (Ashbourn 2000:31-32; Biomeetrilised...11.12.2010; Tabur, Koort 2010:28)
Biomeetriliste passide kiibid võivad asuda dokumentide kaante või isikuandmete lehe sees. Samuti võib kiip paikneda eraldi, spetsiaalselt märgistatud, lehekülje sees teiste dokumendi lehtede vahel.

Kontaktivabade kiipide kasutamine oli valitud sellepärast, et nad olid kiiremad kui kontakt kiibid. Teine põhjus oli see, et kontaktivabad kiibid andsid võimaluse omada lihtsat juurdepääsu salvestatud andmetele niikaua, kui ta oli kiibilugeja raadiuses. (Lion 2005-2006)

ICAO regulatsiooni kohaselt peab kontaktivaba kiibi suurus olema vähemalt 32 kB. Sellise kiibi suurus, mis sisaldab nii näokujutis, kui ka sõrmejälgede kujutist on vähemalt 64 kB. (Lion 2007-2008; Cuthbertson 2008). Enamus riike kasutabki suurema mahuhulga kiipi.

Kõik biomeetrilised ehk e-passid peavad olema märgistatud sümboliga, mida on näha joonisel 2. Sümbol annab märku, et reisidokument sisaldab kiipi, kuid ei näita selle täpset asukohta. (Machine Readable Travel Documents 2006:II-2)

Joonis 2. E-passide sümbol (allikas Machine Readable Travel Documents 2006:II-2)

ICAO nõuete kohaselt peab iga biomeetriline tunnus olema kantud kontaktivaba kiibile (Lion 2005-2006).

2003 aastal mai kuus, võttis ICAO formaalselt vastu regulatsiooni sõrmejälgede ja silma iirise kasutamise kohta reisidokumentides. Alates veebruarist 2009 juuni on EL reisidokumentides sõrmejälje kujutiste kandmine kontaktivaba kiibile kohustuslik. Näiteks on Eesti reisidokumentide kontaktivaba kiibile salvestatud näokujutist ja sõrmejälje kujutist. (Lion 2005-2006)

Silmaiirise kujutise lisamine reisidokumendi kiibile on jäetud esialgu veel vabatahtlikuk (Lion 2005-2006).

Kuna kiibile kantavad andmed peavad olema riigiti sarnased, et oleks võimalik erinevate riikide kiipidel olevaid andmeid lugeda, on ära reguleeritud, lisaks kiibi suurusele, ülejäänud andmete olemus. Näiteks peab reisidokumentides kasutama ainult digitaalset pilti, mis ei tohi olla üle poole aasta vana. Näokujutise suurus peab moodustama 70-80% vertikaalsest kõrgusest. Pilt peab olema värviline, mõõtmetega mitte rohkem kui 45 x 35 mm, ja mitte vähem kui 32 x 26 mm. Isik

fotol peab olema neutraalse ilmega, avatud silmadega, suletud suuga. Vaade peab olema suunatud objektiivi. Taust peab sisaldama heledat värvi ja peab olema ühetooniline. Peakatet võib kasutada ainult erandjuhtudel, mis on seotud religiooniga, meditsiiniliste ettekirjutustega ja kultuuriliste traditsioonidega. Prille lubatakse kasutada juhul kui nad ei ole tumedate klaasidega, valgus ei peegelda ja raam ei ole suur ja paks. (Machine Readable Travel Documents 2006:56-58)

Eestis väljastatakse biomeetrilisi reisidokumente, mille kiip sisaldab näobiomeetriat alates 22.05.2007.aastast ja alates juunist 2009 lisati kiipi sõrmejäljed. (Tabur, Koort 2010:27)

Biomeetrilistest reisidokumentidest väljastatakse Eesti Vabariigi kodanikule:

1. Euroopa Liidu kodaniku pass
2. Diplomaatiline pass
3. Meremehe teenistusraamat.

ning mittekodanikele väljastatkse:

1. Välismaalase pass
2. Meresõidutunnistus
3. Ajutine reisidokument
4. Pagulase reisidokument.

(Isikut tõendavate dokumentide seadus, 15.02.1999; Biomeetrilised...11.12.2010; Document....28.12.2010)

2010 aastal oli üheks peamiseks eesmärgiks Eesti turvalisuspoliitika raames hakata kasutama biomeetriat ka nende isikute hulgas, kes hakkavad taotlema EL liikmesriigi viisat või elamisluba. Praegusel hetkel peavadki Eesti Vabariigi elamisloa taotlemisel isikud, kes on vanemad kui 6 aastat andma oma sõrmejäljekujutised. (Tabur, Koort 2010:28; Elamisluba…02.04.12)

Biomeetrilise passi omanikel on loodud ka suurema võimalused, näiteks viisavabaprogrammi raames Eesti kodanikel, kellele on olemas biomeetriline pass ei ole vaja viisat, et saada Ameerika Ühendriikidesse. (Viisad...24.04.2011)
Samuti, osade riikide biomeetrilise passide omanikud saavad viibida Schengeni viisaruumis ja seal hulgas Eesti Vabariigis kuni 90 päeva poole aasta jooksul viisavabalt. Need riigid on: Albaania, Bosnia ja Hertsegoviina, Makedoonia, Montenegro ja Serbia. (Viisavaba….29.03.2012)

Biomeetrilise passi omanikele on osades piiripunktides piirikontrolli süsteem lihtsustatud, näiteks on võimalus kasutada automaatset piirikontrolli süsteemi Automated Border Control system (edaspidi ABC süsteem). ABC süsteem põhineb reisijate biomeetrilises identifitseerimises. Toimub niinimetatud enese identifitseerimine. ABC süsteemi kasutamine lihtsustab nii piiriületajate kui ka piirivalvurite tegevust. Sellise süsteemi töökiirus on kõrge. Lisaks on ABC süsteem turvaline, kuna kontrollib e-passi andmete õigsust elektroonilise kiibi kaudu ja on võimeline registreerima kas antud e-pass kuulub omanikule või mitte. Samuti võrreldakse kiibil olevaid andmeid andmebaasis olevate andmetega. Kindlasti kõrgendab ABC süsteem praegust piirikontrolli efektiivsust. (Lion 2007-2008; Siciliano 2009)

Näiteks, Soomes kasutusel olev ABC süsteem töötab järgnevalt. Kõigepealt asetab isik e-passi passilugejale, kus fikseeritakse kiibil olevad andmed, seejärel läheb inimene edasi ja seisab kindlaksmääratud kohas, kus tehakse isikust reaalne pilt ning seejärel võrreldakse kiibil olevat ja reaalset pilti. Samal ajal sisestab isik oma reisi eesmärgi ja veel mõningaid andmeid. Kui kõik on korras, süttib roheline tuli ja isik võib piiri ületada. Kui on kolmanda riigi kodanik, kellel on vaja passi piiriületustempel, suunatakse ta politsei ametniku poolte. Kogu protseduur tehakse nn väikeses kontrollkabiinis.

Aastatel 2012-2013 on planeeritud paigutada ABC süsteemid Lennart Meri Tallinna lennujaama.

3. BIOMEETRILISTE REISIDOKUMENTIDE VÕLTSINGUTE AVASTAMINE EESTI VÄLISPIIRIL

Biomeetriliste andmete lisamine dokumentidesse peaks suurendama nende turvalisust ning raskendama võltsimist. Kas seda on täheldanud ka ametnikud, kes kontrollivad reisidokumente Eesti välispiiril? Selle uurimiseks viis töö autor läbi ekspertintervjuud II astme dokumentide kontrolli teostajatega. Autori seisukohalt saavad anda just II astme dokumentide kontrolli teostajad, kes puutuvad kokku oma igapäevases töös põhjaliku dokumentide kontrollimisega ning dokumentide võltsingute avastamisega, täpsema ülevaate biomeetriliste reisidokumentide kasutamisest ning nendega manipuleerimisvõimalustest.

Uuringu ettevalmistamise käigus sai autorile selgeks, et eesmärgi saavutamiseks ei ole piisav teha uuring ainult ühes prefektuuris. Selleks otsustas autor uuringu läbi viia kõikides Eesti Vabariigi rahvusvahelistes piiripunktides.

Uuring on läbi viidud Põhja prefektuuri Tallinna piiripunktis, Lõuna prefektuuri Koidula ja Luhamaa piiripunktides ning Ida prefektuuri Narva maantee piiripunktis. Intervjuude küsimused saadeti II astme dokumentide kontrollijatele meili teel. Kokku viidi läbi 7 intervjuud, mille käigus esitati 13 küsimust, küsimuste järjekorda ei muudetud. Vastused analüüsiti anonüümselt. Järgnevalt toobki autor välja esitatud küsimused ning vastustest analüüsitud kokkuvõtte.

Esimesed kaks küsimust olid iseloomustavad, mis annavad ülevaate II astme dokumentide kontrollijate pädevusest:

1. Kui kaua Teie töötate dokumendieksperdina?
2. Milline on Teie ametialane haridus?

Intervjueeritavate vastustest selgus, et üks ametnik on tegelenud II astme kontrolliga alla aasta, kaks ametnikku kolm aastat, üks ametnik neli aastat, üks neli ja pool aastat, üks ametnik kuus aastat ja üks ametnik kümme aastat. Kõik vastajad on lõpetanud Muraste piirivalvekolledži (praeguse Sisekaitseakadeemia politsei- ja piirivalvekolledž) ning dokumentide kontrolli põhjalikumad teadmised on intervjueeritavatel omandatud erinevatel täienduskoolitustel. Lisaks on kaks ametnikku oma teadmisi täiendanud välismaal. See näitab, et intervjueeritavad on oma ala asjatundjad ning oskavad dokumentide kontrolli tulemuslikkust analüüsida nii enne biomeetriliste reisidokumentide kasutamist, kui ka hinnata nüüdset olukorda ja koostada ka riskianalüüsi.

Antud analüüside koostamisel, autori arvates võib välja töötada statistilise skeemi, kuhu on sisse kantud avastatud biomeetriliste dokumentide võltsingud. Tuleb koostada tabelid, mis hakkavad sisaldama võltsingute tüüpe, näiteks: kas tegemist oli fotovahetusega, isikuandmete lehe võltsimisega, piiriületustemplite manipuleerimisega, kiibi mehaanilise või elektroonilise vigastamisega, kiibi vahetusega, või elektrooniliselt kiibil olevate andmete muutmisega jne. Lähtudes nendes andmetest dokumentidekontrolli teostatavad ametnikud peavad esmajärguliselt kontrollima neid kohti, kus statistika järgi võltsingute arv on kõige suurem ja tõenäolisem. Kindlasti antud tabelit tuleb pidevalt uuendada ja täiendada vastavalt uute võltsingute avastamisele biomeetrilistes reisidokumentides, sest tendents võib muutuda vastavalt dokumendi võltsijate arengule. Oleks mõistlik, et antud andmed oleksid kättesaadavad igas piiripunktis üle Eesti ja kõik piiripunktide ametnikud esimesel võimalusel pidevalt täiendaksid neid.

Järgmiste küsimustega tundis autor huvi efektiivsust ja turvalisust reisidokumentides seoses biomeetriliste tehnoloogiate kasutamisega nendes dokumentides.

3. Kas biomeetriliste reisidokumentide sisseviimine vähendas dokumentide võltsimist?

Sellele küsimusele oli intervjueeritavatel põhimõtteliselt ühesugune jaatav vastus. Selgus, et biomeetriliste dokumentide sisseviimine vähendas dokumentide võltsimist, kuid ainult osaliselt. Petturid püüavad kasutada kas kergemini võltsitavaid dokumente ehk neid, mis ei sisalda kiipi, on lihtsamate turvaelementidega, või siis kuritarvitatakse teisele isikule kuuluvaid dokumente. Muidugi tuleb võltsijatel arvestada, et biomeetriliste dokumentide võltsimine on tunduvalt keerulisem ja aeganõudvam. Autor tahab siinjuures mainida, et võltsingud arenevad sama kiiresti kui tehnoloogia ja kindlasti ei saa dokumentide kontrollijad tugineda teadmisele, et kiibiga reisidokumendid on turvalisemad ja nende kontrollimine ei nõua niipalju tähelepanu kui kiibita reisidokumendid.

Kindlasti biomeetriliste tehnoloogiate kasutamine aitab tõsta Eesti ja kogu Euroopa Liidu riikide turvalisust ja biomeetrilised tehnoloogiad lihtsustavad dokumendikontrollijatel võltsingute avastamist ning uute tehnoloogiate sisseviimine raskendab võltsimese protsessi. Kuigi on juba praegu selge, et petturid „arenevad“ paralleelselt koos dokumentide tootjatega. Järelikult, uute tehnoloogiate arenguprotsess, mis aitab tõsta reisidokumentide turvalisust, peab olema pidev ja jätkuv.

4. Kas biomeetrilisi reisidokumente on võimalik võltsida?
5. Kui jah, siis kuidas, kui ei, siis miks?

Sellistele küsimustele vastasid kõik intervjueeritavad, et biomeetrilisi reisidokumente on võimalik võltsida erineval moel. Toodi välja kolm kõige tõenäolisemat moodust: esiteks, biomeetrilistes passides on võimalik vahetada fotot ja jätta kiibile teise isiku (originaal) andmed ehk võltsing puudutab ainult isikuandmetelehte. Teine variant on foto vahetus ja kiibil olevate andmete muutmine, või kiibi välja vahetamine. Selliste võltsingute tegemine on keerulisem protsess ja dokumendi kasutajale kallim, kuid analoogseid juhtumeid on maailmas juba esinenud. Muidugi eeldab sellise võltsingu teostamine väga hea tehnika olemasolu ja eelkõige spetsiaalseid teadmisi. Kolmanda variandina tõid intervjueeritavad uuesti välja, sarnase fotoga inimese leidmine, ehk võõra isiku

reisidokumendi kuritarvitamise.

Seoses biomeetriliste dokumentide kasutusele võtmisega ja nende populaarsuse suurenemisega, autori arvates erilist tähelepanu peab pöörduma sellistele juhtumitele, kus on tegemist biomeetriliste reisidokumentidega, mille kiip on rikutud ja on võltsitud teised turvaelemendid või on kasutatud võõra isiku dokumenti. Antud meetod on võltsijate jaoks lihtsam ja odavam, kui näiteks kiibi välja vahetamine. Selles olukorras on oht, et läbi kiibi ei saa kontrollida isiku andmed, järelikult peab väga hoolikalt kontrollima, kas ei ole veel tegemist fotovahetusega või teise isiku dokumendiga. Suurem oht võib tulla näiteks Hiina või Kongo kodanikega, kuna enamus isikutest, kes kasutavad võltsitud dokumente, on antud riikide kodanikud. Samuti nende tuvastamine läbi foto on keeruline protsess, ja tõestada et nad ise tahtlikult rikkusid kiibi, on väga raske. Eeltoodust tulenevalt võib eeldada, et selliste juhtumite arv hakkab kasvama nii kaua, kui nad ei suuda oskuslikult muuta kiibi andmeid.

Seega on biomeetrilised tehnoloogiad efektiivsed nii kaua, kui nad on uued ja neid ei ole võimalik võltsida ja töödelda. Biomeetriliste tehnoloogiate kasutamisvõimalused peavad kogu aeg arenema ja sammukese võltsijatest eespool käima, et nendel ei oleks võimalust ära harjuda võltsida biomeetrilised reisidokumendid. Ülalmainitust tulenevalt antud töö autor pöörab tähelepanu sellisele aspektile nagu konfidentsiaalsus ja saladus. Kuna neid tehnoloogiaid kasutatakse riigi julgeoleku turvalisuse tagamiseks, peavad nad olema piiratud taseme kättesaamisega.

Intervjueeritavad mainisid, enda vastustes ka piirikontrollis ABC süsteemi kasutamist ja tõid välja ühe suure ohu, millele tuleks autori hinnangul erilist tähelepanu pöörata, kuna varsti hakkavad analoogsed süsteemid tööle ka Eestis. Näiteks oli juhtum, kus Suurbritannia passis asuv originaal kiip ei töödanud, võltsitud kiip oli kleebitud tagakaane välimisele küljele ja töötas probleemideta. Selge on see, et ABC süsteem lihtsustab piirikontrolli ja aitab avastada nii võltsitud dokumente kui ka illegaalide liikumist, kuid intervjueeritavate poolt

toodud näite põhjal ei saa me ka tulevikus dokumentide kontrollis täielikult inimfaktorit välistada, seega peab autor väga oluliseks ABC süsteemi täiustamist, et sarnaseid olukordi oleks võimalik tulevikus tuvastada. Samuti on autor seisukohal, et analoogseid situatsioone aitab ennetada piiripunktides isikute profileerimine läbi kaamerate, et näha isikute kontrollieelset ning - järgset käitumist.

Järgmisena tundis autor huvi, kas intervjueeritavatel on olnud isiklikult praktilisi kogemusi tuvastada võltsitud biomeetrilisi dokumente:

6. Kas Teie praktikas oli piiriületajate poolt kasutatud võltsitud biomeetrilisi dokumente?

Sellisele küsimusele vastas enamus intervjueeritavaid, et oma praktikas ei ole nad näinud, ega avastanud võltsitud biomeetrilisi reisidokumente. Kaks intervjueeritavad tõid välja, et nägid biomeetrilisi passe kus kiip oli rikutud, aga võltsitud oli teisi turvaelemente. Põhilisteks võltsinguteks , mida intervjueeritavad välja tõid on Eesti välispiiril siiani olnud reisidokumentides kogu isikuandmete lehe vahetus, viisade või elamislubade manipuleerimised.

Ühel dokumendieksperdil oli olemas ka praktiline kogemus võltsitud biomeetrilise reisidokumendi avastamisel 2007 aastal, kui neli Malaysia kodanikku kasutasid võltsitud isikuandmetega biomeetrilisi passe. Nende reisidokumentide kiibid olid kahjustatud või piiripunktis olevatele seadmetele loetamatud. Seega peab autori hinnangul pöörama erilist tähelepanu piiri ületajatele, kes saabuvad meie jaoks nn. eksootilistest riikidest või dokumentidele, mida kontrolltehnika mingil põhjusel ei ole võimeline kontrollima

7. Kas biomeetrilised tehnoloogiad aitavad suurendada dokumentide turvalisust?

Selle küsimusele andsid kõik eksperdid ühese positiivse vastuse, milleni jõudis ka autor tutvudes eelnevalt erinevate materjalidega.. Suureks plussiks toodi intervjueeritavate poolt välja see, et biomeetrilistel reisidokumentidel saab lisaks kontrollida kiibil olevat sõrmejälge ning kiibil olev värviline foto on suurem ja parema kvaliteediga, kui isikuandmete lehele trükkitud foto.

Kuna illegaalide sisseränne on väga tihedalt seotud võltsitud dokumentidega, tundiski autor huvi illegaalide poolt kasutatud võltsitud reisidokumentide vastu ning järgmised kolm küsimust puudutasid illegaalide sisserännet. Autori küsimused olid järgnevad:

8. Kas Teie piiripunktis on olnud illegaalse sisserände tõkestamise juhtumeid?
9. Kui palju illegaalidest kasutasid biomeetrilisi reisidokumente?
10. Mitu illegaali oli Teil võimalik piiriületajate hulgast tuvastada kasutades biomeetrilisi andmeid?

Vastajad tõid välja, et illegaalide sisseränne kõikides piiripunktides on tõusutrendis. Kõige rohkem juhtumeid toimub Tallinna piiripunktis ja Narva maantee ja raudtee piiripunktides. Näiteks 2011 aastal Ida prefektuuri piiripunktides tõkestati nelikümmend üks illegaalse sisserände juhtumit. Perioodil 2011 jaanuar kuni 2012 märts on Eesti Vabariiki illegaalselt sisenejad kasutanud biomeetrilisi reisidokumente alla 30%.
Sellest järeldab autor, et illegaalid kasutavad võimaluse korral ilma kiibita reisidokumente, et viia dokumendi võltsingu avastamisvõimalus miinimumini. Samuti nõuab biomeetriliste reisidokumentide järeleaimamine kõrgemaid teadmisis elektroonika vallas, kallimat tehnikat ning biomeetriliste andmetega võltsitud dokumendid on kallimad, mille omandamist illegaalsed reisijad endale küllaltki tihti lubada ei saa.

11. Kas Teie arvates biomeetriliste tehnoloogiate kasutamine reisidokumentides on efektiivne?

Biomeetriliste tehnoloogiate kasutamise efektiivsuse kohta reisidokumentides olid intervjueeritavad erinevatel seisukohtadel. Ühe intervjueeritava arvamusel kergendab biomeetriliste tehnoloogiate kasutamine võltsitud dokumentide tuvastamist. Mis ühtib täielikult ka autori arvamusega. Kaks intervjueeritavat arvasid, et biomeetriliste tehnoloogiate kasutamine I astmes on veel palju arenguruumi. Samuti toodi välja probleemina biomeetriliste andmete lugejate pikaajaline remont, mida peab autor äärmiselt taunitavaks, sest kontrollimisel ei kasutata olulist informatsioonikandjat ning võltsijad võivad olla sellest teadlikud. Intervjueeritavate arvates on biomeetriline tehnoloogia efektiivne ainult juhul, kui seda on võimalik ka piiril olevate seadmetega kontrollida. Ühe dokumendieksperdi arvamus oli, et biomeetrilised tehnoloogiad on efektiivsed nii kaua, kui võltsijad ei oska neid imiteerida ja töödelda. Samas aga tõid juba intervjueeritavad eelnevalt välja võimaluse, kuidas petturitel on õnnestunud läbida kontroll nii, et kontrolltehnika ei tuvastanud võltsingut.

12. Kas automaatse elektroonilise piiriületuse süsteemi (Automated Border Control system) sisseviimine Teie piiripunktis tõstaks EL riikide turvalisust?

Sellise küsimuse vastused näitasid, et ABC süsteemi sisseviimine kindlasti tõstab EL riikide turvalisust. Intervjueeritavad tõid näite Soome piiripunktist, kus tänu sellele on avastatud hulgaliselt illegaalide sisserände juhtumeid. Samuti toodi välja, et ei saa jääda lootma ainult tehnoloogiale – inimene on ikka see, kes on suuteline tuvastama võltsingu ka siis, kui petturid püüavad kontrolltehnikat segadusse ajada või edastada sellele valet informatsiooni. Ainult üks intervjueeritav arvas, et maantee piiripunktis oleks sellise tehnoloogia kasutamise efektiivsus väga madal. Kuna intervjuu käigus ei olnud võimalus täiendavaid küsimusi esitada, ei saa autor tuua välja sellise vastuse kujunemise põhjust.

13. Kas Te soovite midagi lisada või soovitada biomeetriliste tehnoloogiate kasutamise/rakendamise kohta reisidokumentides?

II astme kontrolli ametnikud vastasid, et üldiselt on olukord ja tendents positiivne ja kui biomeetriliste dokumentide kontroll veel areneb, siis hakkavad tulemused illegaalide avastamisel paranema. Üks intervjueeritav tõi välja, et Eestis peab rohkem arenema ka silmaiirise tehnoloogiate arendamine. Silmaiiris on individuaalne nagu sõrmejälg, aga sellel tehnoloogial on veel puudusi, et tuvastada inimesi sajaprotsendiliselt.

Kõik intervjuus osalenud ütlesid, et turvalisuse tõstmiseks peavad biomeetrilised tehnoloogiad edasi arenema ja jõudma selleni, et oleks võimalik neid pidevalt kasutada ka I astme kontrollis. Seeläbi saaks koheselt kontrollida biomeetrilised dokumendid kõikidel piiriületajatel, kaasa arvatud saab kontrollida kiibi originaalsust ja selline uuendus muudab teise isiku dokumendi kasutamise avastamist lihtsamaks. Samuti I astme kontrollis töötavad ametnikud saaksid võimaluse põhjalikumalt täiendada ja rakendada oma oskuseid ja teadmisi oma igapäevases töös.

Intervjuu kokkuvõtteks saab autor öelda, et kõikide intervjueeritavate arvates on biomeetriliste andmete lisamine reisidokumentidesse loonud juurde efektiivse võimaluse tuvastada dokumentide originaalsust, kuid seda ei tohiks kindlasti ülehinnata. Dokumentide kontrollijad peavad meeles pidama, et tehnika võib eksida ja sellega on võimalik manipuleerida vastavalt petturite soovidele. Võltsijad on alati tehnoloogia arengutega väga hästi kursis ning püüavad pidevalt dokumentide kontrollijaid eksitada.

KOKKUVÕTE

Käesoleva töö eesmärgiks oli uurida biomeetriliste reisidokumentide turvalisust. Töö autor võib öelda, et püstitatud eesmärk saavutati. Töös antakse lugejale ülevaade biomeetriast ning mida loetakse biomeetriaks, millises valdkonnas seda kasutatakse ja mis suunas areneb.

Ühiselt on selge, et pärast 11.septembrit 2001 muutus maailm turvalisemaks, kuna hakati pöörama suuremat tähelepanu just biomeetria uuringutele ja hakati aktiivselt otsima biomeetria kasutamisvõimalusi.

Intervjuude tulemusena saab öelda, et biomeetriliste tehnoloogiate kasutamine aitab muuta nii Eestit kui ka kogu Euroopa Liitu turvalisemaks. Aga sellest olenemata on leitud puudusi ja kitsakohti. Nendest tuginedes alljärgnevalt esitab autor järeldused:

1. Niikaua kui on olemas reisidokumendid, mis ei sisalda biomeetriliste andmetega kontaktivaba kiipi, kasutavad illegaalid võimalust ja võltsivad neid dokumente, mille võltsimise protsess on lihtsam.
2. Kõik uued tehnoloogiad on efektiivsed nii kaua, kui nad on uued ja nende võltsimine on keeruline, kallis ja võltsijate jaoks läbiuurimata.
3. ABC süsteem lihtsustab piirikontrolli ja aitab avastada illegaalse migratsiooni juhtumeid, aga inimfaktorit ei saa ka välistada, kuna ametnikud peavad teostama kontrolli ja nad on suutelised rohkemaks juhtudel, kui piiriületajad püüavad automaatikat petta. Samuti tehnikaga saab ja ongi juba manipuleeritud.
4. Biomeetriliste dokumentide arv maailmas regulaarselt kasvab, kasvab ka võltsingute arv. Intervjuude tulemused näitasid, et tekib lisateaduste ja oskuste vajadus biomeetrilises valdkonnas.

Biomeetriliste tehnoloogiate efektiivsuse tõstmiseks autor esitab järgmised ettepanekud:

1. Turvalisuse tõstmiseks peavad kõik reisidokumendid muutma biomeetrilisteks, et illegaalidel ei oleks võimalust võltsida teisi reisidokumente, mille võltsimise protsess on lihtsam.
2. Uute tehnoloogiate arenguprotsess, mis aitab tõsta reisidokumentide turvalisust, peab olema pidev ja jätkuv.
3. Turvalisuse tõstmiseks ning manipuleerimise tehnikaga vältimiseks inimese ja tehnoloogiate nn koostöö peab tingimata jätkuma ja arenema.
4. Biomeetriliste tehnoloogiate efektiivsuse tõstmiseks on mõistlik kasutada erinevaid biomeetrilisi seadmeid juba I astme kontrollis.
5. On mõistlik organiseerida rohkem koolitusi, mis puudutavad biomeetrilise valdkonna, II astme kontrolli spetsialistide jaoks.

Edaspidise perspektiivi mõttes, antud töö jätkamiseks pakub autor välja uurida täpsemate skaneerimise ja identifitseerimise süsteemide arengut, et võimalikult minimaliseerida isikute tuvastamise eksimuste protsenti. Kuna juba praegu üritatakse manipuleerida kiibi andmetega e-dokumentidel ning kindlasti hakatakse seda tegema ka edaspidi on vajalik alustada tehnoloogiate väljatöötamist, mis aitavad vältida elektroonilistes kiipides olevat informatsiooni sanktsioneerimata muutmist. Selles aitab kaasa kaasaaegsete infotehnoloogiate arendamine. Samuti ei tasu unustada seda, et elektroonilise kiibi laitmatuks funktsioneerimiseks, peab pidevalt täiustama kiibi kvaliteeti, töövõimekust ja töökindlust.

Biomeetria kasutamine annab meile usaldusväärsust ja turvalisuse tunnet. Ja biomeetriasse tuleb suhtuda mitte nagu inimese vabaduse ja identiteedi kallale kippumisele, aga tema turvalisusele.

РЕЗЮМЕ

Биометрия - это популярная наука, чьи методы помогают сделать защиту государства более надёжной, а так же уменьшить количество преступлений и правонарушений. Целью данной дипломной работы было исследовать безопасность биометрических документов.

Для достижения цели было проведено экспертное интервью среди специалистов по контролю документов второго уровня в пограничных пунктах Таллинна, Нарвы, Койдула, и Лухамаа. Результаты интервью были сравнены между собой и проанализированы. На их основании были сделаны выводы и дальнейшие предложения по использованию биометрии в проездных документах. В ходе интервью был получен обзор о использовании биометрии в проездных документах, и связанных с этим позитивных и негативных сторонах. Результаты эмпирической части данной работы показали, что использование биометрических технологий во всех проездных документах является эффективным методом сделать страны-члены Евросоюза, и в том числе Эстонию, безопаснее. А также, изменение всех проездных документов на биометрические проездные документы поможет уменьшить количество попыток вторжения нелегалов на территорию Эстонии.

Для дальнейшего развития данной работы автор предлагает исследование развития ещё более точных систем сканирования биометрических паспортов и распознавания личности. Это необходимо для того, чтобы процент вероятности ошибочной идентификации личности уменьшить до минимума или исключить полностью.

VIIDATUD ALLIKATE LOETELU

2006. Doc 9303. Machine Readable Travel Documents. Part 1. Vol 2. International Civil Aviation Organization publication.

Ashbourn, J. 2000. Biometrics. Advanced Identity Verification. The Complete Guide. Springer publication.

Biomeetrilised reisidokumendid (e-passid). Politsei- ja Piirivalveameti kodulehelt http://politsei.ee/et/nouanded/dokumentide-naidised/Eesti-biomeetrilised-reisidokumendid.dot välja otsitud 11.12.2010.

Cutchberson, M., Mercer, J., Warner, P. 2008. Biometrics. Journal of Documents & Identity, 27, 12-15.

Document: EST-AD-01002. Euroopa Liidu Nõukogu PRADO kodulehelt http://www.consilium.europa.eu/prado/ET/3047/docHome.html välja otsitud 28.12.2010.

Elamisluba. Politsei- ja Piirivalveameti kodulehelt http://www.politsei.ee/et/teenused/elamisluba/ välja otsitud 02.04.2012.

Ida prefektuuri piirivalvebüroo teenistujate ametijuhendite kinnitamine. Kinnitatud Ida prefektuuri prefekti käskkirjaga 17.12.2010, kättesaadav „Postipoiss“ andmebaasis, välja otsitud 26.04.2012.

Integrated Automated Fingerprint Identification System. Föderaal Juurdlus Büroo kodulehelt http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis välja otsitud 17.03.2012.

Isikuandmete kaitse seadus 15.02.2007, jõustunud 01.01.2008 – RT I 2007, 68, 421

Isikut tõendavate dokumentide seadus 15.02.1999, jõustunud 01.01.2000 – RT I 1999, 25, 365... RT I, 29.12.2011,1

Jain, A., Bolle, R., Pankanti, S. 2006. Biometrics Personal Identification in Networked Society. Springer publication.

Karton, I., Kratovotš, M., Plaks, P., Talmar, A. 2011. Üliõpilastööde koostamise ja vormistamise juhend. Publitseerimata raamat. Sisekaitseakadeemia, Tallinn.

Лакин, Г. 1990. Биометрия. Издание четвёртое, переработанное и дополненное. Москва Высшая школа.

Lall, A. 2010. Kuritegude jälgede kriminalistikaline uurimine. Sisekaitseakadeemia kirjastus.

Li, S., Jain, A. 2009. Encyclopedia of Biometrics (Vols 1-2, pp 62, 81, 438, 677-678, 715, 810-811, 1091, 1128, 1411). Springer publication.

Liikmesriikide poolt väljastatud passide ja reisidokumentide turvaelementide ja biomeetria standardid. Vastu võetud Nõukogu määrusega 13.12.2004, jõustunud Eestis 29.12.2004

Lion, R. 2005-2006. Introduction. Technology landscrape. Keesing. Journal of Documents & Identity, 3-5.

Lion, R. 2007-2008. The p(l)ains of 2007. The mountains ahead. Keesing. Journal of Documents & Identity, 7-9, 11-13.

Modi, S. 2011. Biometrics in Identity Management: Concepts to Applications. Artech House publication.

Naan, G. 1985. Eesti nõukogude entsüklopeedia (2. trükk, lk 549). Kirjastus Valgus.

Прохоров, А.1978. Большая Советская Энциклопедия. Третье издание.

Siciliano, M. 2009. The HII-point in our future. ICAO MRTD REPORT, 4 (1), 19-20.

Tabur, L., Koort, E. 2010. Turvalisuspoliitika 2010. Kokkuvõte "Eesti turvalisuspoliitika põhisuunad Aastani 2015" täitmisest. Sisekaitseakadeemia kirjastus.

Viisad. Kes võivad viisavabadusprogrammi raames reisida? Ameerika Ühendriikide suursatkonda kodulehelt http://estonian.estonia.usembassy.gov/whois_est.html välja otsitud 24.04.2011.

Viisavaba reisimine Eestisse. Eesti Vabariigi välisministeeriumi kodulehelt http://www.vm.ee/?q=node/4850 väljaotsitud 29.03.2012.

Ворона, В., Тихонов, В. 2010. Системы контроля и управления доступом. Горячая линия – Телеком.

Välismaalase seadus 09.12.2009, jõustunud 01.10.2010 – RT I 2010, 22, 108, RT I 2010, 34, 184, RT I 2010, 41, 240

LISA 1. EKSPERTINTERVJUU KAVA

Hea vastaja!

Palun Teie abi uurimuse "Biomeetria ja biomeetrilised reisidokumendid" läbiviimisel. Intervjuu peamine eesmärk on saada ülevaade biomeetria kasutamisest reisidokumentides ja sellega seotud positiivsetest ja negtiivsetest külgedest.
Samuti soovin saada Teie arvamust antud valdkonnas positivsete külgede ja puuduste kohta.

Tegemist on struktureeritud süvaintervjuuga, mille käigus esitatakse intervjueeritavale kokku 13 küsimust. Süvaintervjuus kasutatakse vastaja vastuseid uuritavasse temaatikasse sügavamale sukeldumiseks, ehk küsimuste vahele võivad tulla täiendavad või täpsustavad küsimused.

Käesoleval uurimusel on ainult teaduslikud eesmärgid. Intervjuu on anonüümne ehk uurimustöö käigus ei avaldata Teie nime ega personaalseid isikuandmeid.

Ette tänades
Veronika Kiprejeva

1. Kui kaua Teie töötate dokumendieksperdina?
2. Milline on Teie ametialane haridus?
3. Kas biomeetriliste reisidokumentide sisseviimine vähendas dokumentide võltsimist?
4. Kas biomeetrilisi reisidokumente on võimalik võltsida?
5. Kui jah, siis kuidas, kui ei, siis miks?
6. Kas Teie praktikas oli piiriületajate poolt kasutatud võltsitud biomeetrilisi dokumente?
7. Kas biomeetrilised tehnoloogiad aitavad suurendada dokumentide turvalisust?
8. Kas Teie piiripunktis on olnud illegaalse sisserände tõkestamise juhtumeid?
9. Kui palju illegaalidest kasutasid biomeetrilisi reisidokumente?
10. Mitu illegaali oli Teil võimalik piiriületajate hulgast tuvastada kasutades biomeetrilisi andmeid?
11. Kas Teie arvates biomeetriliste tehnoloogiate kasutamine reisidokumentides on efektiivne?
12. Kas automaatse elektroonilise piiriületuse süsteemi (Automated Border Control systems (ABC süsteemi)) sisseviimine Teie piiripunktis tõstaks EL riikide turvalisust?
13. Kas Te soovite midagi lisada või soovitada biomeetriliste tehnoloogiate kasutamise/rakendamise kohta reisidokumentides?

Suur tänu Teile!