MYKOLO RIOMERIO UNIVERSITETAS
EKONOMIKOS IR FINANSŲ VALDYMO FAKULTETAS
INFORMATIKOS IR STATISTIKOS KATEDRA

VIOLETA KRASAUSKAITĖ

BIOMETRINIS SIENŲ SAUGUMAS: E. SIENA IR LIETUVA ŠENGENO ERDVĖJE

Magistro baigiamasis darbas

Vadovas:
prof. dr. A. Augustinaitis

VILNIUS, 2008

MYKOLO RIOMERIO UNIVERSITETAS
EKONOMIKOS IR FINANSŲ VALDYMO FAKULTETAS
INFORMATIKOS IR STATISTIKOS KATEDRA

BIOMETRINIS SIENŲ SAUGUMAS: E. SIENA IR LIETUVA ŠENGENO ERDVĖJE

Elektroninės valdžios administravimo magistro baigiamasis darbas
Studijų programa 62603F204

Vadovas
prof. dr. A. Augustinaitis
2008 12

Recenzentas

Atliko
EVAmn7-01 gr. stud.
V. Krasauskaitė
2008 12 05

VILNIUS, 2008

TURINYS

LENTELĖS

PAVEIKSLAI

PRIEDAI

ĮVADAS

Temos aktualumas ir naujumas: Valstybių sienos samprata – tokia, kokia ji mums buvo iki šiol pažįstama – pasikeitė, kadangi technologiniai bei globalizacijos procesai sąlygoja pasikeitusią sienos suvokimo paradigmą: atsiranda nauji reikalavimai, pakinta sienos saugumo funkcijos kai kalbama apie perėjimą nuo fizinio prie informacinio ir technologinio sienų saugumo. Transformuojasi pati sienos koncepcija, keičiasi regioninio saugumo užtikrinimo metodai, o tai sąlygoja e.sienos sampratos atsiradimą, todėl iškyla būtinybė naujai spręsti sienos saugumo užtikrinimo problemą, kadangi e.siena įsitraukia jau į e.valdžios, e.paslaugų tyrimų sritį. Pagrįstai kyla klausimas, koks e.sienos modelis efektyviausiai užtikrintų piliečių srautų kontrolę bei teritorinį saugumą. Todėl šiame baigiamajame magistro darbe yra sukuriamas e.valdžios biometrinės e. sienos sprendimų realizacijos Lietuvai modelis.

21-ojo amžiaus pasaulis yra kuriamas atvirumo ir judrumo pagrindu, kuomet žmonių, informacijos, prekių ir pinigų srautai tampa neatsiejamu globalios visuomenės pamatu. Tačiau tokie srautai kuria ne tik visapusišką bendradarbiavimą pasauliniu mastu, bet ir naujus pavojus, kurių neigiamas poveikis nebėra izoliuotas ir gali turėti gilių ir skaudžių padarinių visame pasaulyje. Įvairūs neigiami faktoriai – nusikaltėliai, narkotikų karteliai, organizuoto nusikalstamumo sindikatai ar teroristų grupės gali išnaudoti pernelyg atvirą sistemą ir anonimiškumą, taip inicijuodami neteisėtą ir žalingą veiklą.

Nuo 2007 m. gruodžio 21 d. Lietuva, kaip ir kitos naujosios Europos Sąjungos šalys[1] tapo Šengeno erdvės nare, iš viso sudarydamos 24 šalių tinklą (iš kurių dvi – ne ES narės). Tai reiškia, kad buvo panaikinta vidinės sausumos ir jūrų sienų kontrolė, oro sienas panaikinant nuo šių metų kovo 31 d. Šengeno erdvės atsivėrimas lėmė tai, kad nuo šiol Europos Sąjungos valstybes skiriančių vidinių sienų ir Lietuvos piliečiai per 23 Šengeno erdvei priklausančias šalis gali važiuoti taip, kaip šiuo metu važiuoja per Lietuvos savivaldybių ribas – nestabdomi, be asmens tapatybės dokumentų patikrinimo ar vizų. Tačiau Šengenas turi garantuoti ne tik atviras sienas, bet ir užtikrinti pakankamą saugumą, todėl vis labiau pripažįstama, kad nuo kryptingos ES išorinių sienų apsaugos politikos ir nuolatinės kokybiškos kontrolės priklauso kiekvienos valstybės ir jos piliečių saugumas. Tai – bendra visų ES valstybių atsakomybė, kuri įgyvendinama e.valdžiai pasitelkiant biometrines saugumo užtikrinimo priemones, nes sienos valdymo institucijos vis dažniau susiduria su strateginėmis problemomis, kurių sprendimas reikalauja pokyčių tradiciniame valstybės valdyme. Vadinasi, biometrinio sienų saugumo klausimas e.valdžios ir e.sienos kontekste tampa kaip niekad aktualus ir reikšmingas.

[1] Kitos į Šengeno erdvę kartu su Lietuva įstojusios šalys: Lenkija, Latvija, Estija, Čekija, Slovėnija, Slovakija, Vengrija ir Malta.

Problema: XXI a. pradžios saugumo iššūkiai paskatino naujų asmens identifikavimo metodų taikymą bei politines ir akademines diskusijas dėl asmens biometrinių duomenų naudojimo, kaupimo ir saugojimo metodų suderinamumo su jau išplėtotais žmogaus teisių standartais. Darbe keliama problema: su kokiais naujais iššūkiais susiduriama sprendžiant spartų biometrinių technologijų plėtros ir jų taikymo klausimą, nes biometrinėms technologijoms teikiama politinė svarba reikalauja atidaus jų nagrinėjimo duomenų apsaugos požiūriu.

Darbo objektas: Biometrinis sienų saugumas e.valdžios ir e.sienos kontekste, atsižvelgiant į Šengeno erdvės politiką ir susitarimus.

Darbo tikslas: Ištirti biometrinių duomenų panaudojimo galimybę realizuojant e.sienos koncepciją, užtikrinant sienų saugumą. Taip pat darbe siekiama išanalizuoti biometrinių duomenų naudojimo aspektus bei jų sąsajas su duomenų apsaugos reikalavimais, įvertinti biometrinio sienų saugumo užtikrinimo būklę, plėtros kryptis, akcentuojant kitų šalių teikiamas e.paslaugas pasienyje bei pateikiant pasiūlymus dėl efektyvesnio jų taikymo Lietuvoje.

Darbo hipotezė: Šiuo darbu siekiama pagrįsti, kad egzistuoja tiesioginis sąryšis tarp biometrinių sienų saugumo ir e.valdžios politikos projekcijų sienų saugumo klausimais. Iškeliama prielaida, kad tik tokia sienų saugumo politika būtų tinkama ir efektyvi, kuri skatintų efektyvų piliečių judėjimą, tačiau nesukeltų papildomo pavojaus. *Individualizuojant bei optimizuojant asmeninės informacijos apie piliečius įvedimo procesą – pakeičiant jį automatizuotu biometrinių duomenų nuskaitymo procesu – galima realizuoti biometrinio saugumo e.sienos koncepciją Lietuvoje ir užtikrinti e.valdžios nacionalinio tinklo viešojo administravimo efektyvumą.* Atsižvelgiant į šią hipotezę, formuluojami tokie **darbo uždaviniai:**

1) Ištirti biometrijos sąsajas su e. sienos koncepcija;
2) Aptarti naudojamas biometrinių duomenų technologijas;
3) Ištirti užsienio valstybių e.valdžios panaudojimo praktiką užtikrinant valstybės saugumą;
4) Nustatyti Lietuvos dalyvavimo e.sienos kūrime pagrindines kryptis.
5) Atlikti VSAT valstybės sienos apsaugos įvertinimo netiesioginį tyrimą.
6) Sukurti integruotą Lietuvos biometrinės e.sienos modelį ir rekomendacinius pasiūlymus LR vyriausybei.
7) Nubrėžti e.sienos diegimo Lietuvoje rekomendacines gaires.

Darbe naudoti metodai: šiame baigiamajame darbe visa informacija analizuojama ir vertinama naudojant loginės, statistinės, istorinės, palyginamosios (skirtingų laikotarpių rezultatų palyginimo) ir tendencijų analizės metodus. Empirinei analizei atlikti naudotasi Valstybės kontrolės auditorių medžiaga, VRM vidinio naudojimo dokumentais. Taip pat buvo analizuoti tarptautiniai Šengeno erdvės teisės aktai, valstybinių institucijų informacinių sistemų rezultatai, SIS sistemos veikimas.

Teisinių dokumentų analizės metodas taikytas nagrinėjant įvarius Lietuvos ir užsienio šalių šaltinius, siekiant visapusiškai atskleisti Lietuvos priklausymo Šengeno erdvei aspektus. Teminių sprendimų požiūrių buvo susipažinta su Aleksandro Ivanovo darbu „E. valdžios taikymas valstybės sienos apsaugoje“, siekiant išnagrinėti e.sienos koncepcinį modelį bei e.paslaugų e.sienoje realizavimo ypatumus, kritiškai įvertinant, bet nedubliuojant aukščiau minimo autoriaus požiūrio, kadangi iškyla būtinybė atskleisti menkai išgvildentą e.sienos bei e.valdžios tarpusavio sąveiką.

Darbo praktinė reikšmė: Elektroninės valdžios taikymas pastaruoju metu yra viena iš svarbiausių, daugelio pasaulio vyriausybių strategijos dalis. Pagrindiniai e.valdžios uždaviniai yra aprūpinimas priėjimu prie valstybinių informacinių išteklių, viešųjų paslaugų gerinimas, viešųjų valdymo organų veiklos efektyvumo didinimas, demokratinių principų konsolidavimas. Daugelio šalių vyriausybės įžvelgia didelę naudą pereinant nuo viešųjų paslaugų teikimo įprastais būdais (daugeliu atvejų grįstų tiesioginiu bendravimu bei popierinių formų pildymu) prie viešųjų paslaugų teikimo elektroninėmis formomis.

Įvairiose šalyse atlikti tyrimai rodo, kad daugelis paslaugų, pradėjus jas teikti elektronine forma, pateikė labai gerų rezultatų ir ne tik pagerino paslaugos teikimą, bet ir leido sumažinti paslaugų teikimo kaštus. Prie bendros Šengeno informacinės sistemos prisijungę šalies pareigūnai gali greičiau keistis informacija apie nusikaltimus, pavogtus daiktus, ieškomus nusikaltėlius (jų biometrinius duomenis) ir efektyviau kovoti su nelegalia migracija, tarptautiniu nusikalstamumu, automobilių vagystėmis, narkotikų ar ginklų kontrabanda. Kadangi Lietuva neturi vientisos biometrinių kontrolės postų sistemos, šiame darbe, remiantis VRM duomenimis, valstybės kontrolės ataskaitomis, konferencijų, kursų bei seminarų medžiaga, yra sukuriamas e.sienos biometrinių postų sistemos Lietuvoje integruotas (SIS) modelis. Tokio pobūdžio darbas Lietuvoje yra pirmas, nes jame yra suprojektuojama integruota su SIS pasienio kontrolės postų biometrinė e. sienos sistema.

Darbo struktūra: Magistrinis dabas susideda iš trijų dalių: teorinės, analitinės ir projektinės.

Teorinėje darbo dalyje nagrinėjami ES elektroninės valdžios integruotų e.sienų valdymo ir biometrinio saugumo aspektai, akcentuojama informacinės visuomenės svarba. Detaliau aptariama integruota Europos sienų valdymo strategija bei išplėstas integruotas sienų valdymas: nacionalinio tinklo įtaka sienos vadybai, rizikos valdymas. Išskirtinis dėmesys skiriamas Lietuvos Šengeno erdvėje pozicijai ištirti. Plačiau apžvelgiamas Šengeno (*acquis*) teisynas, informacinė sistema ir jos paskirtis, „EURODAC“ bei vizų informacinės sistemos (VIS) analizė bei biometriniai pasai bei jų taikymo problemos Lietuvoje.

Analitinėje darbo dalyje aptariama e.sienos integruoto valdymo praktinė realizacija, biometrinių perimetro saugos sistemų realizavimo ypatumai ES bei pasaulio šalių praktikoje. Išanalizuojamas efektyvios sienos kontrolės užtikrinimo projektas, detaliau aptariant e.sienos paskirtį bei vaidmenį užtikrinant biometrinį perimetro saugumą e.sienos kontrolės kontekste. Atliekama biometrinės

sistemos analizė, išanalizuojamos biometrinės operacijos, duomenų apdorojimo etapai, ištiriamas biometrijos sistemų funkcionalumas ir efektyvumas; pritaikomumas pasienio kontrolėje. Analitinės darbo dalies pabaigoje pateikiama e.sienos integruoto valdymo praktinė realizacija.

Projektinėje darbo dalyje aptariamos biometrinio saugumo e.valdžios įgyvendinimo Šengeno erdvėje problemos diegiant e.valdžios e.sienos paslaugą Lietuvoje . Apžvelgiami elektroninės valdžios e.paslaugų administravimo aspektai informacinės visuomenės kontekste bei pateikiami sprendimai dėl biometrinės saugumo SIS e.valdžios koncepcijos įgyvendinimo Šengeno erdvėje bei problemos diegiant e.sienos paslaugą Lietuvoje. Atliekamas VSAT valstybės sienos apsaugos įvertinimo netiesioginis tyrimas bei pasiūloma e.valdžios biometrinės e.sienos sprendimų realizacija, pateikiami pasiūlymai bei rekomendacijos.

Darbe vartojami sutrumpinimai:

ES	Europos Sąjunga
LR	Lietuvos Respublika
VRM	Vidaus reikalų ministerija
ŠK	1990 m. birželio 19 d. Konvencija dėl Šengeno susitarimo įgyvendinimo
SIS	Šengeno informacinė sistema
N.SIS	Nacionalinė Šengeno informacinė sistema
C.SIS	Centrinė Šengeno informacinė sistema
SIRENE	Papildoma informacija nacionaliniams perspėjimams
LKPB TRV	Lietuvos kriminalinės policijos biuro Tarptautinių ryšių valdyba
VSAT URC	Valstybės sienos apsaugos tarnybos prie Vidaus reikalų ministerijos Užsieniečių registracijos centras
Šengeno *acquis*	Teisės aktų, susijusių su Šengeno susitarimo nuostatų įgyvendinimu, visuma
VIS	Vizų informacinė sistema
IVPK	Informacinės visuomenės plėtros komitetas prie Lietuvos Respublikos Vyriausybės
VDAI	Valstybinė duomenų apsaugos inspekcija

1. ES ELEKTRONINĖS VALDŽIOS INTEGRUOTŲ E. SIENŲ VALDYMO BIOMETRINIO SAUGUMO ASPEKTAI INFORMACINĖS VISUOMENĖS KONTEKSTE

1.1. Integruota Europos sienų valdymo strategija: dabartinė padėtis bei esamos priemonės

Didėjant asmenų judėjimui Europos Sąjungai iškyla uždavinys, kaip sudaryti sąlygas sąžiningiems keliautojams greitai kirsti sienas, palengvinti jiems atvykimą ir kartu didinti saugumą. Siekiant išspręsti šį uždavinį reikės toliau visapusiškai plėtoti Europos Sąjungos integruotą sienų valdymo strategiją, atsižvelgiant į naujųjų technologijų galimybes. Galimybė plačiai, nuosekliai ir proporcingai naudotis naujosiomis technologijomis, nustatyti sistemų sąsajas, kad būtų galima kuo veiksmingiau taikyti šias technologijas, yra svarbiausias integruotos sienų valdymo strategijos vidutinės trukmės laikotarpio elementas. Reikia laipsniškai įgyvendinti tai, kas jau suplanuota bei nuspręsta ir kartu plėtoti esamomis iniciatyvomis pagrįstą ilgalaikę strategiją.

Paskelbtame komunikate „Pasirengimas kitiems Europos Sąjungos sienų valdymo etapams“[2] teikiami pasiūlymai dėl naujų priemonių, kurios ateityje bus neatsiejama Europos sienų valdymo dalis, įskaitant:

- pasiūlymus dėl atvykimo ir išvykimo sistemos, kuri leistų elektroniniu būdu registruoti trečiųjų šalių piliečių atvykimo į Šengeno erdvę ir išvykimo iš jos datas,
- pasiūlymus palengvinti sienų kirtimą sąžiningiems keliautojams, įdiegus automatizuotas sienos kirtimo priemones ES piliečiams ir trečiųjų šalių tam tikrų kategorijų piliečiams,
- elektroninio kelionės leidimo sistemos galimo diegimo parametrus.

Europa yra ir ateityje bus turistų lankomiausia vieta pasaulyje. ES-27 išorės sienos nustatytuose sienos kirtimo punktuose per metus kertamos apie 300 mln. kartų (t.y. maždaug 150 mln. kartų atvykstama į ES ir 150mln. kartų iš jos išvykstama). Manoma, kad iš jų apie 160 mln. kartų sienas kerta ES piliečiai, 60 mln. – trečiųjų šalių piliečiai, kuriems nereikia vizos, ir 80mln. – trečiųjų šalių piliečiai, kuriems reikia vizos. Šiuo metu Eurostatas teikia tik oficialiuosius duomenis. Tačiau šie duomenys pagrįsti nakvynių skaičiumi.

Valstybių narių pateiktais duomenimis, 2005m. ES-27 išorės sienos kirstos 880 mln. kartų, o

[2] Darbo dokumentas Nr. 1dėl Komisijos komunikato COM(2008) 0069 Pasirengimas kitiems Europos Sąjungos sienų valdymo etapams. Piliečių laisvių, teisingumo ir vidaus reikalų komitetas: http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dt/744/744600/744600lt.pdf; prisiingimo laikas: 2008-11-22

2006m. – 878 mln. kartų. Valstybės narės nuosekliai neregistruoja tokio judėjimo, todėl skaičiai pagrįsti apytiksliais skaičiavimais arba pasirinktinai atliktais pavieniais patikrinimais. Nežinoma, kiek kartų sienas kirto trečiųjų šalių piliečiai.

Manoma, kad 2006m. ES buvo iki 8 mln. nelegalių imigrantų. Apskaičiuota, kad 80% jų buvo Šengeno erdvėje. Manoma, kad daugiau nei pusė nelegalių imigrantų į ES atvyksta teisėtai, bet tampa nelegaliais imigrantais pasilikę ilgiau nei leistina.

2006m. ES buvo sulaikyta apie 500000 (2005m. – 429000, 2004m. – 396000) nelegalių imigrantų. Apskaičiuota, kad apie 40% iš jų buvo išsiųsta.

Nacionaliniu lygmeniu surinktais duomenimis, daugiau kaip 75% nelegalių migrantų, sulaikytų valstybių narių teritorijoje 2006m., buvo iš trečiųjų šalių, kurių piliečiams kelionei į ES privalomos vizos. Taigi tikėtina, kad dauguma užsibuvusių asmenų yra iš šių trečiųjų šalių.

Vykdant pasienio kontrolę tikrinama tapatybė ir įvairiose duomenų bazėse ieškoma informacijos apie asmenis, kuriuos reikia sulaikyti arba neleisti jiems atvykti į šalį. Radus tokių duomenų, asmeniui gali būti uždrausta atvykti į ES. 2006m. daugiau kaip 300000 (2005m. – 280000, 2004m. – 397000) asmenų ES pasienyje buvo uždrausta atvykti. Dauguma šių asmenų buvo iš trečiųjų šalių, kurių piliečiams privalomos vizos. Tai galima palyginti su apytiksliai apskaičiuotu 70mln. trečiųjų šalių piliečių (turinčių vizas ir jų neturinčių) atvykimu į ES; vidutiniškai keturiems iš tūkstančio pasienyje uždraudžiama atvykti į šalį. Daugelis asmenų, kuriems uždraudžiama atvykti, neturi tinkamų kelionės dokumentų, be to, kyla įtarimų, kad jie ateityje gali tapti nelegaliais imigrantais.

Yra pagrindo manyti, kad daug keliautojų kerta sieną dažniau nei du kartus per metus ir kad maža dalis sienos kirtimo atvejų tenka dažnai keliaujantiems asmenims. Pavyzdžiui, tikėtina, kad verslo tikslais keliaujantys ES ir trečiųjų šalių piliečiai, mokslininkai ir jų techninis personalas, studentai, ES piliečiai, turintys artimų šeimos ryšių su trečiosiomis šalimis, trečiųjų šalių piliečiai ir ES piliečiai, gyvenantys ES pasienio regionuose, per metus kerta sieną daug kartų. Apskaičiuota, kad apie 20% sienų kirtimo atvejų tenka dėl Šengeno erdvės vizų išdavimo besikreipiantiems trečiųjų šalių piliečiams, kurie reguliariai keliauja ir jiems reikia daugkartinių vizų.

Dažniausiai išorės sienos kertamos oro uostuose. Antri pagal dažnumą – sausumos sienos kirtimo punktai. ES yra 1792 išorės sienos kirtimo punktai, kuriuose vykdoma kontrolė (665 – prie oro sienų, 871 – prie jūrų sienų ir 246 – prie sausumos sienų).

Kalbant apie integruotą sienų valdymo sąvoką, reikia pabrėžti, kad šioji sąvoka apima kontrolės mechanizmų ir priemonių, pasirenkamų pagal asmenų srautus ES link arba į ją, derinimą. Ši sąvoka apima priemones, taikomas valstybių narių konsulatuose trečiosiose šalyse, taip pat priemones, taikomas bendradarbiaujant su kaimyninėmis trečiosiomis šalimis, priemones, taikomas prie pačios sienos, ir priemones, taikomas Šengeno erdvėje. Šiuo metu pagrindiniai šią sąvoką sudarantys elementai – toliau minimos priemonės, taikomos trečiųjų šalių piliečiams, keliaujantiems į Šengeno

bendradarbiavimo sistemai priklausančią valstybę narę arba prie tokio bendradarbiavimo prisijungusią šalį.

Kaip nustatyta Bendrijos teisėje, keliautojams iš tam tikrų trečiųjų šalių privalomos vizos[3]. Pirmasis šios kategorijos asmenų patikrinimas dėl atvykimo ir buvimo šalyje sąlygų atitikimo susijęs su prašymu išduoti vizą ir atliekamas valstybių narių konsulatuose trečiosiose šalyse.

Trumpalaikę vizą pageidaujantys gauti trečiųjų šalių piliečiai bus tikrinami naudojantis Vizų informacine sistema (VIS), kuri visu pajėgumu pradės veikti (tai taip pat reiškia, kad ji bus įdiegta konsulatuose ir sienos kirtimo punktuose) ne anksčiau kaip 2012m. 2007m. Europos Parlamentas ir Taryba pasiekė politinį susitarimą dėl VIS teisinio pagrindo ir tikimasi, kad jis oficialiai bus priimtas pirmąjį 2008m. pusmetį. Pagrindinė VIS paskirtis asmenims atvykstant – patikrinti vizos autentiškumą ir jos turėtojo tapatybę. Biometriniai identifikatoriai – veido atvaizdas ir pirštų atspaudai – į VIS bus įvedami nuo pat jos veikimo pradžios. Komisija pateikė pasiūlymą iš dalies pakeisti Šengeno sienų kodeksą taip, kad vizos turėtojo tapatybę būtų privaloma tikrinti kiekvienąkart asmeniui atvykstant.

Asmenų, į ES keliaujančiu oro transportu, duomenys, atitinkantys paso duomenis, paskirties valstybės narės prašymu, kaip išankstinė informacija apie keleivius perduodama prieš įlaipinimą arba jo metu, siekiant perspėti sienos apsaugos tarnybas apie keleivius, galinčius kelti grėsmę[4]. Išankstinė informacija apie keleivius negali būti naudojama siekiant neleisti asmeniui atvykti į paskirties valstybės narės sienos perėjimo punktą.

Pagal Šengeno sienų kodeksą[5] atvykstantys trečiųjų šalių piliečiai turi būti „nuodugniai patikrinami“, t.y. turi būti patikrinamas ne tik jų kelionės dokumentas, bet ir atvykimo tikslas bei buvimo šalyje trukmė, taip pat tai, ar jie turi pakankamai pragyvenimo lėšų. Be to, asmenų duomenis reikia patikrinti Šengeno informacinėje sistemoje ir nacionalinėse duomenų bazėse ir nustatyti, ar jie nekelia grėsmės Šengeno valstybių viešajai tvarkai, vidaus saugumui, visuomenės sveikatai ir tarptautiniams santykiams. Taigi sienos apsaugos pareigūnas, užduodamas tam tikrus klausimus keleiviui, tikrina, ar jis atitinka nustatytas sąlygas. Be to, sienos apsaugos pareigūnas kiekvienu atveju turi patikrinti, ar tebegalioja kelionės dokumentas. Asmenys tikrinami vienodai, nepaisant, ar jiems privalomos vizos. Sienos apsaugos pareigūnai įpareigoti išorės sieną kertančių trečiųjų šalių piliečių kelionės dokumentuose dėti atspaudus su atvykimo ir išvykimo datomis bei vieta.

Konsulatuose ir pasienyje duomenys tikrinami Šengeno informacinėje sistemoje (SIS) – ar jokia

---

[3] Reglamentas (EB) Nr.539/2001 nustatantis trečiųjų šalių, kurių piliečiai, kirsdami išorines sienas, privalo turėti vizas, ir trečiųjų šalių, kurių piliečiams toks reikalavimas netaikomas, sąrašus. Prieiga per internetą: http://eur-lex.europa.eu/Notice.do?mode=dbl&lang=en&ihmlang=en&lng1=en,lt&lng2=bg,cs,da,de,el,en,es,et,fi,fr,hu,it,lt,lv,mt,nl,pl,pt,ro,sk,sl,sv,&val=258858:cs&page=

[4] Direktyva 2004/82/EB 2004 m. balandžio 29 d. dėl vežėjų prievolės teikti su keleiviais susijusius duomenis. Prieiga per internetą: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:261:0004:0004:LT:PDF

[5] EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS (EB) Nr. 562/2006 2006 m. kovo 15 d. nustatantis taisyklių, reglamentuojančių asmenų judėjimą per sienas, Bendrijos kodeksą (Šengeno sienų kodeksas) OLL105, 2006413, p.1. Prieiga per internetą: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0001:0032:LT:PDF

valstybė narė nėra nurodžiusi, kad konkrečiam asmeniui uždrausta atvykti. SIS ir būsimoje SISII registruojami su trečiųjų šalių piliečiais susiję perspėjimai dėl asmenų, kuriems uždrausta atvykti į Šengeno erdvę, ieškomų asmenų ir asmenų, kuriems turi būti skirta apsauga. Visi trečiųjų šalių piliečiai, nepaisant, ar jiems privalomos vizos, sistemingai tikrinami SIS.

Galiausiai taip pat reikėtų remtis oro transportu atvykstantiems asmenims taikomu Komisijos pasiūlymu dėl keleivio duomenų įrašo, kuris iš esmės atitinka skrydžio rezervavimo duomenis, naudojimo[6]. Ši informacija teisėsaugos institucijoms perduodama taip pat prieš pat įlaipinimą arba įlaipinimo metu. Ši sistema turėtų būti taikoma visose valstybėse narėse, nes ji nesiejama su Šengeno bendradarbiavimu. Keleivio duomenų įrašas perduodamas siekiant užkirsti kelią terorizmui ir organizuotam nusikalstamumui, o ne atlikti patikrinimus pasienyje.

Sienos kirtimo principai:

Trečiųjų šalių piliečiams: įdiegus automatizuotas pasienio kontrolės sistemas bus galima automatiškai tikrinti keliautojo tapatybę nedalyvaujant pasienio kontrolės pareigūnams. Įrenginys nuskaitytų biometrinius duomenis, esančius kelionės dokumente arba saugomus sistemoje ar duomenų bazėje, ir palygintų juos su keliautojo biometriniais duomenimis. Tai paspartintų pasienio kontrolę, nes būtų kelios automatizuotos juostos, kurios pakeistų tradicinius kontrolės namelius.

Registruoto keleivio statusas asmenims turėtų būti suteikiamas atlikus tinkamą patikrinimą, pagrįstą bendrais kontrolės kriterijais, įskaitant patikimumą ankstesnių kelionių metu (ankstesnių apsilankymų ES metu asmuo neturėtų būti viršijęs leidžiamos buvimo šalyje trukmės), pakankamų pragyvenimo lėšų įrodymą ir biometrinio paso turėjimą. Ribotą laiką (pavyzdžiui, penkerius metus arba vizos galiojimo laikotarpiu) valstybės narės turėtų nuolat stebėti, kaip laikomasi kontrolės kriterijų.

ES piliečiams: automatizuoti vartai prie išorės sienų gali būti įdiegti pagal dabartinę teisės sistemą (reikėtų tai skatinti). Per automatizuotus vartus galėtų vykti asmenys, turintys biometrinius pasus arba, kaip pereinamąją priemonę, tam tikrą lustinę kortelę, išduotą asmeniui prašant ir laikantis nacionalinių reikalavimų.

Europos elektroninio kelionės leidimo sistema:

Reikalavimas trečiųjų šalių piliečiams turėti elektroninį kelionės leidimą gali būti alternatyva reikalavimui turėti vizą arba šį reikalavimą galima būtų taikyti trečiosios šalies piliečiams, kuriems šiuo metu vizos neprivalomos. 2008m. Komisija ketina inicijuoti tyrimą tokios sistemos įgyvendinimui išnagrinėti.

Duomenų apsauga:

---

[6] Council framework decision on the use of Passenger Name Record (PNR) for law enforcement purposes. Brussels, 6.11.2007. COM(2007) 654 final
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0654:FIN:EN:PDF
.

Sistemos turi atitikti ES duomenų apsaugos taisykles, įskaitant būtinumo, proporcingumo, tikslo ribojimo ir duomenų kokybės reikalavimus. Visų pirma reikia stengtis užtikrinti visapusišką atitiktį Direktyvos 95/46/EB[7] 16 ir 17straipsniuose nustatytiems konfidencialumo ir saugumo reikalavimams, taip pat Reglamente(EB) Nr.45/2001 nustatytiems su tinklo saugumu ir konfidencialumu susijusiems reikalavimams. Būtų tikslinga taikyti VIS duomenų apsaugos taisykles ir išlaikyti *status quo*, įskaitant informacijos saugojimą tik penkerius metus.

Atvykimo ir išvykimo sistemoje surinktais duomenimis turėtų daugiausia naudotis kompetentingos imigracijos tarnybos. Asmenims turėtų būti užtikrinta teisė susipažinti su apie juos turima informacija ir ją užginčyti bei ištaisyti, kaip numatyta Bendrijos ir nacionalinėje teisėje. Reikėtų patvirtinti nuostatas, kuriose būtų numatytas apskundimo mechanizmas, taikytinas tais atvejais, kai trečiųjų šalių piliečiai yra priversti viršyti leistiną buvimo šalyje trukmę.

Registruotų keliautojų programai būtų taikomi tie patys Bendrijos teisėje nustatyti duomenų apsaugos reikalavimai. Vertėtų nustatyti duomenų apsaugos nuostatas, įskaitant teisę susipažinti su asmenine informacija, kuri naudojama neigiamam atsakymui į prašymą pagrįsti. Į Registruotų keliautojų programą taip pat turėtų būti įtrauktas reikalavimas, pagal kurį valdžios institucijos turi pateikti neigiamo atsakymo priežastis, ir numatyta galimybė pareiškėjams apskųsti neigiamą atsakymą.

1.2. Išplėstas integruotas sienų valdymas

Vyriausybės vadovams, kurie yra atsakingi už sienos vientisumo įvaizdį, tampa vis sudėtingiau vykdyti savo užduotis. Visame pasaulyje terorizmo grėsmė ir globalizacijos fenomenas įgyja naujas formas kalbant apie fundamentalų sienų pobūdį ir jų priežiūrą. Pirmaujančiose šalyse kontrolės operacijos dabar vykdomos ne tik fizinėje sienoje, bet ir prieš atvykstant į valstybės oficialų įvažiavimo punktą. Rezultatas: daug platesnis ir sudėtingesnis sienos kirtimo valdymas.

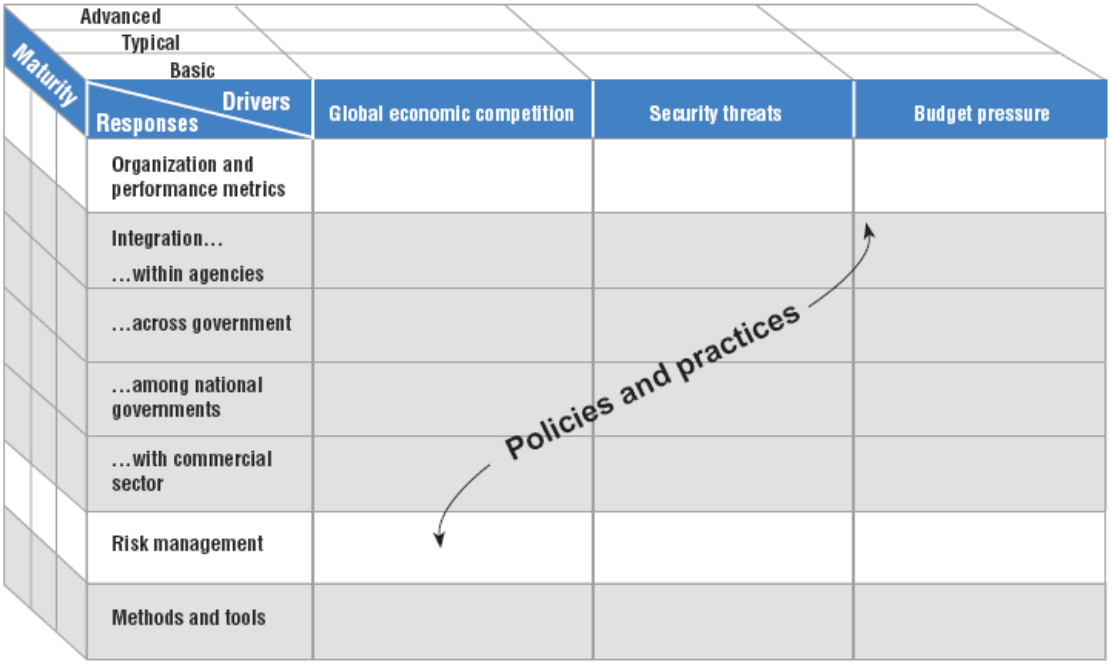
1.2.1. Nacionalinio tinklo įtaka sienos vadybai

Neatskiriamas prekybos, kelionės, sienos aplinkos ir plataus pagrindo sujungtų, heterogeninių sprendimų uždavinys – pavaizduoti suformuoto sienų kirtimo metodo strategijų reikalingumą, siekiant užtikrinti didesnį racionalumą ir sinchronizaciją.

Kad padėtų vyriausybėms jų strateginių sienos vadybos planų formuluotėje, IBM sukonstravo

[7] Europos parlamento ir tarybos direktyva (95/46/EB),1995 m. spalio 24 d. dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo.(OL L 281, 23.11.1995, p. 31)
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1995L0046:20031120:LT:PDF

trimatę struktūrą[8] (1 pav.).



pav. 1 Strateginių sienos valdymo planų trimatė struktūra

Šaltinis: IBM Institute for Business Value. Expanded borders, integrated controls. Achieving national prosperity and protection through integrated border management. http://www-935.ibm.com/services/us/imc/pdf/g510-6218-expanded-borders.pdf

Suformuota struktūra gali padėti vyriausybėms formuluoti integruotą sienos vadybos strategiją.

Vyriausybės gali panaudoti šią priemonę, kad nustatytų savo politikos etaloną ir išvystytų tinklą, pritaikytą integruotos sienos vadybos strategijos vykdymui.

Pirmas struktūros matmuo atspindi tris pagrindinius faktorius, įtakojančius sienos vadybos strategijas. Tai: globalinis ekonominis konkuravimas, terorizmo ir kitos neteisėtos veiklos pavojus, ir biudžeto ir darbo krūvio didėjimo grėsmė.

Antras matmuo į kategorijas suskirsto vyriausybinius sprendimus šiems faktoriams. Šių matmenų aplinkoje, struktūra dokumentuoja politikos ir praktikų spektrą, kurias vyriausybės įgyvendino, modernizuojant savo sienos vadybos programas. Programų diapazonas kiekvienoje aplinkoje yra klasifikuotas į trečią matmenį pagal brandos lygmenį: pagrindinės programos, tipiškos programos ir aukštesnės programos.

- *Pagrindinės programos* gauna įgaliojimą pagal tarptautinius standartus, ir yra būtinos sąlygos pažangesniam veikimui.
- *Tipiškos programos* yra bendrai naudojamos daugelio valstybių, atspindėdamos efektyvias technologijas.

[8] IBM Institute for Business Value. Expanded borders, integrated controls. Achieving national prosperity and protection through integrated border management. http://www-935.ibm.com/services/us/imc/pdf/g510-6218-expanded-borders.pdf

- *Pažangios programos* naudojamos pažangesnių valstybių. Šios programos dažnai būna išvystytos kaip optimalūs sprendimai prioritetiniams nacionaliniams tikslams siekti. Jos būtų visiškai įgyvendintos tik pateisinus nacionalinės politikos prioritetus.

Naudojant pateiktą struktūrą, vyriausybės gali atlikti praktikas, tinkamas jų aplinkai ir politikos prioritetams, ir suformuoti jas laipsniškame plane įgyvendinant integruotą nacionalinę sienos vadybos strategiją. Struktūra ir struktūros turinys gali padėti vyriausybėms išsiaiškinti tikslingus sienų valdymo kelius, identifikuoti tarpusavio ryšius ir priimti sprendimus, susietus su jų prioritetais.

Apžvalga, pasiūlyta sienos vadybos lyderių, parodytų šioje analizėje, kartu su tyrinėjimu ir patirtimi, siūlo reikšmingą pokytį vyriausybėms:

- *Integracija daugiau nebėra laisvai pasirenkama*. Teroristų tinklai ir kriminaliniai karteliai dabar naudoja pažengusias strategijas ir techniką, kuriai reikalingi koordinuoti, tarptautiniai sprendimai. Be to, prekybininkai ir keliautojai laukia integruotų elektroninių vyriausybinių paslaugų, panašių į pasiekiamas privačiame sektoriuje.
- *Kontrolė ir efektyvumas nėra privilegija*. Nors atrodo, kad saugumas ir sienos kirtimo supaprastinimas yra skirtingi dalykai, jie iš tikrųjų yra kaip dvi tos pačios monetos pusės. Kadangi daugumos valstybių patirtis parodė, kad sienos kirtimo ir jos saugumo bendras stiprėjimas gerina visa apimantį rizikos valdymą.
- *Kelionių, krovinių ir sienos vadybos disciplinos šalys gali pasimokyti viena iš kitos*. Pagrindinės praktikos ir tarptautiniai standartai, patobulinti vienoje srityje, gali būti panaudoti kaip modeliai kitiems, nes pagreitintų progresą ir lengvintų integraciją. Pavyzdžiui, standartinis turinys kelionėje ir imigracijos srityje gali išvystyti nurodymų komplektą, kuris atitinka WCO[9] Standartų Struktūrą, lengvinančią globalinę prekybą.
- *Būtinas suformuotas strategijos išsivystymo metodas*. Neatskiriamas prekybos, kelionės, sienos aplinkos problemiškumas ir plataus pagrindo sujungtų, heterogeninių atsakymų poreikis reikalauja suformuoto sienos vadybos strategijų metodo nacionaliniu lygmeniu.

Šiandien pavojai yra neatskiriami nuo žmonių ir prekių, įveikiančių sienas, srautų. Tačiau sienos kontrolės operacijos turi tapti efektyvesnės. Todėl gyventojai ir kompanijos laukia didesnės savo nacionalinių lyderių iniciatyvos ir sprendimų: jie iš vyriausybių laukia apsaugos, netrukdančios tarptautinei prekybai ir kelionei. Iš tikrųjų valstybių piliečiai tikisi klestinčios komercijos per meistriškai atliekamas vyriausybinių organų iniciatyvas, kurios greitintų legalią prekybą ir kelionę. Tai yra gąsdinanti misija – tokia, kuri reikalauja konkrečios ir patikimos integruotos sienos vadybos strategijos.

Globalinis ekonominis konkuravimas:

[9] Word customs organization. http://www.wcoomd.org/home.htm

Daugumai valstybių politinis ir ekonomikos stabilumas priklauso nuo dalyvavimo sudėtingame tarptautinės prekybos tinkle. Kai kurios šalys priklauso nuo pramoninių prekių eksporto, tuo metu, kai kitos klesti turizmo pagrindu. Kai kurioms šalims reikalingas žaliavų importas ar darbo jėga iš kaimyninių valstybių. Ir visos valstybės pasižymi skirtingomis ekonomikomis, paremtomis sudėtingu visų šitų elementų susimaišymu. Bet kokia forma, nacionalinių ekonominių tikslų pasiekimas yra patvari jėga, visur istorijoje akcentuojanti sienos vadybą.

Nacionalinis saugumas:

Nesenų teroro atakų tikrovė sustiprino gyventojų ir vyriausybių rūpestį nacionaliniu savo šalies saugumu. Nors terorizmas nebėra apribotas daugiau ties regioniniais karštaisiais taškais, jis prasiveržė penkiuose žemynuose, grasindamas visoms pasaulinėms rinkoms. Suprantama, vyriausybės nori apsaugoti keliautojus ir krovinius nuo šios didėjančios grėsmės, tačiau tuo pačiu metu vyriausybės turi tęsti rūpinimąsi prekių, keliaujančių tarptautinėmis tiekimo grandinėmis, saugumo ir vientisumo priežiūra, trukdydamos neteisėtam sienos kirtimui ir mažindamos kitus aktualius su sienos kirtimu susijusius klausimus, tokius kaip, pavyzdžiui, prekybą žmonėmis.

Operacijų efektyvumas:

Nepaisant siekio rūpintis nacionaliniais, ekonominiais ir saugumo tikslais, sienos vadybos sistemos operacijoms dažnai tenka apdoroti vis didesnės apimties prekių ir keliautojų srautą, be atitinkamo išteklių ar biudžeto padidėjimo. Naudojamo produktyvumo didėjimas yra kritiškas. Todėl vis didės reikalavimai vyriausybiniam efektyvumui, nes vyriausybės yra priverstos vykdyti atitinkamus socialinius įsipareigojimus, susijusius su jų senstančia populiacija, tokius kaip pensijos ir sveikatos priežiūra.

1.2.2. Rizikos valdymas: atramos taškas integruotam sienos valdymui

Fundamentaliame lygmenyje, sienos valdymas yra rizikos valdymas. Jei kelionės ir prekyba būtų nerizikingos, sienos kontrolė būtų mažiau svarbi. Bet efektyvus rizikos valdymas apima balansavimą tarp kontrolės ir legalumo – kontrolė, reiškianti identifikavimą, interdiktą ir saugumo pažeidimų sulaikymą, ir legalumas, reiškiantis efektyvias operacijas ir valdymą ir paspartintą legalios kelionės ar prekybos užtikrinimą.

Efektyvus skanavimas identifikuoja nepavojingą kelionę ir prekybą, kuri gali būti paspartinta, tuo metu, kai efektyvus legalizavimas leidžia vyriausybėms sutelkti nepakankamus išteklius, kur pavojus yra aukštesnis ar nežinomas. Operatyviai, šitie du faktoriai yra tarpusavyje susiję – jie naudoja tuos pačius duomenis, sukasi aplink tuos pačius įvykius ir yra atliekami to paties personalo.

Kad būtų galimas efektyvus rizikos valdymas, būtina integracija. Teroristų tinklai ir kriminaliniai karteliai dabar naudoja pažengusias strategijas ir technologijas, kurioms reikalingi koordinuoti ir

tarptautiniai atkirčiai. Kai nusikaltėliai apeina saugumo kontroles oficialiuose įėjimo punktuose, atsakymai turi būti koordinuoti tarp sienos išteklių, sienos kontrolės pareigūnų ir vidaus policijos agentūrų. Iš tikrųjų, tarptautiniai standartai dabar įpareigoja teikti „vieno langelio" (sujungtą) aptarnavimą prie sienos, kuris paspartintų legalią prekybą.

Adekvatus rizikos valdymas apima keturis skirtingus integracijos lygmenis:

- Verslo proceso integracija: kad būtų supaprastintos agentūrų operacijos;
- Partnerystė tarp agentūrų: kad būtų pasidalijama informacija ir kad būtų koordinuotos ar sujungtos tos pačios srities operacijos;
- Tarptautinis bendradarbiavimas tarp vyriausybių, jungiant sienas, racionalizuojant įėjimo/išėjimo informaciją, jungiant procesus ir nustatant pilną krovinių ir vizitų kontrolę.
- Bendradarbiavimas tarp visuomeninio ir privataus sektoriaus: kad būtų dalinamasi tinkama informacija, kuri įgalintų verslo partnerių sertifikavimą, palaikytų atitikimo identifikavimą ir patvirtinimus, ir lengvintų legalią prekybą ir kelionę su mažiau užlaikymų ir žemesnėmis kainomis.

Reikia pabrėžti, kad sienų valdymo funkcijos, natūralūs integracijos metodai jau pakankamai efektyviai egzistuoja: pavyzdžiui, kryžminės kontrolės pareigūnų komandos, įkurdintos tarp agentūros komandų centruose, centralizuoti portalai priėjimui, integruota informacija iš daugialypių šaltinių, nacionaliniai taikymai vietoj regioninių ar vietinių sistemų, ir skanavimo įrankiai, kurie apima daugialypių vyriausybės įstaigų ir privataus sektoriaus įmonių kontroles.

Nepaisant to, kad didžia dalimi segreguoti šiandien, krovinių ir kelionių procesai turi daug panašumų. Šitie bendri komponentai kuria galimybes kryžminiam funkciniam studijavimui, pakartotiniam naudojimui ir potencialiai konsolidacijai – formuojant pagrindus integruotai sienos vadybai:

- *Rizikos valdymo metodologija* - Empiriniai sutikimo ir tarptautinio naudojimo matmenys yra rizikos valdymo metodologijos pagrindas. Metrika rūpinasi kalba, naudojama komunikuoti tarp intervencijos objektų. Ir krovinių, ir keleivių apdorojimui, faktiškas ir greitas informacijos naudojimas leidžia vyriausybėms atrankos būdu pritaikyti išteklius pagal pavojaus lygmenį.
- *Pažangi informacija* – Efektyvus skanavimas priklauso nuo pažangios informacijos. Krovinio atžvilgiu rizikos įvertinimas tiekimo grandinėje prasideda nuo pažangios informacijos perdavimo iš tolimo atstumo. Kelionių atžvilgiu sienos kirtimo procesas turi prasidėti kaip galima ankstesniame kelionės procese – anksčiau nei atvykimas į oro uosto ar sienos postą.
- *Nukreipimo komandos ir įrankiai* – Muitinės nustato nukreipimo vienetus specifinėms grėsmėms. Taipogi, migracijos agentūros kuria keleivinių analizės postus ir sujungia komandų centrus, kad greičiau vyktų skanavimas.
- *Integruotas rizikos įvertinimas* – Pasidalinimas duomenimis ir rizikos įvertinimo atlikimas po

platesnio informacijos komplekto – nuo daugialypių vyriausybės įstaigų iki šalių – didina visaapimantį efektyvumą. WCO struktūra identifikuoja šalių poreikį priimti bendrus apibrėžimus ir kriterijus tam, kad nustatytų didelės rizikos krovinius ir tam, kad turėtų rizikos įvertinimo rezultatus. Integruotas rizikos įvertinimas taip pat leidžia numatyti visapusišką prekybos partnerio „atpažinimą" (pavyzdžiui, žemos rizikos dalyviams). Pavojaus įspėjimų pasidalinimas tarp agentūrų ir vyriausybių yra svarbiausias tokios integracijos pavyzdys. Ši padidinta standartizacija taip pat įgalina automatizavimą: WCO standartas automatizuotam rizikos įvertinimui buvo plačiai priimtas muitinių. Imigracijos agentūroms, visos pasiekiamos keleivinės pavojaus informacijos integracija yra taip pat pagrindinis prioritetas, bet turi būti išspręstos privatumo problemos.

- *Žemo pavojaus kelionių palengvinimas* – Kelios valstybės įgyvendino paspartintą įgaliotų prekybininkų keliavimą, kaip nustatyta WCO standartuose. Panašiai šalys nustato „patikimo keliautojo" programas, kurios leidžia žemo pavojaus keleiviams judėti pagreitinta tvarka.
- *Autentiškumo, apžiūros ir apsaugos technologija* – Neįkyrios apžiūros technologijos, tokios kaip rentgeno spindulys, gama spindulys ir sprogstamasis susekimas padidina kontrolės pareigūnų efektyvumą ir saugumą tuo pačiu metu.

Kad pasiektų tuos pačius dvejopus tikslus keleivių apdorojimui, imigracijos agentūros leidžia „protingus" mandatus, kurie remiasi veido atpažinimu ir biometrinėmis technologijomis keliautojo identifikavimui ir mandatiniam atitikimui. Radijo dažnio identifikavimo (RFID) davikliai yra naudojami prekinių konteinerių ir keleivinio bagažo kontrolei; davikliai taip pat vaidina vaidmenį kontroliuojant nesankcionuotą sienos kirtimą.

Privačiuose ir visuomeniniuose sektoriuose, tapatumo vagystės baimė trukdė skleistis plačiam biometrinės informacijos identifikavimui. Slaptažodžius ir PIN kodus yra lengva pasikeisti, kai iškyla pavojus – bet su piršto atspaudais ir veidais taip nėra.

Be abejo, reikia pastebėti, jog biometrinių duomenų kaupimas kelia tam pavojų, tačiau dabar šiam pavojui yra alternatyva. IBM mokslininkai neseniai išvystė „atšaukiamą" biometrinę sistemą, kurioje transformacijos algoritmas sąmoningai iškraipo asmens biometrinių duomenų pavaizdavimą. Tokie „iškraipyti" biometriniai bruožai panaudojami identifikavimo tikslais. Jei ši informacija yra pavogta, ji gali būti panaikinta ir atgaivinama skirtingo transformacijos algoritmo. Dar svarbiau, iškraipytas bruožas negali būti pakeistas, kad atkurtų originalą, net jei vagis turi transformacijos algoritmą[10].

[10] Marlin, Steven. "IBM Showcases Tech Innovations For Financial Services: The company has new biometric-security, risk-management, and customer service technology under development at R&D lab." http://www.informationweek.com/authors/showAuthor.jhtml;jsessionid=YR4NMOE5ZMAZ0QSNDLRSKH0CJUNN2JVN?authorID=1111.

- *Tarptautiniai standartai* – kai standartai plėtojasi kiekvienoje disciplinoje, iškyla galimybės bendrai veiklai. Pavyzdžiui, daugelis pagrindinių elementų WCO struktūros viduje gali būti panaudoti kelionių srityje. Deja, nepaisant pripažinto globalinio reikalingumo integracijai, standartų priėmimas tebėra lėtas.
- *Sistemos su grįžtamuoju ryšiu valdymas* – integruota sienos vadybos strategija turi numatyti sistemos su grįžtamuoju ryšiu procesus, kurie koordinuotų sienos perėjimo atvejus, kurių istorija lieka aktyvi daug metų. Krovinių atžvilgiu, sulaikymas gali apimti likvidavimą ar trūkumo apmokėjimą per tinkamumo metus. Tačiau tokie sulaikymo veiksmai, susieti su sienos pažeidimais, gali apimti ilgus metus bylinėjimosi, kol galutinis nuosprendis bus įvykdytas. Krovinys, vizitas ar sulaikymo veiksmas – kiekvienas atvejis turi būti sekamas ir valdomas iki visiško išsprendimo.

Krovinių ir keliautojų informacijos apdorojimo susiejimas šiomis aštuoniomis sritimis teikia galimybes bendrai veiklai sienos vadybos programų viduje. Aišku, ištekliai sumažėja ir gali sukurti efektyvumo santaupas, išreikštas personalu ir ICT investicijomis. Bet dar svarbiau tai, kad susiliejimas padeda didinti efektyvumą.

Taigi apibendrinant galima teigti, jog išteklių perskirstymas gali būti naudingas, nes padėtų susitelkti ties aukštesnio prioriteto pavojais. Pareigūnų įgūdžiai ir agentūrų gebėjimai auga. Procesas ir ICT integracija padeda gerinti skanavimo ir intervencijos veiksmo kokybę. Ir nacionaliniame lygmenyje, integruotos, elektroninės vyriausybinės paslaugos, sujungtos su pažangiomis intelekto technologijomis, gali pagreitinti ekonominį vystymąsi, identifikuodamos, supaprastindamos ir spartindamos įgaliotų prekybininkų ir keliautojų verslą.

1.3. Lietuva Šengeno erdvėje

Šengeno erdvė – tai vidinių sienų neturinti valstybių teritorija, pavadinta Šengeno miesto Liuksemburge vardu, kuriame buvo pasirašytas susitarimas.

Šengeno susitarimas pasirašytas 1985 m. birželio 14d. Jo tikslas – panaikinti asmenų, valstybių narių piliečių, kertančių bendras sienas kontrolę ir palengvinti transporto ir prekių judėjimą. Šį susitarimą pasirašė penkios narės: Belgija, Vokietija, Prancūzija, Nyderlandai ir Liuksemburgas.

Šiuo metu prie Šengeno erdvės yra prisijungusios jau dvidešimt keturios valstybės: 22 ES narės: Austrija, Belgija, Danija, Graikija, Ispanija, Italija, Liuksemburgas, Nyderlandai, Portugalija, Prancūzija, Suomija, Švedija ir Vokietija, Lietuva, Latvija, Čekija, Estija, Lenkija, Malta, Slovakija, Vengrija, Slovėnija ir 2 ne ES valstybės: Norvegija ir Islandija[11].

[11] Lietuvos Respublikos Užsienio reikalų ministerija. Bendra informacija apie Šengeno erdvę. Prieiga per internetą: http://www.urm.lt/index.php?1639143581

Verta akcentuoti, kad tokios ES valstybės narės kaip Didžioji Britanija ir Airija nepriklauso Šengeno erdvei ir tebevykdo pasienio su kitomis ES valstybėmis narėmis kontrolę (tačiau jos yra įgaliotos taikyti tam tikras priemones dėl policijos ir teisinio bendradarbiavimo baudžiamosiose bylose).[12]

Šengeno sutartis leidžia panaikinti Šengeno valstybių narių vidaus sienų kontrolę, nustato bendrąsias išorės sienų kontrolės taisykles, bendrąją vizų politiką ir įveda papildomas priemones, leidžiančias tam tikrais atvejais taikyti vidaus sienų kontrolės procedūras (dėl policijos ir teisinio bendradarbiavimo baudžiamosiose bylose).

Kertant Šengeno valstybių narių vidaus sienas, nebėra asmens dokumentų kontrolės. Tačiau tai nereiškia, kad judėjimas Šengeno erdvėje yra prilyginamas judėjimui vienoje valstybėje narėje be kelionės ar tapatybės dokumento. Šengeno šalių teisėsaugos institucijų atstovai, vadovaudamiesi nacionaliniais teisės aktais, turi teisę savo šalies teritorijoje patikrinti asmens tapatybę. Kiekvienos valstybės narės teisės aktuose numatyta, ar asmuo privalo tokį dokumentą turėti su savimi.

ES šalies pilietis turi teisę laisvai keliauti asmeniniais ar darbo reikalais po visą Europos Sąjungą, pakanka turėti galiojantį pasą arba tapatybės kortelę. ES piliečio teisė keliauti gali būti apribota tik viešosios tvarkos, visuomenės saugos ar visuomenės sveikatos sumetimais.

Valstybės narės pasiliko sau teisę tam tikram laikui sugrąžinti kontrolės pasienyje procedūras, jeigu kiltų grėsmė jų saugumui ar viešajai tvarkai. Pasienio kontrolė gali būti atkurta ir masinių tarptautinių sporto renginių metu.

26-ojoje tarptautinėje duomenų apsaugos ir privatumo komisijos narių konferencijoje[13], Šveicarijos federalinis Duomenų apsaugos Komisijos narys pabrėžė tai, kad biometrinių duomenų rinkimas ir apdorojimas turi būti atliekamas griežtai pagal duomenų apsaugos reguliavimo reikalavimus ir ypač jų pagrindinius principus (teisėtumas, pasitikėjimas, tikslo siekimas, duomenų saugumas, proporcingumas ir susijusių asmenų teisės). Privačiame sektoriuje, biometriniai duomenys iš principo gali būti panaudoti su susijusio asmens sutikimu, ir sutikimas turi būti laisvas, specifinis, ir įformintas (teisėtas).

Biometrinių duomenų rinkimo ir apdorojimo procesas turi būti aiškus, ir neįvykti be subjekto žinios (pasitikėjimo principas). Tikslo siekimo principas teigia, kad, jei mažiau pažeidžianti privatumą technologija, tokia kaip patikrinimas vietoj identifikavimo, gali pasiekti nustatytą tikslą (pavyzdžiui, prieigos kontrolę), tai ji turi būti naudojama.

Proporcingumo principas reiškia, kad asmeniniai duomenys gali būti renkami tik tada, jei jie yra būtini dėl tikslo, kuriuo jie turi būti surinkti ir apdoroti. Turi būti užduotas klausimas, ar

[12] Valstybės sienos apsaugos tarnyba. Šengeno teritorija ir bendrijos teisė. Prieiga per internetą: http://www.pasienis.lt/lit/Sengeno_teritorija_ir_bendrijos_teise/240

[13] 26th International Conference on Privacy and Personal Data Protection. http://26konferencja.giodo.gov.pl/data/rezolucje/en/rezolucja1.doc

pageidaujamas tikslas negalėtų būti pasiektas, nepanaudojus asmeninių duomenų. Pritaikius biometrikai, tai reiškia, kad identifikavimo sistemos diegimas nėra būtinas, kur patikrinimo sistema yra pakankama, ir kad tuo atveju turėtų būti teikiama pirmenybė anoniminiams ir užšifravimo metodams, kurie leistų autentiškumo nustatymą be identifikavimo.

Proporcingumo principas yra taikytinas pagal šalį, ir su kiekvienos šalies duomenų apsaugos komisijos nariu konsultuojamasi pagal kiekvieną atvejį atskirai.

Pagal duomenų saugumo principą, biometrikos sistemų duomenų saugumas yra būtinas. „Tapatybės vagystės" atveju, aukai bus labai sunku įrodyti, kad ji neatliko kokio nors nusikaltimo, padaryto vagies. Taigi, saugumo priemonės turi būti įdiegtos pirmiausia, prasidedant duomenų kaupimo procesui.

Kaip minėta aukščiau, joks biometrikos teisinis apibūdinimas šiuo metu neegzistuoja nei Europoje, nei tarptautiniame lygmenyje. Net jei saugumas darosi vis svarbesnis, teisė į privatų gyvenimą ir pagarba žmogaus kūnui yra taip pat labai svarbu daugumoje šalių. Ši teisė į privatų gyvenimą reiškia taip pat bet kokių jautrių asmeninių duomenų apsaugą, kadangi tai yra biometrika. Teisiniai klausimai kai kuriose šalyse bus pristatyti šioje dalyje, pradedant nuo Šveicarijos, Europos ekonominės bendrijos, ir po to aptariant JAV, kuri darė didžiausią įtaką tarptautinei teisinei struktūrai nuo 2001.

1.3.1. Šengeno (*acquis*) teisynas, informacinė sistema ir jos paskirtis

Pagal Šengeno sutartį turėjo būti panaikintos vidinės sienos, kad būtų užtikrintas laisvas prekių, paslaugų ir asmenų judėjimas. Tačiau įgyvendinant šią sutartį atsirado keblumų, todėl 1990 m. birželio 19 d. tos pačios penkios valstybės pasirašė Šengeno sutarties taikymo konvenciją. Šioje konvencijoje buvo numatytos konkrečios priemonės Šengeno susitarimo įgyvendinimui. Svarbiausias dėmesys buvo skiriamas informacijos apsikeitimui ir išorinių sienų kontrolės griežtinimui. Įsigaliojus Amsterdamo sutarčiai 1999 m. Šengeno susitarimas dėl bendrų sienų kontrolės panaikinimo ir jį įgyvendinančios Konvencijos nuostatos tapo Europos Sąjungos teisinės bazės dalimi ir kartu tapo privalomi norint integruotis į Europos Sąjungą.[14] Nuo tada Europos Sąjungos teisinėje ir institucinėje bazėje buvo imtos taikyti ir toliau plėsti Šengeno teisyno (*acquis*) nuostatos. Šengeno teisynas yra tarpvyriausybinis Šengeno grupės taisyklių rinkinys. Šengeno teisyne yra numatytos konkrečios priemonės, kompensuojančios vidaus sienų kontrolės panaikinimą ir stiprinančios Europos Sąjungos išorės sienų saugumą. Išorės sienas turinčios valstybės narės privalo užtikrinti tinkamą ir veiksmingą ES išorės sienų kontrolę.

[14] Europos Bendrijos steigimo Sutarties (Konsoliduota redakcija) - B. Protokolai, pridedami prie Europos Sąjungos sutarties ir Europos bendrijos steigimo sutarties - Protokolas (Nr. 2) dėl Šengeno *acquis* integravimo į Europos Sąjungos sistemą (1997). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12006E/PRO/02:LT:HTML

Pagrindiniai dokumentai sudarantys Šengeno teisyną yra:

- Šengeno sutartis,
- Šengeno sutarties taikymo konvencija,
- Šengeno sutarties prisijungimo protokolai bei stojimo sutartys,
- Vykdomojo komiteto sprendimai bei aktai.

Šengeno informacinės sistemos paskirtis – susitariančiųjų šalių teritorijose palaikyti viešąją tvarką ir visuomenės saugumą, įskaitant nacionalinį saugumą, ir, naudojant šia sistema perduodamą informaciją, Kiekviena Šengeno šalis turi sukurti savo nacionaline Šengeno informacinę sistemą, kurią turi išlaikyti savo sąskaita. Tačiau kurdama šią sistemą šalis privalo laikytis duomenų perdavimo protokolų ir tvarkos, kurie yra numatyti susitarančių šalių. Kiekvienos nacionalinės sekcijos duomenų byla yra prieinama atliekant automatines paieškas kiekvienos iš susitariančiųjų šalių teritorijoje. Tačiau negalima ieškoti duomenų bylų kitų susitariančiųjų šalių nacionalinėse sekcijose.

Taip pat yra įkurta pagrindinė kompiuterinė bazė, kurios priežiūrą atlieka centrinė techninio aptarnavimo tarnyba. Už šią centrinę duomenų bazę yra atsakinga Prancūzija, tačiau išlaiko visos susitariančios šalys. Ji yra įkurta Strasbūre.

Konvencijos dėl Šengeno susitarimo įgyvendinimo 101 straipsnis nustato, kad teisę prieiti prie duomenų, įtrauktų į Šengeno informacinę sistemą, ir teisę tiesiogiai atlikti tokių duomenų paiešką turi tik institucijos, atsakingos už:

a) pasienio kontrolę;

b) kitus šalyje policijos ir muitinės atliekamus tikrinimus ir jų koordinavimą.

Taip pat Konvencijos dėl Šengeno susitarimo įgyvendinimo 101 straipsnio 2 dalyje nustatyta, kad prieiti prie duomenų, įtrauktų pagal Konvencijos dėl Šengeno susitarimo įgyvendinimo 96 straipsnį, ir teise tiesiogiai atlikti duomenų paiešką gali naudotis institucijos:

1) atsakingos už vizų išdavimą,

2) centrinės institucijos, atsakingos už vizų prašymų nagrinėjimą,

3) institucijos, atsakingos už leidimų gyventi išdavimą bei užsieniečiams skirtų teisės aktų administravimą, taikant šios Konvencijos nuostatas dėl asmenų judėjimo.

Priėjimą prie duomenų reglamentuoja kiekvienos susitariančiosios šalies nacionaliniai teisės aktai. Naudotojai gali atlikti tik duomenų, kurių jiems reikia savo užduotims atlikti, paiešką. Konvencija dėl Šengeno susitarimo įgyvendinimo nustato pareigą kiekvienai Susitariančiajai Šaliai nusiųsti Vykdomajam komitetui sąrašą kompetentingų institucijų, kurios yra įgaliotos atlikti Šengeno informacinėje sistemoje esančių duomenų paiešką. Tame sąraše konkrečiai nurodoma, kokių duomenų ir kokiems tikslams kiekviena institucija gali ieškoti.

Šengeno informacinės sistemos SIS II kūrimą reglamentuoja 2001 m. gruodžio 6 d. Tarybos reglamentas Nr. 2424/2001 dėl antros kartos Šengeno informacinės sistemos (SIS II) sukūrimo[15]. Šengeno informacinė sistema, sukurta pagal 1990 m. Konvencijos, įgyvendinančios 1985 m. birželio 14 d. Šengeno sutartį dėl laipsniško kontrolės prie bendrų sienų panaikinimo, toliau vadinamos "1990 m. Šengeno konvencija", IV dalies nuostatas, sudaro esminę Šengeno *acquis*, integruotos į Europos Sąjungos teisės sistemą, nuostatų taikymo priemonę.

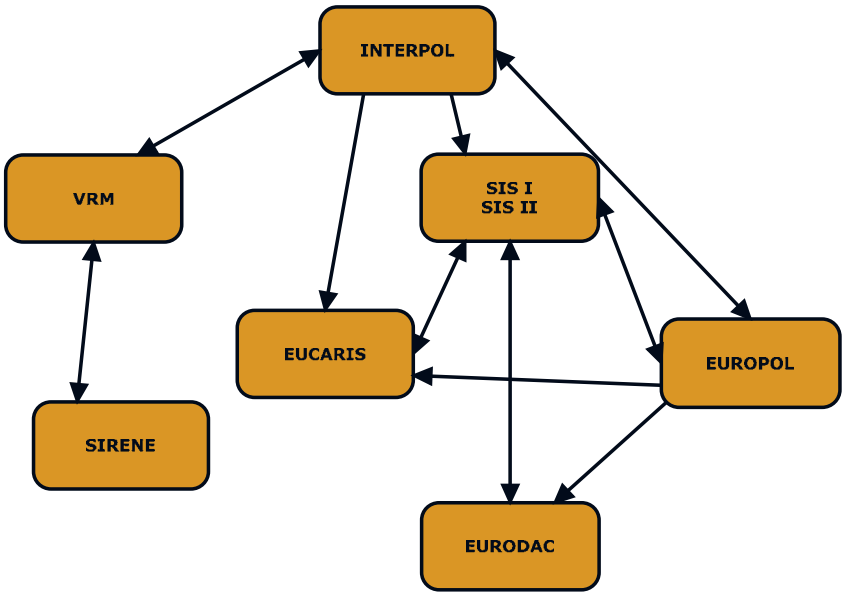
Šengeno informacinė sistema dabartine forma yra pajėgi aptarnauti ne daugiau kaip 18 dalyvaujančių valstybių. Šiuo metu ji veikia 13 valstybių narių ir 2 kitose valstybėse (Islandija ir Norvegija), o artimoje ateityje numatoma, kad į ją įsitrauks Jungtinė Karalystė ir Airija. Tačiau ji nebuvo sukurta, kad aptarnautų po Europos Sąjungos plėtimosi padidėjusį valstybių narių skaičių. Dėl šios priežasties ir siekiant pasinaudoti naujausiais informacinės technologijos laimėjimais ir sudaryti sąlygas įdiegti naujas funkcijas, reikia sukurti naują, antrosios kartos Šengeno informacinę sistemą (SIS II).

Pagal 2001 m. gruodžio 6 d. Tarybos sprendimą dėl antros kartos Šengeno informacinės sistemos (SIS II) sukūrimo (2001/886/TVR)[16], Šengeno informacinė sistema turi leisti valstybių narių paskirtoms institucijoms, naudojantis automatine paieška, prieiti prie perspėjimų dėl asmenų ir daiktų vykdant pasienio kontrolę bei atliekant kitus policijos ir muitinės tikrinimus šalyje pagal nacionalinius teisės aktus, taip pat išduodant vizas, leidimus gyventi ir administruojant užsieniečiams taikomus teisės aktus Šengeno *acquis* nuostatų, skirtų asmenų judėjimui, taikymo kontekste.

SIS II, kaip bendrą integruotą sistemą, kuria Komisija 2001 m. gruodžio 6 d. Tarybos reglamente Nr. 2424/2001 “dėl antros kartos Šengeno informacinės sistemos (SIS II) sukūrimo” numatyta tvarka pateikiama 2 paveiksle.

[15] 2001 m. gruodžio 6 d. Tarybos reglamentas (EB) Nr. 2424/2001 dėl antros kartos Šengeno informacinės sistemos (SIS II) sukūrimo. http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!CELEXnumdoc&numdoc=32001r2424&lg=lt

[16] Tarybos sprendimas 2006/1007/TVR 2006 m. gruodžio 21 d. iš dalies keičiantis Sprendimą 2001/886/TVR dėl antros kartos Šengeno informacinės sistemos (SIS II) sukūrimo. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:411:0078:0081:LT:PDF



2 pav. Informacijos sąveikos schema

Sudaryta autorės

1.3.2. „*Eurodac*“ bei vizų informacinės sistemos (VIS) analizė

2000 m. gruodžio 11 d. Tarybos reglamente Nr. 2725/2000/EB dėl „*Eurodac*“ sistemos sukūrimo pirštų atspaudams lyginti siekiant veiksmingiau taikyti Dublino konvenciją numatyta skirti nacionalinę priežiūros instituciją, atsakingą už nacionalinio „*Eurodac*“ padalinio priežiūrą, ar teisėtai jis tvarko ir perduoda centriniam „*Eurodac*“ padaliniui asmens duomenis. „*Eurodac*“ sistemos paskirtis – padėti nustatyti, kuri valstybė narė pagal 1990 m. birželio 15 d. Dubline pasirašytą Konvenciją, nustatančią valstybę, atsakingą už vienoje iš Europos Bendrijų valstybių narių paduotų prieglobsčio prašymų nagrinėjimą (Žin., 2004, Nr.112-4181) (toliau vadinama – Dublino konvencija), turi būti atsakinga už kurioje nors valstybėje narėje paduoto prieglobsčio prašymo nagrinėjimą, ir kitaip palengvinti Dublino konvencijos taikymą 2000 m. gruodžio 11 d. Tarybos reglamente Nr. 2725/2000/EB nustatytomis sąlygomis[17].

„*Eurodac*“ sistemą sudaro: centrinis padalinys, kompiuterizuota centrinė duomenų bazė, duomenų perdavimo tarp valstybių narių ir centrinės duomenų bazės priemonės. Įsteigiamas Komisijai pavaldus Centrinis padalinys, kuris yra atsakingas už centrinės duomenų bazės valdymą valstybių narių vardu. Centriniame padalinyje įrengiama kompiuterizuota pirštų atspaudų atpažinimo sistema.

[17] Tarybos sprendimas dėl Europos Sąjungos, Europos bendrijos ir Šveicarijos Konfederacijos susitarimo dėl pastarosios asociacijos įgyvendinant, taikant ir plėtojant Šengeno acquis pasirašymo Europos Sąjungos vardu. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0593:FIN:LT:DOC

Duomenys apie prieglobsčio prašytojus, asmenis, centriniame padalinyje yra apdorojami kilmės valstybės narės vardu laikantis 2000 m. gruodžio 11 d. Tarybos reglamente Nr. 2725/2000/EB nustatytų sąlygų.

Pirštų antspaudai iš karto turi būti paimti ir perduoti į centrinį padalinį šių asmenų:

1) užsieniečių, sulaikytų dėl išorinės sienos kirtimo;
2) valstybėje narėje aptiktų neteisėtai gyvenančių užsieniečių,
3) pripažintų pabėgėlių,

Atitinkama valstybė narė Centriniam padaliniui nedelsdama perduoda šiuos su užsieniečiu susijusius duomenis:

1) kilmės valstybė narė, sulaikymo vieta ir data;
2) pirštų atspaudų duomenys;
3) lytis;
4) kilmės valstybės narės vartojamas nuorodinis numeris;
5) pirštų atspaudų ėmimo data;
6) duomenų perdavimo Centriniam padaliniui data.

Vizų informacinės sistemos (VIS) naudojimas turi pagerinti bendrosios vizų politikos administravimą, konsulinį bendradarbiavimą, centrinių konsulinių įstaigų konsultavimąsi ir taip neleisti atsirasti grėsmėms vidaus saugumui ir prekybai vizomis („*visa shopping*“), palengvinti kovą su sukčiavimu ir patikrinimus išorės sienos kontrolės punktuose, valstybių narių teritorijoje, padėti identifikuoti ir grąžinti nelegalius migrantus, taip pat palengvinti 2003 m. vasario 18 d. Tarybos reglamento Nr. 343/2003/EB,[18] nustatančio valstybės narės, atsakingos už trečiosios šalies piliečio vienoje iš valstybių narių pateikto prieglobsčio prašymo nagrinėjimą, nustatymo kriterijus ir mechanizmus (toliau vadinama – *Dublin II* reglamentas), taikymą. Greitesnis ir tikslesnis vizų prašymų nagrinėjimas, įskaitant centrinių institucijų konsultavimąsi, prašytojų patikrinimas ir identifikavimas konsulinėse įstaigose ir pasienio kontrolės punktuose padėtų užtikrinti didesnį valstybių narių vidaus saugumą ir veiksmingą kovą su terorizmu, o tai – vienas iš pagrindinių bendrosios vizų politikos tikslų ir pagrindinis jos vertinimo kriterijus, taip pat nelegalia migracija. VIS turėtų būti naudinga ir užsieniečiams, nes tobulės vizų išdavimo ir patikrinimo procedūros.[19]

Užsieniečiui norint keliauti po Šengeną, reikia tik vienos vizos. Lietuva nuo pirmos narystės Šengene dienos išduos bendras trumpalaikes vizas, tinkamas vykti į Šengeno susitarimo teritoriją, o

[18] Commission Regulation (EC) No 1560/2003 of 2 September 2003 laying down detailed rules for the application of Council Regulation (EC) No 343/2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003R1560:EN:HTML

[19] Lietuvos Respublikos Vyriausybės 2006 m. birželio 8 d. nutarimas Nr.559 „Dėl Lietuvos Respublikos Vyriausybės 2002 m. liepos 19 d. nutarimo Nr. 1194 “Dėl nacionalinio šengeno acquis priėmimo veiksmų plano pakeitimo” // www.lrvk.lt/teises_aktai/files/2006/06/6666.doc

užsieniečiai, jau turintys galiojančias kitų Šengeno partnerių išduotas vizas, galės būti visoje Šengeno teritorijoje, įskaitant Lietuvą, vizoje nurodytu jos galiojimo laikotarpiu.

Šengeno susitarimo šalys taiko vienodą vizų išdavimo praktiką, atsižvelgdamos į viena kitos interesus, vienodus reikalavimus pateikiamiems dokumentams, ima vienodą mokestį už prašymo išduoti vizą nagrinėjimą. Todėl vienoje Šengeno valstybėje narėje išduota viza galioja ir kitose valstybėse narėse. Tai yra itin naudinga trečiųjų šalių piliečiams, ketinantiems aplankyti kelias Šengeno valstybes nares.

Išimties atvejais asmenims, neatitinkantiems bendrųjų vizų išdavimo sąlygų, Šengeno valstybė narė gali išduoti tik toje šalyje galiojančią vizą. Tokie atvejai gali būti susiję su humanitarinėmis, nacionalinių interesų ar tarptautinių įsipareigojimų priežastimis.

Tapusi visateise Šengeno erdvės nare, Lietuvos Respublika pradės išduoti Šengeno vizas (vienodos formos visoje Europos Sąjungoje). Vizoms išduoti bus naudojama Nacionalinė vizų informacinė sistema (NS-VIS), taip pat teikiamos VISION (angl. *Visa Inquiry Open Border Network*; Vizų prašymų nagrinėjimo atviras tinklas) konsultacijos. NS-VIS suteiks galimybę gauti informaciją apie visas užsieniečiui anksčiau išduotas vizas, konsultacijos apsaugos Šengeno erdvę nuo grėsmę nacionaliniam saugumui ir viešajai tvarkai keliančių asmenų, pasieniečiai galės ne tik patikrinti informaciją apie išduotas vizas, bet ir palyginti užsieniečio pirštų atspaudus.

Lietuvai tapus visateise Šengeno erdvės nare, bus atnaujinta vizų tarnybų Lietuvos Respublikoje ir užsienio valstybėse įranga, skirta vizoms išduoti. Turimos įrangos (skaitytuvų, spausdintuvų) nepakanka. Be to, NS-VIS tarnybinės stotys tiek Užsienio reikalų ministerijoje, tiek konsulinėse įstaigose įrengtos patalpose, kurios neatitinka Europos Sąjungos duomenų apsaugos reikalavimų. Lietuvai tapus visateise Šengeno erdvės nare, reikalavimai šiai visas Lietuvos konsulines įstaigas jungiančiai sistemai gerokai padidės. Bus įsigyta ir sumontuota saugyklų įranga, prijungta prie infrastruktūros tinklų, į kuriuos bus perkeltos NS-VIS tarnybinės stotys.

Diegiant Užsienio reikalų ministeriją ir jos konsulines įstaigas jungiančią Konsulinių procedūrų valdymo sistemą (toliau vadinama – KPVS), susidurta su techninėmis ryšio problemomis labiau nuo Lietuvos nutolusiose užsienio valstybėse. Dėl menko informacinių technologijų sklaidos lygio ryšio kanalai, jų techninė įranga veikia nestabiliai, taigi ne visada galima užtikrinti nuolatinę ir tinkamą KPVS veiklą. Ši problema ypač opi dabar, kai Lietuva stengiasi tapti visateise Šengeno erdvės nare ir vykdomi pasirengimo prisijungti prie Šengeno informacinės sistemos (toliau vadinama – SIS II)/VIS įsipareigojimai. Ryšiai bus tobulinami, nes prastas ryšys gali kliudyti įdiegti nacionalines SIS II / VIS dalis ir jų sąsajas su Lietuvos konsulinėmis įstaigomis užsienyje.

1.3.3. Biometriniai pasai bei jų taikymo problemos Lietuvoje

ES šalys pereina prie biometrinės pasų kontrolės – technologijų ir inovacijų kompanija „Siemens“ ES šalių piliečių pasuose diegia mikroprocesorius, kuriuose saugoma individuali asmens informacija: pirštų antspaudai ir veido nuotrauka. Šios technologijos jau yra įdiegtos keliose ES šalyse. Jos padės sumažinti pasų klastojimo galimybes ir užtikrinti didesnį saugumą Europos pasienio punktuose.

Biometrinės sistemos programinė įranga, kuria pasų kontrolės punkte nuskaitomi duomenys ir palyginami su skaitmenine keliautojo nuotrauka, sukurta Austrijos mieste Grace įsikūrusiame „Siemens“ „Biometrijos centre“.

Naujoji sistema, kaip jau minėta, veikia keliose šalyse. Biometrinius pasus praėjusiais metais pradėjo naudoti Šveicarija[20]. Elektroninių pasų sprendimus „Siemens“ IT sprendimų ir paslaugų grupė neseniai įdiegė ir Čekijoje – šioje šalyje jau įrengti 230 pasų kontrolės punktai, kuriuose naudojami fotografavimo, paso nuskaitymo įrenginiai, spausdintuvai ir atitinkamos IT sistemos.

Ateityje planuojama čekiškuose pasuose integruoti ypač ploną RFID (radijo dažnių identifikavimo) lustą su antena. RFID elektroninėje laikmenoje bus saugomi paso savininko duomenys: vardas, gimimo data, skaitmeninis veido atvaizdas ir pirštų atspaudai. Kol prie šalies sienos su specialiais įrenginiais bus nuskaitomi tikri keliautojo pirštų atspaudai, skaitmeninė foto kamera nufotografuos keliautojo veidą, kuris iš kart bus palyginamas su nuotrauka, saugoma paso elektroninėje laikmenoje. Vienas iš identifikavimo kriterijų, kuriais naudosis sistema bus unikali kiekvieno asmens akių padėtis.

„Siemens“ pasienių kontrolės sistema pradėta diegti ir Kroatijoje. Dabar Kroatijos pasienio pareigūnai gali patikrinti keleivio vizos galiojimą bei asmeninius duomenis ir palyginti juos su informacija, saugoma Vidaus ministerijos centrinėje duomenų bazėje. Be to, naudodama foto kameras, sistema gali užfiksuoti automobilio numerį bei modelį ir taip greičiau atpažinti, kuris iš jų yra vogtas. Naujoji sistema jau naudojama Bajakovo pasienyje ir Zagrebo oro uoste.

Europos šalyse automatinės-biometrinės pasienio kontrolės sprendimus „Siemens“ diegia Registruotų keleivių programos (RTP) pagrindu. Europos Sąjungos šalys narės ir Šengeno sutarties signatarai pasižadėjo iki 2009-ųjų metų įrašyti biometrinius identifikatorius (nuotrauką ir pirštų atspaudus) į savo pasų elektroninę laikmeną.

Lietuvoje visuomenė nėra tinkamai informuojama apie biometrinių pasų patikimumą, efektyvumą ir svarbiausia - apie jų įtaką asmens teisei į privatų gyvenimą. ES duomenų apsaugos darbo grupė 2006 m. pabaigoje pareiškė, kad prieš įvedant pasus su biometriniais duomenimis, yra

[20] Biometric passport for Switzerland. http://www.it-solutions.siemens.com/b2b/it/en/global/Documents/References/ePass_swiss-PDF_e.pdf

būtina išsami diskusija visuomenėje dėl šių dokumentų teisinių, etinių ir techninių aspektų.

Daugelyje vakarų Europos šalių tokia diskusija vyksta ir joje aktyviai dalyvauja valstybės institucijos, nevyriausybinės organizacijos bei biometrinių duomenų naudojimo pasekmėms analizuoti įsteigtų institucijų ekspertai. Todėl pasų su biometriniais duomenimis pradėti naudoti neskubama - pirmiausia stengiamasi išspręsti visus esminius klausimus. Lietuvoje jokia diskusija nevyksta, o visuomenės informavimas yra panašus į viešųjų ryšių akciją ar reklamos kampaniją, kurioje biometrinių pasų įvedimas yra pristatomas tik kaip patraukli, piliečių saugumą didinanti technologinė naujovė.

Pagrindinės su biometrinių pasų įvedimu susijusios problemos yra galimi teisės į privatų gyvenimą pažeidimai – ypatingai dėl biometrinių duomenų specifikos bei saugojimo būdų, bei šių duomenų patikimumo klausimas.

Europos Tarybos reglamente (EB) Nr. 2252/2004[21] dėl valstybių narių išduodamų pasų ir kelionės dokumentų apsauginių savybių ir biometrikos standartų, kuris numatė biometrinių pasų įvedimą, yra nustatyta, kad bus naudojami veido atvaizdo bei pirštų atspaudų biometriniai duomenys. Nepaisant Europos Parlamento, Europos Sąjungos duomenų apsaugos darbo grupės, bei įvairių ekspertų nuomonės rinktis saugesnius biometrinius duomenis, kaip pavyzdžiui rankos kontūrą, buvo pasirinkti ypač nesaugiais laikomi duomenys, nes jie atskleidžia ypatingą informaciją apie asmenį ir gali būti naudojami kartu su įvairiomis technologijomis. Pavyzdžiui piršto atspaudų duomenys gali nurodyti įvairias genetines anomalijas, ar polinkį tam tikroms ligoms. Be to, jie palieka pėdsaką, o naudojant pėdsakus paliekančius biometrinius duomenis iškyla reali grėsmė, kad jie bus renkami ir saugomi be asmens sutikimo. Tuo tarpu veido atvaizdo biometriniai duomenys gali būti naudojami kartu su nuotolinio veido atpažinimo technologija, kuri leidžia identifikuoti asmenį ir sekti jį per atstumą be jo žinios ir sutikimo. Taip iškyla reali piktnaudžiavimo bei visuotinės kontrolės grėsmė, todėl prieš įvesdama biometrinius pasus valstybė privalo imtis ypatingų priemonių užtikrinti asmenų teisę į privatų gyvenimą.

Daugiausia klausimų kyla dėl planuojamo biometrinių duomenų saugojimo Gyventojų registre. Reglamentas biometrinių duomenų saugojimo būdą paliko valstybių narių atsakomybei, nors dar svarstant Reglamentą, Europos Parlamentas, Europos Sąjungos duomenų apsaugos darbo grupė, bei nevyriausybinės organizacijos siūlė uždrausti juos kaupti duomenų bazėse, ir leisti juos saugoti tik asmens dokumente, nes į duomenų bazes galima įsilaužti, klastoti, keisti ir naikinti jose saugomus duomenis. Tuo tarpu programinei įrangai suklydus ir duomenis priskyrus ne tam asmeniui, įrodyti klaidą bus ypač sudėtinga, nes biometriniai duomenys yra laikomi unikaliais ir labai patikimais. Be to,

[21] Tarybos reglamentas (EB) Nr. 2252/2004 2004 m. gruodžio 13 d. dėl valstybių narių išduodamų pasų ir kelionės dokumentų apsauginių savybių ir biometrikos standartų. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0001:0006:LT:PDF

saugant biometrinę informaciją duomenų bazėse, kils duomenų bazių susijungimo ir nekontroliuojamo duomenų panaudojimo rizika. Taip bus sukurta ypač patogi infrastruktūra valstybei sužinoti apie asmenis beveik viską.

Ši rizika yra ypatingai didelė Lietuvoje, kur žmonių informuotumas ir sąmoningumas duomenų rinkimo, saugojimo ir panaudojimo srityje yrą žemas, duomenų registrų sistema yra ypač centralizuota ir saugomi duomenys yra gana nesunkiai prieinami trečiosioms šalims. Įvertinus šią riziką, Valstybė turėtų pateikti ypač svarius argumentus, kodėl Lietuvoje yra paliekama galimybė biometrinius duomenis saugoti Gyventojų registre.

Nors dažnai skelbiama, kad biometrinių dokumentų patikimumas yra didelis, paprastai tokie teiginiai yra nepagrįsti - iki šiol biometriniai dokumentai niekur nebuvo ilgai ir masiškai naudojami. Priešingai, laikinosios bandomosios biometrinių dokumentų naudojimo studijos parodė, kad prognozės yra pesimistinės. Biometriniais pasais neužilgo naudosis milijardai žmonių visame pasaulyje. Remiantis išankstiniais tyrimais tai reikštų, kad milijonai žmonių bus klaidingai identifikuoti. Tai ne tik nepadidins saugumo, bet sukels nemažai sumaišties.

Žmogaus teisių stebėjimo institutas siūlo įstatymų pataisų rengėjams susilaikyti nuo nepagrįstų teiginių apie ypatingą biometrinių pasų saugumą, patikimumą ir efektyvumą ir visapusiškai informuoti Seimo narius bei visuomenę apie biometrinių pasų įvedimą, biometrinių duomenų saugojimą, išsamiai paaiškinti kodėl Lietuvoje yra paliekama galimybė biometrinius duomenis saugoti gyventojų registre ir aptarti galimas neigiamas pasekmes teisei į privatų gyvenimą. Seimui pateiktas teisės aktų paketas turėtų būti papildytas aiškiomis nuostatomis, kurios užtikrins biometrinių dokumentų bei duomenų saugumą ir numatys atsakomybę už pažeidimus bei piliečių galimybę nuo jų apsiginti. Raginame Seimo narius atsakingai pažvelgti į siūlomų teisės aktų projektų privalumus ir trūkumus.

2. E.SIENOS INTEGRUOTO VALDYMO PRAKTINĖ REALIZACIJA, BIOMETRINIŲ PERIMETRO SAUGOS SISTEMŲ REALIZAVIMO YPATUMAI ES BEI PASAULIO ŠALIŲ PRAKTIKOJE

2.1. Efektyvios sienos kontrolės užtikrinimo projektas

E.sienos yra svarbus Vyriausybės sienų transformacijos programos komponentas, kurios tikslas yra atlikti modernizuotą sienos kontrolę, kuri būtų iš esmės efektyvesnė, veiksmingesnė ir saugesnė, patenkinanti ateities sienų apsaugos reikalavimus.

2.1.1. E.sienos paskirtis bei vaidmuo užtikrinant sienos kontrolę

Besitęsiantis keleivių skaičiaus didėjimas ir padidintos neteisėto migravimo grėsmės, terorizmo ir organizuoto nusikalstamumo problemos reikalauja radikalios sienos kontrolės modernizacijos, jei norime, kad ji būtų efektyvi. E.sienos garantuos galimybę:

1) turėti visą informaciją apie visus, kas kerta sieną.
2) padidinti gyventojų ir atvykstančių saugumą.
3) palengvinti teisėtą kelionę ir prekybą.
4) apsaugoti sienos kontrolės vientisumą:
    a) tiksliai įspės, kas siekia kirsti sienas, tikrindama juos pagal asmenų sąrašus, kurie kelia grėsmę;
    b) kaups išsamią kelionių istoriją su galimybe atlikti duomenų tikrinimą per agentūras pagal pareikalavimą; didelis laimėjimas laiko sutaupymo ir tarptautinių patikrinimų atlikimo srityje. Kad ir kaip bebūtų, dar nepavyko nustatyti šios naudos masto dėl pradinių duomenų nebuvimo;
    c) visapusis įtariamų asmenų, kelionės modelių ir tinklų profiliavimas
    d) aprūpinimas daugybės agentūrų operaciniais gebėjimais, koordinuotais ir integruotais metodais;
    e) potencialių grėsmių visuomenės saugumui aptikimas, ir būtinų veiksmų jiems atlikti nustatymas.
    f) leis sutelkti sienos kontrolės pareigūnus, muitinę ir policininkus prieš tuos, kas kelia grėsmę; ir
    g) pagerins gebėjimą sulaikyti imigracijos pažeidėjus ir nusikaltėlius, ir paskui neleisti jiems grįžti,
    h) įgalins praleisti daugiau žmonių per sienas ir valdyti 50 % keleivių skaičiaus padidėjimą,

prognozuojamą per ateinančius 10 metų; ir

i) automatizuos rankinius ir išteklių reikalaujančiu procesus.

Svarbiausias e.sienų programos tikslas yra sukaupti ir analizuoti duomenis iš kelionės pramonės (oras, jūra ir geležinkeliai), visų keleivių ir komandos, ketinančios išvažiuoti ar įvažiuoti į šalį. E.sienos įvertins pavojus, nešamus keleivių, įvažiuojančių ir paliekančių šalį, identifikuodamos stebėjimo vertus asmenis dar prieš jų atvykimą į šalį[22].

Ši informacija bus perduodama „pavojaus signalo“ pavidalu atitinkamai sienos kontrolės agentūrai, kuri nustatys tinkamą įsikišimą. Yra praktikos su vadybos informacija, kuria dalinasi Sienų Agentūros, Muitinė, ir policija. Tai išsprendžia e.sienos ir kitų kartu dirbančių programų duomenų pasidalinimą, naudojimą ir laikymą pagal e.sienų ir kitus įstatymus.

E.sienų programa buvo pradėta su trimis pirminiais tikslais. Tai yra, padidinti:

1) saugumą;
2) efektyvumą;
3) našumą.

Ši programa pradėta, kad eksploatuotų besivystančias technologijas, ypač apimančias biometriką, garantuotų efektyvią identifikacijos vadybos sistemą.

Bus renkama kelionės dokumentų ir paslaugų informacija konkrečios kelionės metu. Ši informacija susideda iš biografinės informacijos, esančios paso zonoje, apdorojamoje kompiuteriu, ir detalios paslaugos, kuria keleivis naudojasi, informacija (pavyzdžiui, skrydžio reiso numeris). Ši informacija kartais vadinama pažangesne keleivio informacija (*API*). Taip pat bus išsaugota kita informacija apie keleivius, tokia kaip rezervacijos ir mokėjimų detalės (kartais žinomi kaip PNR duomenys). Ši informacija yra neįkainojama identifikuojant potencialiai grėsmę keliančius objektus. Tam tikro asmens kelionių informacija bus sujungta, formuojant kelionės istoriją.

Pasienio apsaugos sustiprinimas

Daug šalių siekia griežtesnės sienų kirtimo kontrolės, kovodamos su nelegalia imigracija. Imtasi daug iniciatyvų ir svarbių programų, kad automatiškai galima būtų patikrinti biometrines duomenų bazes. Pavyzdžiu gali būti siekis sustiprinti ID dokumentų saugumą, diegiant e-Pasų sistemą, kuri tampa vis populiaresnė. Kitas žingsnis po kelionės dokumentų saugumo padidinimo, yra pačių sienų ir jų kontrolės apsaugos didinimas. Taigi sienų kontrolė turės sugebėti nustatyti e-Pasų autentiškumą.

Iš tikrųjų, Europos Sąjunga naudoja patobulintą biometrikos versiją centrinėje bazėje tam, kad apsikeistų informacija apie vizas tarp valstybių narių. Tokia sistema vadinasi Vizų Informacinė Sistema (VIS). Kitas Europos Sąjungos pavyzdys yra nauja Šengeno informacinė sistema SIS II stebimųjų sąrašas, kuris yra naudojamas, norint sukaupti ir skleisti informaciją apie ekstradiciją, apie

[22] Coesys eBorder Solutions for National Security - Providing effective border control. Helping citizens to travel freely and securely, 2007. http://www.gemalto.com/brochures/download/coesys_border.pdf

piliečius, kuriuos buvo atsisakyta įleisti į Europos Sąjungą ir apie asmenis, gavusius bet kokį Europos arešto orderį ar sekamiems dėl nusikalstamos veikos. Panaši biometrinė sistema yra naudojama JAV, pavadinimu US - VISIT[23] programa.

Šitos naujos programos užtikrina, kad sienos kontrolė turės peržiūrėti keliautojo pirštо atspaudus ir pritaikyti elektroninį tikrinimą pagal kelis biometrinius baltus ar juoduosius sąrašus.

Keleivių patikrinimo palengvinimas

Negana to, kad būtina reaguoti į padidintus saugumo reikalavimus su naujų e-Paso technologijų įdiegimu, lėktuvų keleivių skaičiaus augimas reiškia, kad valdžios organams būtina surasti būdą palengvinti keleivių tikrinimą. Taip pat laukiama, kad nauji didelės talpos lėktuvai, tokie kaip A380, pablogins šią spūsties problemą oro uosto sienos kontrolėje.

Numatomi sprendimai, kaip, pvz., elektroniniai bilietai, savarankiškas užsiregistravimas, įlaipinimas ir greitosios juostos sienos kontrolėje yra vis labiau įgyvendinami. Iniciatyvos, kaip Tarptautinė Oro Transporto Asociacija (IATA) SPT (Keleivių Kelionės Supaprastinimas) ar privačios iniciatyvos, tokios kaip registruotų keliautojų programos, taip pat siekia pateikti paspartintą saugumo patikrinimą teisėtiems keleiviams.

Taip pat manoma, kad biometrinis e-Paso patikrinimo procesas, apimantis ir RF lusto skaitymą ir visas naujas biometrines variacijas, pridės bent jau 50 % prie vidutinio patikrinimo laiko, o kai kuriais atvejais jį net padvigubins. Tokiu būdu Biometrinių elektroninių dokumentų įvedimas padidins saugumą, bet taip pat ir pailgins eiles prie sienų.

Yra du sprendimai šiai problemai: arba įdarbinti daugiau tikrinančių pareigūnų, arba įdiegti automatizuotas sienos kontrolės sistemas, kad būtų palengvintas sienos kirtimas.

Projektas „e.sienos vartai“

„E. sienos Vartai“ sumažina apžiūros laiką ir žmogaus įsikišimą, kad padėtų valdžios organams susidoroti su padidėjusiu oro keleivių skaičiumi. Ši vartų sistema yra savitarnos paslauga, ir didžiąją laiko dalį kelios stotys yra prižiūrimos tik vieno inspektoriaus. Ši vartų sistema padarys galą ilgoms eilėms oro uosto sienos kontrolėje[24].

Kita vertus, sienų apsaugojimas yra būtinas, ir yra nenuginčijamai reikalingas šiandieniame pasaulyje. Štai kodėl buvo išplėsta patirtis didinant dokumentų saugumą, kad išvystytų „e-Sienos Vartus”, kurie taiko išsamiausias procedūras saugumo, patikrinimo ir saugaus keleivių identifikavimo atžvilgiu.

Viso proceso metu keliautojas yra instruktuojamas pagalbos ekranų, kurie pataria jiems kaip elgtis. Keliautojas padeda kelionės dokumentą ant dokumento skaitytuvo. Sistema patikrina paso ir vartotojo teisę eiti per vartus duomenų bazėje. Toliau sistema įvykdo pilną dokumento autentiškumo

[23] Most M.Biometrics and Border Control Beyond US-VISIT. http://magazine.digitalidworld.com/Sep04/Page18.pdf
[24] Coesys eBorder Solutions for National Security - Providing effective border control. Helping citizens to travel freely and securely, 2007. http://www.gemalto.com/brochures/download/coesys_border.pdf

patikrinimą ir nuskaito visą dokumentą. Po to, kai keliautojas įeina į vartus, sistema tikrina, ar yra tik vienas asmuo viduje. Tada keliautojas atsistoja prieš kamerą ir/arba uždeda abu smilius ant piršto atspaudo skaitytuvo.

Kitame etape atliekamas veido atpažinimas ir/arba piršto atspaudo palyginimas, kad būtų patikrinta keliautojo tapatybė pagal biometrinius duomenis, arba pagal biometrinę keliautojų registracijos duomenų bazę. Tuo pačiu metu, asmeninė ir biometrinė informacija gali būti panaudojama atliekant elektroninį patikrinimą. Sistema atlieka elektroninį keliautojo patikrinimą patenkant ir išvykstant iš šalies pagal tekstinį arba AFIS stebimųjų sąrašą (SIS-2, VIS, Interpol ir tt.). Sistema taip pat leidžia keleivio įvažiavimų / išvažiavimų iš teritorijos stebėjimą. Tai yra labai svarbus informacijos apie keliautoją šaltinis, kuris gali būti panaudojamas daugybe būdų, taipogi ir policijos tyrimams.

Pagaliau, jei visos kontrolės praeinamos sėkmingai, atidaromos antros durys. Jei per kontrolės procesą iškyla problemų, atidaromos šoninės durys, ir keliautojas nukreipiamas į sienos kontrolės postą.

Inspektorius gali kontroliuoti ir prižiūrėti, kas vyksta keliuose vartuose (pavyzdžiui, ketveri vartai vienam inspektoriui) stebėjimo ekrane. Kiekvieną kartą, kai asmuo įeina pro vartus, inspektorius yra įspėjamas ir gali sekti apsaugos kontrolės procesą žingsnis po žingsnio, ir pagaliau jam pranešama apie sėkmingą ar nesėkmingą apsaugos kontrolės baigtį. Inspektorius yra taip pat įgaliotas kontroliuoti ir valdyti vartus (Įėjimų/išėjimų blokavimas ir t.t.).

Automatizuota sienos kontrolė: geresnių paslaugų ir padidinto saugumo pasiūlymas visuomenei

Palyginus su tradiciniu sienos kontrolės procesu, automatizuotos procedūros siūlo kelis privalumus keliautojams, valdžios organams, avialinijoms ir oro uostams, pavyzdžiui:

Supaprastinta kelionė

- Greita, paprasta ir nekelianti streso kelionė visiems nepavojingiems asmenis;
- Greitesnis sienų kirtimas;

Darbuotojai, susitelkę ties „pavojingomis" grupėmis

- Apžiūros laiko ir darbuotojų-inspektorių judėjimo iš vietos į vietą sutrumpinimas, siekiant susidoroti su padidėjusiu keleivių skaičiumi;
- Žmogiškojo faktoriaus įtakos sumažinimas, nes darbuotojai gali būti panaudoti efektyviau, susitelkdami ties „adatomis šieno kupetose".

Labai saugi ir sisteminga kontrolė

- Aukščiausias saugumo procedūrų lygis yra pritaikomas kiekvienam keliautojui;
- Išvengiama bet kokios rūšies žmogaus klaidos;

Projekto „e.sienos Vartai“ sprendimai

E. sienos sprendimas yra pilna Sienos Kontrolės sistema. Ji gali būti pritaikoma visose skirtingose sienos kontrolės situacijose, įskaitant ir oro uostus, uostus ir pan.

E.siena yra pritaikoma įėjimo/grįžimo patikrinimui pagal biometrinį palyginimą: avialinijoms, kelionėms jūra ar traukiniu.

Registracijos sprendimas gali būti panaudotas, kad užregistruotų keliautojus, įgaliotus panaudoti „e.sienos Vartais“.Registracija siekia pirmiausia pateikti apklausą ir būtiną tapatybės patikrinimą, kad garantuotų, kad keliautojas atitinka programos narystės taisykles. Tada sistema įrašo į atmintį keliautojo asmeninius duomenis, veidą ir piršto atspaudus, ir išsaugo šią informaciją biometrinėje keliautojų registracijos sistemoje.

Atliekant kontrolę, „e. sienos Vartai“ patikrinama keliautojo narystė, ir sutikrinami jo piršto atspaudai su biometrine registracijos duomenų baze.

(State-of-the-art) dokumentų autentiškumo nustatymas

„e. sienos Vartai“ siūlo tiksliausią elektroninį ir grafinį saugumo patikrinimą, kad garantuotų dokumento autentiškumą:

1. Naujausi ICAO lusto autentiškumo nustatymo mechanizmai:
    a) BAC, aktyvus autentikavimas, pasyvus autentikavimas;
    b) EAC: lusto/terminalo autentikavimas, duoda saugų priėjimą prie piršto atspaudų;
2. Sertifikuotos saugumo grandinės patikrinimas prieš bet kokį naudojimą.

Dokumentų skaitytuvai e.sienos stočiai ir e.sienos Vartams, kurie gali pritaikyti automatinį grafinį tikrinimą (pavyzdžiui, vaizdų atpažinimas) po bet kokiu apšvietimu (infraraudonoji, UV, matoma šviesa, koaksialinė šviesa).

Griežtas biometrinis identifikavimas

1) “State-of-the-art “ piršto atspaudo sensoriaus tikslumas:
    a) Naudojama geriausia pramonėje padirbintų aptikimo technologija, kuri nustato klastotę ir padirbtus pirštus, tokius kaip lateksiniai, silikoniniai ir želatininiai;
    b) Toleruojami odos pakitimai: sausa, šlapia, purvina, taip pat atpažįstami senėjimo procesai.
    c) Dirba su ryškia supančia šviesa;
2) Efektyvi veido pripažinimo technologija:
    a) Su daugiafunkcine kameros sistema ir automatiniu aukščio reguliavimu;
    b) Atpažinimo patikimumas garantuojamas dėl nuoseklaus natūralaus apšvietimo;

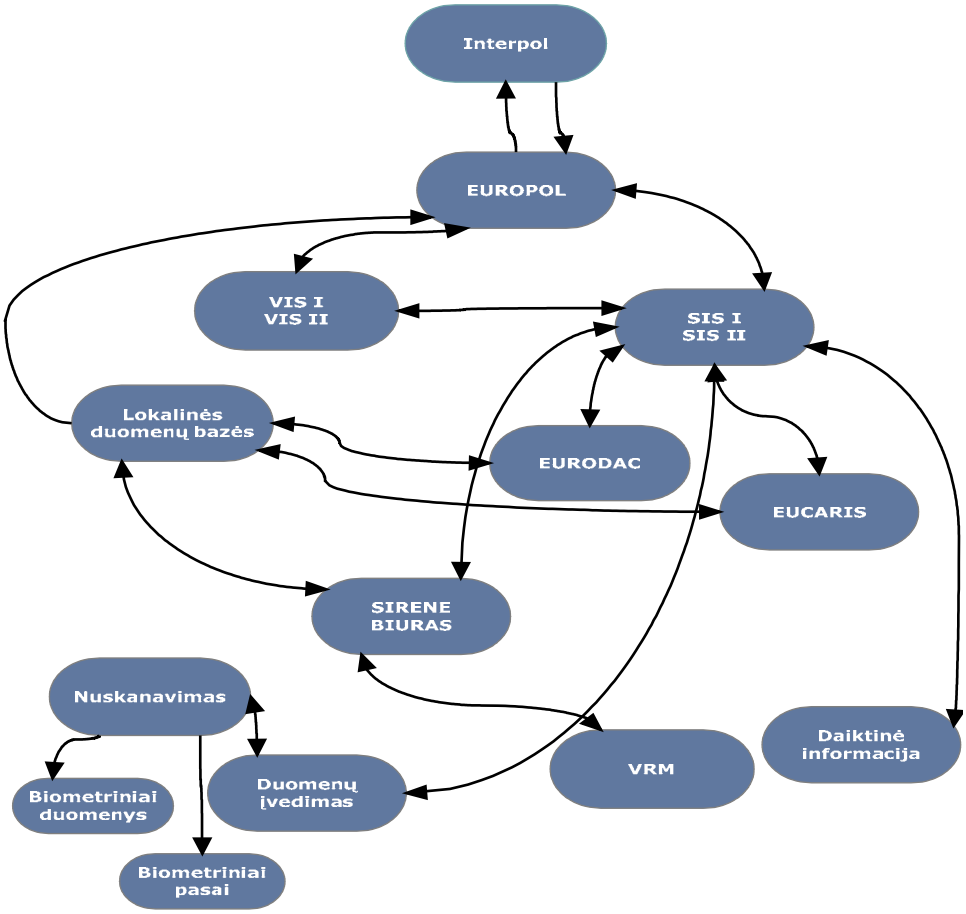
3) Didžiulis neteisingų priėmimo ir atmetimo normų sumažinimas (FAR ir FRR[25]) dėl multimodalinės biometrinės sistemos galimybės (Veidas + 2 Piršto atspaudai).

Prieinama visiems keliautojams

1) „e.sienos Vartai“ gali būti naudojamas su visais egzistuojančiais e-Pasais ir yra suderinamas su plačiu spektru elektroninių kelionės dokumentų, tokių kaip vizos ir asmens tapatybės kortelės. Tai garantuoja, kad vartai funkcionuos su plačiausia įmanoma populiacija.
    a) Suderinamas su visais ISO 14443 tipo A/B lustais.
    b) Suderinamas su visais ICAO 9303 dokumentais.
    c) Sistema ir skaitytuvai patikrinti pagal ICAO operacinio suderinamumo testus.
2) Kai reikia „e-sienos Vartai“ gali veikti tiktai su biometriniais duomenimis (pavyzdžiui, žmonės, neturintys visų pirštų);
3) specialus vartų projektas siūlo pilną invalidų vežimėlių prieigą.

Žemiau yra pateikiamas e.sienos integruotas informacijos bei biometrinių duomenų perdavimo tinklo hipotetinis modelis, apimantis globalių pasaulio informacinių mazgų tarpusavio sąveikas. Modelis buvo sukurtas remiantis konferencijų bei VSAT veiklos efektyvumo gerinimo vidaus naudojimo medžiaga, siekiant pavaizduoti asociacinius ryšius tarp SIS, VIS, EUROPOLO, INTERPOLO institucijų integruojant į esamą struktūrą VRM bei SIRENE biurus; užtikrinant biometrinių duomenų mainus (3 pav.)

[25] A Recent Study on Anti-Spoofing Methods in Biometrics.
http://www.inderscience.com/www/newsletter/2008/autumn08_biometrics.pdf



3 pav. E. sienos informacijos tinklas

Sudaryta autorės

2.2. Biometrinės sistemos analizė

Biometrija – tai automatiniai asmens atpažinimo metodai, pagrįsti fiziologinėmis arba elgsenos charakteristikomis. Tarp charakteristikų ir savybių tiksliausios yra šios sistemos: veido, pirštų atspaudų, plaštakos geometrijos, akies rainelės, akies ragenos, balso bei kapiliarų (kraujagyslių). Biometrinės technologijos tampa vis platesne erdve aukšto lygio saugumo sistemose asmens tapatybės patvirtinimo bei identifikavimo sprendimams. Šia biometrine technologija pagrįsti sprendimai yra pajėgūs apsaugoti ir užtikrinti slaptumą tiek konfidencialių bankų finansinių transakcijų, tiek ir asmeninių duomenų. Biometrinės technologijos poreikis itin svarbus valstybiniams, valdžios, armijos bei komerciniams objektams[26].

Biometrijoje skiriami du tapatumo nustatymo metodai – **identifikacija ir verifikacija.** Identifikacijos metu informacinė sistema bando surasti, kam priklauso pateiktas pavyzdys, sulygindamas jį su duomenų baze **(one-to-many)**. Kai reikia nustatyti asmenį, palikusį pėdsakus, pirštų atspaudus, ar atpažinti lavoną, kalbame apie **identifikaciją.** Verifikacija – tai procesas, kurio metu biometrinė sistema bando patvirtinti asmens tapatybę sulygindama du pavyzdžius **(one-to-one)**.

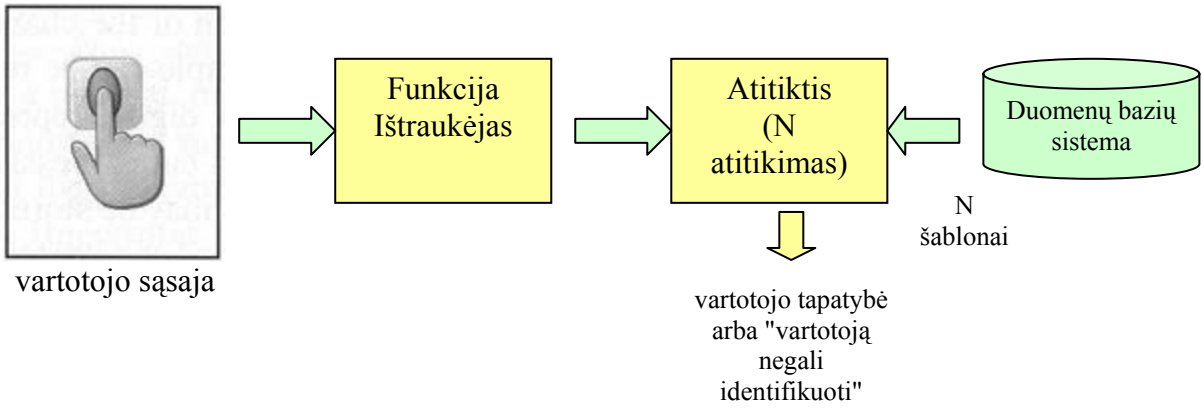
[26] P. Zubavičius. Biometrinės autentifikavimo sistemos. http://pasidaryk.shakes.lt/biometrines-autentifikavimo-sistemos/

Beveik visos sistemos gali nustatyti ar suderinti asmens biometriją ir biometrinį šabloną per kelias sekundes.

Taigi biometrinė sistema iš esmės yra modelių atpažinimo sistema. Ši sistema apima tris aspektus: duomenų įsisavinimą ir pirminį apdorojimą, duomenų pateikimą, ir sprendimo priėmimą. Tokiu būdu galima palyginti specifinę fiziologinių ir elgesio charakteristikų grupę su charakteristikomis, prieš tai išgautomis iš žmogaus, ir atpažinti paskutiniąsias. Skaitmeninis atvaizdavimas, įrašytas į duomenų bazę, kuri aprašo fizinio bruožo savybes ar ypatybes, yra apibūdinamas kaip modelis. Jis pasiekiamas per ypatybių išgavimo algoritmą. Biometrinės sistemos tradiciškai naudojamos trimis skirtingais būdais: fizinė priėjimo kontrolė apsisaugojimui nuo neįgaliotų asmenų priėjimo prie tam tikrų vietų ar kambarių, loginė priėjimo kontrolė, saugant tinklus bei kompiuterius, ir laiko bei lankomumo kontrolė[27].

Autentifikavimo procedūra, tai yra būdas „leisti sistemai atpažinti vartotojo tapatybę" informacijos technologijoje, biometrinėse sistemose gali būti vykdomas dviem metodais:

Identifikacija. Šį metodą sudaro teisingos nežinomo asmens tapatybės parinkimas iš registruotų tapatybių duomenų bazės (4 pav.).



4 pav. Identifikacija

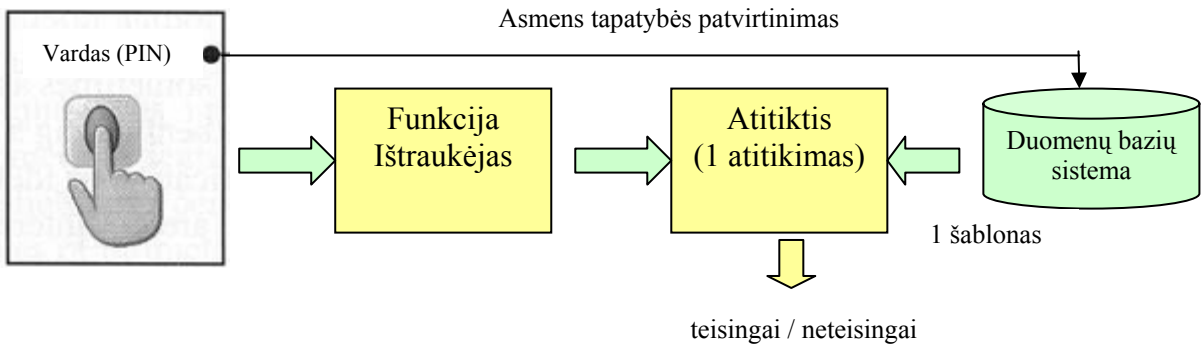
Šaltinis: Dessimoz D., Richiardi J., Champod C., Drygajlo A. Multimodal Biometrics for Identity // State-of-the-Art Research Report PFS 341-08.05 (Version 2.0). http://www.europeanbiometrics.info/images/resources/90_264_file.pdf

Tai vadinamasis „vienas iš daugelio" atitikimo procesas, nes sistemai liepiama atlikti palyginimą tarp asmens biometrikos ir visų biometrinių modelių, esančių duomenų bazėje. Sistema gali pateikti arba „geriausią atitikmenį", arba ji gali pateikti visus galimus atitikmenis, ir išrikiuoti juos atitikimo tvarka. Galimi du modeliai – pozityvus ir negatyvus atpažinimas, kaip aprašyta taikymų sistematikoje. Pozityvus atpažinimas nustato, ar asmuo tikrai yra specifinėje duomenų bazėje. Šis metodas taikomas, kai norima išvengti, kad ta pačia tapatybe naudotųsi daug vartotojų. Negatyvus atpažinimas nustato, ar

[27] Dessimoz D., Richiardi J., Champod C., Drygajlo A. Multimodal Biometrics for Identity // State-of-the-Art Research Report PFS 341-08.05 (Version 2.0). http://www.europeanbiometrics.info/images/resources/90_264_file.pdf

asmuo nėra „stebimųjų sąrašo" duomenų bazėje. Toks metodas taikomas, pavyzdžiui, kai norima nustatyti, ar asmuo neregistruotas keliomis tapatybėmis.

Verifikacija. Šis metodas patikrina, ar asmuo tikrai yra tas, kuo prisistato (5 pav.).



5 pav. Verifikacija

Šaltinis: Dessimoz D., Richiardi J., Champod C., Drygajlo A. Multimodal Biometrics for Identity // State-of-the-Art Research Report PFS 341-08.05 (Version 2.0). http://www.europeanbiometrics.info/images/resources/90_264_file.pdf

Tai vadinamasis „vienas iš vieno" atitikimo procesas, nes sistemai liepiama atlikti palyginimą tarp asmens biometrikos ir tik vieno išrinktojo modelio, esančio centralizuotoje arba išskirstytoje duomenų bazėje, pvz., tiesiai ant lusto ant atpažinimo dokumento. Šis metodas taikomas, kai siekiama apsaugoti ir užkirsti specifinius priėjimus akivaizdžiai kooperuotiems vartotojams[28].

Biometrinės sistemos taikymo aplinkos labai įvairios, todėl buvo pasiūlyta sistematika šioje srityje. Jos skirstomos į šešias kategorijas:

- *Tiesioginis prieš paslėptą*. Jei vartotojas žino apie jo biometrinių charakteristikų įsisavinimą, tada taikymas vadinamas tiesioginiu; jeigu ne, tada taikymas vadinamas paslėptu.
- *Įprastas prieš neįprastą*. Vartotojas pateikia savo biometrines charakteristikas kiekvieną dieną, taikymas vadinamas įprastu (po trumpo laiko tarpo); jei pateikimo dažnumas nedidelis, taikymas laikomas ne įprastiniu.
- *Prižiūrimas prieš neprižiūrimą*. Jei vartotojas per procesą prižiūrimas ir pamokomas prižiūrėtojų, tai taikymas laikomas prižiūrimu; jeigu ne, tai taikymas vadinamas neprižiūrimu.
- *Standartinė prieš nestandartinę aplinką*. Jei visos sąlygos gali būti kontroliuojamos ir jeigu veiksmas vyksta patalpoje standartinėmis sąlygomis, laikoma, kad taikymas vyksta standartinėje aplinkoje; jeigu ne, tuomet laikoma, kad jis vyksta nestandartinėje aplinkoje.
- *Viešas prieš privatų*. Jeigu vartotojai yra sistemos klientai, tai taikymas yra viešas; jeigu vartotojai yra darbuotojai, tuomet taikymas laikomas privačiu.

[28] J. L. Wayman, A. K. Jain, D. Maltoni, and D. Maio, "An introduction to biometric authentication systems," in Biometric Systems: Technology, Design and Performance Evaluation, J. L. Wayman, A. K. Jain, D. Maltoni, and D. Maio, Eds. London: Springer-Verlag, 2005, ch. 1, pp. 1–20.

- *Atviras prieš uždarą*. Jeigu sistema dirba su absoliučiai privačiais formatais, taikymas vadinamas uždaru; jeigu sistema gali keistis bet kuriais duomenimis su kitomis biometrinėmis sistemomis naudojamomis kituose taikymuose, tada taikymas laikomas atviru.

2.2.1. Biometrinės operacijos, duomenų apdorojimo žingsniai

Visiems biometriniams moduliams biometriniai duomenys pertvarkomi pagal apdorojimo žingsnius, aprašytus toliau[29]:

- *Įsisavinimo užfiksavimas*. Biometriniai duomenys (balsas, elektroninis parašas, piršto atspaudas), kitaip vadinami biometrine prezentacija, pervedami į skaitmeninę formą per įvesties mechanizmą (mikrofoną, bloknotą, piršto atspaudą ir pan.) ir išsaugomi atmintyje.
- *Pirminis apdorojimas*. Įsisavintieji duomenys paruošiami ypatybių išgavimui. Tai paprastai daroma, kad normalizuotųsi duomenys ir pasišalintų paklaidos ar korupcijos šaltiniai sistemos modelyje. Tarkim, kalbai bus naudojamas DC komponentų pašalinimas ir tylos aptikimas bei pašalinimas. Parašams, šis žingsnis numatytų parašo išvertimą pradžioje į (0, 0) koordinates ir pavyzdžio perdarymą. Pirštų atspaudams, šis žingsnis numato rotacijos normalizavimą ir retinimą.
- *Ypatybių išgavimas*. Diskriminacinės savybės išgaunamos iš pirmiau apdorotų duomenų. Nors ypatybės labai skiriasi kiekviename biometriniame modelyje, pagrindinis teisingas principas išlieka vienas: šis apdorojimo žingsnis paprastai sumažina įeinančių duomenų apimtį, ir leidžia sukurti pilną ypatybių pavaizdavimą, ir klasifikatorius galės jas naudoti modelio atpažinimui.
- *Poprocesinis apdorojimas*. Ypatybės normalizuojamos, kad būtų pašalintos paklaidos, arba kad jas galima būtų adaptuoti klasifikatoriui. Ypatybių srities paklaidų pašalinimo pavyzdys yra kalbos pašalinimas, kai perdavimo kanalo poveikiai gali būti kompensuojami. Be to, kai kurie klasifikatoriai, kaip neutralūs tinklai ar palaikymo mechanizmai veikia geriausiai, kai jų įvesties mechanizmai turi lyginamąsias dinamines sritis.
- *Modelio sukūrimas*. Vartotojų modeliai sukuriami iš bandomųjų ypatybių rinkinių, norint išgauti bendrą vartotojo, kuris bus naudojamas tolesniems palyginimams, atvaizdavimą. Daug algoritmų ir procedūrų gali būti naudojami priklausomai nuo ypatybės ir modelio klasės. Kalbai ar parašams jie gali apimti mokomuosius *Gaussian* sumaišymo modelius (GMMs), naudojant pasikartojančias procedūras.

[29] R. Clarke, "Human identification in information systems: Management challenges and public policy issues," Information Technology and People, p. 6–37, 1994.

- *Pagrindo modelio sukūrimas*. Pagrindo modelis, dar vadinamas pasaulio modeliu arba anti – modeliu, reikalingas kai kuriems biometriniams algoritmams, kad būtų galima normalizuoti vartotojų prisistatymą. Jie reprezentuoja "vidutinį" sistemos populiacijos naudotoją. Jie paprastai sukuriami, suvienijant daug skirtingų vartotojų savybių.
- *Modelio laikymas*. Kai vartotojų modelių parametrai nustatomi, jie patalpinami saugioje aplinkoje tolesnėms biometrinėms operacijoms.
- *Modelių derinimas*. Biometrinė prezentacija palyginama su konkretaus vartotojo biometriniu modeliu. Paprastai tada nustatomas prezentacijos rezultatas, kuris yra susijęs su tuo, kiek panašus šis konkretus vartotojas su prezentacijos šaltiniu. Priklausomai nuo modelio ir klasifikatoriaus tipo, šis procesinis žingsnis gali skirtis. Pavyzdžiui, GMM klasifikatorius naudos panašumo rezultatą. Šiai prezentacijai, derinimo rezultatai paprastai įvertinami kaip prezentacijos rezultato reitingas, atsižvelgiant į konkretaus vartotojo modelį, lyginant su prezentacijos rezultatu, atsižvelgiant į pagrindo modelį. Tokiu būdu iškeliamas hipotetinis patikrinimas, kur hipotezė yra "ar ši prezentacija yra panašiausia į būtent šito vartotojo, iš visų vartotojų, esančių pagrindinėje populiacijoje?"
- *Slenksčio skaičiavimas*. Kelios prezentacijos, priklausančios konkrečiam vartotojui, ir kelios prezentacijos, nepriklausančios šiam konkrečiam vartotojui (melagingos prezentacijos), palyginamos su to vartotojo modeliu, kad būtų nustatyta griežta riba (slenkstis), kurią pasiekus, prezentacija nebus laikoma priklausančia šiam konkrečiam vartotojui. Slenkstis gali būti nepriklausomas nuo vartotojo (sistemos ribose) arba priklausomas nuo vartotojo – šiuo atveju gaunama akivaizdžiai mažiau klaidų. Vėlgi, yra daug slenksčio skaičiavimo procedūrų, bet daugelis veikia prezentacijos rezultato srityje.

Ne visiems biometriniams moduliams reikia slenksčio, pavyzdžiui, piršto atspaudo derinimui slenksčio nereikia.

Toliau paminėti apdorojimo žingsniai bus naudojami aukštesnio lygio biometrinėse operacijose[30].

- Užregistravimas.

Vartotojas užregistruojamas biometrinėje sistemoje. Tam tikras konkretaus vartotojo biometrinių prezentacijų skaičius įvedamas, apdorojamas, perverčiamas į ypatybes, tuomet vėl apdorojamas, tada naudojamas vartotojo modeliui ir pasaulio modelio adaptavimui. Vartotojo modelis kartu su melagingomis prezentacijomis įgalina išgauti slenkstį šiam vartotojui. Išsaugomas naujasis modelis, jei reikia, kartu su slenksčio modeliu.

- Patikrinimas.

[30] Dessimoz D., Richiardi J., Champod C., Drygajlo A. Multimodal Biometrics for Identity // State-of-the-Art Research Report PFS 341-08.05 (Version 2.0). http://www.europeanbiometrics.info/images/resources/90_264_file.pdf

Vartotojo tapatybė patikrinama, palyginus pateiktus biometrinius duomenis su šio vartotojo modeliu. Taip biometriniai duomenys įsisavinami, apdorojami, perverčiami į ypatybes, ir vėl apdorojami, tuomet derinami su vartotojo modeliu, o rezultatas palyginamas su turima „klaida", suskaičiuota šiam vartotojui ar „klaidos" lygiui.

- Identifikavimas.

Vartotojų modelių duomenų bazėje ieškoma panašiausio biometrinės prezentacijos šaltinio. Taip biometriniai duomenys įsisavinami, apdorojami, perverčiami į ypatybes, ir vėl apdorojami, tuomet derinami su visais galimais vartotojo modeliais. Vartotojo modelis, turintis geriausią prezentacijos rezultatą, laikomas prezentacijos šaltiniu.

Standartai

Tarptautiniai biometrikos standartai tobulinami, ir daugelis yra jau prieinami. Jie palaiko operacinį suderinamumą ir duomenų mainus tarp taikymų ir sistemų, tokiu būdu vengdami problemų ir kainų, kylančių iš patentuotų sistemų.

Tapatumo dokumentams, tokiems kaip pasai, tarptautiniai standartai yra būtini, kad biometrinis patikrinimas galėtų būti įvykdytas.

Operacinio suderinamumo pavyzdys yra tai, kad visi e-Pasai, išleisti bet kurios šalies, yra lengvai skaitomi skaitytuvų, esančių prie sienų. Neseniai pasų skaitytuvų operacinio suderinamumo testas buvo atliktas Japonijoje 2005 m. kovo 8-10[31]. Svarbiausias testo tikslas buvo "garantuoti, kad visi pasai būtų perskaityti visuose sienų punktuose, nepriklausomai nuo to, kas gamino pasus ir gamino skaitytuvus", atitinkamai pagal ICAO specifikaciją ir reikalavimus. 16 skaitytuvų pardavėjų ir 30 pasų pardavėjų (gamintojų) (gaminantys apytiksliai 100 skirtingų pasų) dalyvavo šiuose testuose. Testai parodė, kad vidutiniškai, 82.9 % visų pasų galėjo būti perskaityti, kai tuo metu, kiekvienas skaitytuvas galėjo perskaityti 79.5 % visų pasų.

Be to, Java paremtiems sprendimams reikėjo mažiausiai laiko perskaityti duomenis, turėtus luste pasyviame tapatumo nustatymo būde: 2 sekundės su 20 kB paveikslu ant lusto. Jei naudojama ir Pagrindinė Prieigos Kontrolė, skaitymo laikas padidėja iki 20 sekundžių.

2005 m. lapkritį buvo atliktas kitas pasų operacinio suderinamumo testas Singapūre[32]. Organizatoriai turėjo 140 e-Paso pavyzdžių ir 45 skaitytuvų testui, bet tiktai 95 e-Pasų ir 29 skaitytuvų rezultatai buvo publikuoti:

22 skaitytuvai iš 29 turėjo aukštesnį operacinio suderinamumo procentinį lygį negu 90 %, ir tiktai 1 skaitytojas iš likusių 7 turėjo operacinio suderinamumo procentinį dydį žemesnį nei 79 % (apytiksliai 55 %).

---

[31] Biometric Technology Today, "Part 1: Biometrics and ePassports," Bio-metric Technology Today, Nr. 6, p. 10–11, 2005.
[32] http://www.securitydocumentworld.com

Kitas operacinio suderinamumo pavyzdys yra biometrinės sistemos efektyvumas, dirbant su mainų formatais. MIT (Detalių Šablono Operacinio suderinamumo Testas) projektas išbandys ir patobulins piršto atspaudo biometrikos operacinį suderinamumą. Svarbiausi MIT projekto tikslai yra[33]:

1) Apibrėžti kriterijus operacinio suderinamumo išbandymui;
2) Vystyti piršto atspaudo atvaizdų duomenų bazę,
3) Vystyti bandomąją terpę, įgalinančią automatizuotą ir pakartotinį išbandymą piršto atspaudo detalių operacinio suderinamumo, ir taip pat tyrimą to, kaip faktoriai, tokie kaip atvaizdo kokybė, yra svarbūs operaciniam suderinamumui;
4) Įtraukti pagerinimo žingsnį, kuriuo išbandytų sistemų operacinis suderinamumas pagerėtų;
5) Numatyti operacinio suderinamumo išbandymą būsimų pardavėjų būsimoms sistemoms.

1 lentelėje trumpai aprašomi biometrikos standartai.

1 lentelė. Biometrikos standartai

Standartai	Paskirtis
1. BioAPI	BioAPI specifikacijos 1.1 versija ketina skatinti operacinį suderinamumą tarp pardavėjų. BioAPI 1.1 specifikacija apibrėžia du API: Taikomojo programavimo sąsaja (API), kuri parodo struktūros funkcionalumą taikymui, ir Paslaugų teikėjo sąsają (SPI), kuri parodo biometrinį funkcionalumą struktūrai.
2. CBEFF	Bendras Biometrinis Bylų Apsikeitimo formatas (CBEFF) yra standartas, kad būtų galima keistis biometriniais duomenimis tarp sistemų ir organizacijų. Šis formatas numato, kad biometriniai duomenys turi būti užkoduoti trijose dalyse: Standartinė Biometrinė Antraštė (SBH), Biometrinis Specifinis Atminties Blokas (BSMB), kuris turi biometrinius duomenis, ir Parašo Blokas, kuris yra BSMB ir antraštės mišinys.
3. ANSI X9.84	ANSI X9.84 standartas, Biometrinės Informacijos Valdymas ir Saugumas Finansinių paslaugų Pramonei, apibūdina saugumo ypatybes, kurios reikalingos biometriniam patikrinimui finansinėms paslaugoms. Pagrindiniai Saugumo reikalavimai: biometrinių duomenų ir patikrinimo rezultatų vientisumas, biometrinių duomenų šaltinis ir gavėjas turi būti autentifikuoti, biometrinių duomenų konfidencialumas
4. ISO/JTCI/SC37	Tarptautinė Organizacija Standartizacijai (ISO) ir Tarptautinė Elektrotechnikos Komisija (IEC), sukurta 1980-ųjų pradžioje, Jungtinis Techninis Komitetas Vienas (JTC1), kuris turi kelis aktyvius pakomitečius, kurių keli įdomūs biometrinei sričiai. SC17, Kortelėms ir Asmeniniam Identifikavimui, SC27 IT Saugumo Technikai ir SC37 Biometrikai.
5. ICAO	Tarptautinė Civilinės aviacijos Organizacija (ICAO) ir Tarptautinė Standartizacijos Organizacija (ISO) sujungė savo kompetencijas tam, kad publikuotų Doc 9303 specifikacijas trimis atskiromis bendros struktūros dalimis: pasams, vizoms ir oficialiems kelionės dokumentams (kortelėms). ICAO paruošė rekomendacijas apie biometrinių duomenų išdėstymą kompiuteriu apdorojamuose kelionės dokumentuose. Čia nurodomi svarbiausi reikalavimai biometrikai: inkorporacija "optimaliai suspausto" veido atvaizdo, ir papildomai, pagal valstybių nuožiūrą, pirštо atspaudo ir/ar rainelės atvaizdo.

1 lentelės tęsinys kitame puslapyje

[33] http://www.MITproject.com

1 lentelės tęsinys

Standartai	Paskirtis
6. Wavelet Scalar Quantization (WSQ)	FTB pasiūlė Wavelet Scalar Quantization (WSQ) atvaizdo suspaudimo algoritmą kaip būdą standartizuoti pilko masto piršto atspaudo pervedimą į skaitmeninę formą ir suspaudimą. WSQ Koduotojas. Jis susideda iš discrete wavelet transform (DWT) skaidymo, skaliarinio kvantavimo, ir Huffman entropijos kodavimo.WSQ Dekoderis. Jis turi sugebėti iššifruoti šiuos tris procesus ir visus jų variantus, kurie yra leistini pagal bendrą specifikaciją.
7. JPEG2000	Jungtinė Fotografinė Ekspertų Grupė (JPEG) nuo 1988 pasiūlė populiarų atvaizdo suspaudimo standartą, kurio efektyvumas buvo padidintas su naujo JPEG-2000 standarto priėmimu, naudojamo tarp kitų skaitmeniniams archyvavimo taikymams. JPEG 2000 standartas yra sudarytas iš dvylikos dalių, tarp kurių šešios buvo priimtos kaip ISO standartai.

Sudaryta autorės pagal Dessimoz D., Richiardi J., Champod C., Drygajlo A. Multimodal Biometrics for Identity // State-of-the-Art Research Report PFS 341-08.05 (Version 2.0).
http://www.europeanbiometrics.info/images/resources/90_264_file.pdf

2.2.2. Biometrijos funkcionalumas ir efektyvumas, bei jos panaudojimas pasienio kontrolėje.

Visos biometrinės technologijos veikia praktiškai vienodai. Pirma, sistema išsaugo biometrinės charakteristikos pavyzdį (rašymo procesas). Įrašymo metu sistemos gali paprašyti kelių pavyzdžių tam, kad sukurtų tikslesnį biometrinės charakteristikos vaizdą. Po to gauta informacija apdorojama ir paverčiama skaitmeniniu kodu. Be to, sistema gali atlikti papildomus veiksmus tam, kad priskirtų biometrinį pavyzdį asmeniui. Sakykime, asmens kodas (PIN) priskiriamas nustatytam pavyzdžiui. Visose sistemose sutapatinimas vyksta keturiomis stadijomis: Įrašymas – fiziologinis arba elgesio pavyzdys įrašomas sistemoje; Išskyrimas – unikali informacija išrašoma iš pavyzdžio ir sudaromas biometrinis pavyzdys; Sulyginimas – išsaugotas pavyzdys sulyginamas su pateiktu; Sprendimas – sistema sprendžia, ar sutampa pavyzdžiai.

Biometrinės technologijos saugumo atžvilgiu naudingos identifikavimui ir verifikavimui. Prieš pradedant naudoti biometrines technologijas reikia įvertinti turimas galimybes, sistemos darbą. Tikslumas, apgavystės galimybė ir vartotojų pripažinimas taip pat yra svarbūs momentai. Didelę įtaką turi ir aukšta tokių sistemų realizavimo kaina[34].

Akies rainelės identifikacija. Akies rainelės atpažinimo technologija priklauso nuo ryškaus spalvoto žiedo. Rainelė turi maždaug 266 skiriamųjų charakteristikų, tame tarpe ir vagotumus, žiedus, raukšles, strazdanas. Paprastai apytiksliai, 173 iš tokių skiriamųjų charakteristikų naudojamos šablonui

[34] Kochems A., Schwartz A. Biometric Technologies: Security, Legal, and Policy Implications by Paul Rosenzweig. http://www.heritage.org/Research/HomelandSecurity/upload/65326_1.pdf

sukurti. Aštunto neštumo mėnesį formuojasi akies rainelė ir nesikeičia per visą gyvenimą, išskyrus žaizdas.

Šitos sistemos naudoja mažą baltai-juodą kamerą, rainelės aukšto ryškumo vaizdą. Algoritmai tuomet apibrėžia rainelės ribą ir sukuria ant vaizdo tinklelio koordinates. Visos parinktos charakteristikos zonų viduje saugomos duomenų bazėse kaip individualus biometriniai šablonai.

Rainelės atpažinimo technologija palyginus patogi ir greičiau aptarnauja didelį žmonių srautą. Bet spalvoti lęšiai arba stiprus akiniai trukdo efektyviam atpažinimui pagal akies rainelę. Riški šviesa ir atspindys daro neigiamą įtaką kameroms. Yra dar viena problema, žmonės su silpnu regėjimu negali sufokusuoti akies žvilgsnį į kamerą. O žmonės su glaukoma ar katarakta negali patikimai panaudoti akies rainelės technologiją.

Rankos geometrija. Rankos geometrija priklauso nuo aukščio, pločio, pirštų ilgio, atstumo tarp sąnarių ir pirštų sąnarių formos išmatavimų. Panaudojant optines kameras ir šviesos diodus, kurie turi veidrodžius ir atšvaitas, du ortogonalus, daromas delno galinės dalies ir šono dviejų dimensijų vaizdas. Šitų vaizdų pagrindu, 96 išmatavimai apskaičiuojami ir sukuriamas šablonas. Dauguma rankų „skaitytojų“ turi prispausti ranką. Toks prispaudimas padeda laikyti ranką vienoje padėtyje, kas leidžia daryti šablono pakartojamumą. Taigi yra žemas neteisingos padėties rodiklis ir žema sutapimo rodiklio klaida.

Rankos geometrija subrendusi technologija, dažniausiai, naudojama kontrolės punktuose, kur didelis srautas žmonių. Nors žmonių rankos skiriasi, jos individualiai nesiskiria. Todėl rankos geometrija negali būti panaudojama „one-to-many“. Tokia technologija labai patikima, nes sukurti kitą identišką ranką beveik neįmanoma.

Daugumą žmonių įvardija šią technologiją kaip patogią naudojimuisi. Be to, tai ne mažiau higieniška negu durų rankenos palietimas.

Pirštų atspaudų identifikacija. Pirštų atspaudų technologija labai dažnai naudojama ir yra paplitusi biometrijoje. Pirštų atspaudų identifikacija priklauso nuo skirtingų rumbelių piršto galiukuose savybių. Yra du pirštų atspaudų tipai: valcuotas ir plokščias. Plokščias spausdinimas turi atspaudą tik centrinės piršto dalies, tuo tarpu valcuotas spausdinimas apima papildomai piršto rumbelius taip pat, kaip ir centrinę dalį tarp galiukų ir pirmo piršto sąnario.

Pirštų atspaudų vaizdas skanuojamas, padidinamas ir po to paverčiamas į šablonus. Šie šablonai išsaugomi duomenų bazėje būsimam palyginimui naudojant optinius, silicio ir ultragarso skanerius. Ultragarso principas tikslesnis, bet retai naudojamas. Dažniausiai naudojami optiniai skaneriai.

Tik nedidelis žmonių procentas negali būti užregistruotas, nes jų pirštų rumbeliai dėl amžiaus išdžiūvo, „susidėvėjo“, arba „susidėvėjo“ dėl chemikalų. Be to, yra žmonių, kurie nenori duoti savo pirštų atspaudų, kadangi priklauso tam tikrai kultūrai, pvz., teisėtvarkoje (pirštų atspaudų sulyginimas identifikavimui kriminalistikoje ir pasipriešinimas panaudoti biometriją). Kyla susirūpinimas, kad

vienam tikslui surinkti pirštų atspaudai gali būti panaudoti kitam tikslui. Žmonės kartais skundžiasi dėl to, kad liečiant skanerį, jiems kelia susirūpinimą tokios procedūros higieną. Be to, pirštų atspaudų biometrinės sistemos ne visur veikia: jos netinka, pvz., ligoninėje, kur dauguma darbuotojų dirba mūvėdami pirštines.

Veido bruožų identifikacija. Veido bruožų identifikavimui sukuriamas 3D veido modelis, kuriame išryškinami antakių, akių, nosies, lupų ir t.t. kontūrai, apskaičiuojami atstumai nuo jų. Šiame metode, priklausomai nuo panaudojimo tikslų (identifikacija, verifikacija, veido paieška minioje), sudaroma daugybė veido modelio variantų, įskaitant galvos pasukimą ir palinkimą, o taip pat ir veido mimikos pakeitimą.

Veido bruožų identifikacijos technologija paprastai turi žemą lygį registracijos tempo požiūriu. Aplinkos faktoriai taip pat turi didelę įtaką, nes pakitimai kameroje, veido padėtis, išraiška arba savybės gali trukdyti algoritmams, kuomet bandoma sutapatinti turimą veidą su šablonu. Šablono „amžius“ gali ateityje sumažinti sugebėjimą koreguoti palyginimą.

Apibrėžiant tai, kas buvo pasakyta, galima teigti, kad siekiant padidinti laisvę ir saugumą, naudinga naudoti kai kuriuos pagrindinius principus, įvertinant tam tikras biometrines technologijas. Toks principų įstatymas privalo apimti tokius punktus:

- Registracija biometriniuose sistemose bus vieša, o ne slapta. Prieš „registraciją“ biometrinėje sistemoje kiekvienas turi būti susipažinęs su registracijos principais. Tokiu būdu, tampama skeptiškais biometrinėms programoms, tokioms kaip viešasis veido atpažinimas, kurios leidžia užslaptinti užgrobtus biometrinius duomenis.
- Biometrinės sistemos labiau panaudojamos verifikacijoje, o ne identifikacijoje. Apskritai, jos labiau tinka „one-to-one“ metodui, kuris garantuoja, kad „aptariamas“ asmuo turi leidimą dalyvauti „aptariamojoje“ veikloje. Biometrija yra mažiau naudinga ir daugiau problemiška politikos kontekste, kai tokios technologijos panaudojamos „one-to-many“ metode tam, kad panaudotų asmens anonimiškumą be būdingo pateisinimo.
- Biometrinės sistemos turi būti suprojektuotos dirbti su vietine duomenų saugykla (pvz., kortelės atitikimo šablonu), o ne su centrine saugykla. Centrinė biometrinių duomenų saugykla kelia susirūpinimą dėl privatumo. Aišku, kad kai kurioms technologijoms ir programoms vietinė saugykla dėl masto nebus įmanoma, tačiau yra pageidautina.
- Turime suteikti pirmenybę biometrinėms sistemoms, kurios yra „parengtos“ ir reikalauja asmens sutikimo, o ne yra privalomos. Bet tai ne visada įmanoma, nes pvz., įvažiavimas į JAV reikalaus biometrinių duomenų. Ir tai vėl bus išimtis iš bendrų savanoriškumo taisyklių.
- Slaptumo ir saugumo pagrindui reikės suteikti pirmenybę biometrinėms sistemoms, kurios sumažina biometriją iki šablono, vietoj to, kad palaikytų saugyklos vaizdą. Visų pirma,

šablonus sunkiau padirbti. Vaizdus, vis dėl to šiek tiek lengviau užšifruoti. Bet kokiu atveju, pasirinkimas bus labai priklausomas nuo pritaikymo.

- Bet kuri biometrinė sistema turi turėti stiprų patikrinimo ir apsirikimo programas, užkertant kelią piktnaudžiavimui.
- Bet kuri biometrinė sistema turėtų būti tokia patikima kaip ir inicialų registracijos sistema. Idealus būdas išvengti biometrinio suradimo – klaidingai įsiregistruoti kaip teisėtam naudotojui. Tokiu būdu, kartu su bet kurios biometrinės sistemos diegimu, reikia pasirūpinti registracijos procesų kontrole, tikrinti ir periodiškai testuoti sistemas. Registracijos duomenys taip pat turi būti tikrinami papildomai, siekiant identifikuoti klaidingai per pirmą bandymą užsiregistravusius asmenis.
- Biometrinė sistema turi būti tokia stipri kaip ir jos dubliavimo alternatyva. Sluoksniuoto saugumo principas reikalauja, kad tie, kurie įgyvendina biometrinio identifikavimo sistemas, turėtų tinkamą antrinę identifikavimo sistemą, kai pirminė identifikavimo sistema suges arba pateiks iškreiptą rezultatą.

Taigi apibendrinant galima teigti, jog biometrinės technologijos gali ir turi būti suprojektuotos su atitinkamais protokolais, užtikrinant privatumą jų įgyvendinimo atžvilgiu. Šie protokolai gali būti techninės įrangos dalimi ir gerinami per operatyvines gaires.

Biometrijos kaip identifikavimo priemonės panaudojimas sienos saugumui užtikrinti yra labai patrauklus, nes su jos pagalba galima atpažinti kertančius sieną asmenis, remiantis fiziologinėmis charakteristikomis arba elgesio ypatybėmis. Skirtingai nuo kitų identifikavimo priemonių, pvz., asmens liudijimų arba identifikavimo kodų, biometrinius duomenis sunku prarasti, pavogti arba spėti.

Dabartiniu metu biometriniai duomenys naudojami prieigos ir atpažinimo kontrolėje baudžiamosiose bylose. Išnagrinėta daug pažangių ir vis tobulėjančių biometrinių technologijų, kurios ateityje gali būti panaudojamos nacionalinėje sienos apsaugoje (2 lentelė) . Tarp septynių pagrindinių biometrinių technologijų yra veido bruožų, pirštų atspaudų, delno geometrijos, akies rainelės, tinklainės, parašo ir balso identifikacija. Tinkamiausios sienos saugume yra veido bruožų, pirštų atspaudų, akies rainelės ir tinklainės identifikacijos, nes visą tai jau anksčiau buvo naudojama pasienio kontrolės eksperimentuose ir taikomuosiuose tyrimuose. Tuo tarpu delno geometrija negali būti naudojama pasienio kontrolėje, nes yra nepakankamai patikima. Bet delno geometrijos panaudojimas kaip identifikavimo priemonės yra galimas ir naudojamas identifikacijos patikrinimui registracijos metu[35].

[35] Определение уровня неопределенности при осуществлении проектов в области электронного правительства. Национальный доклад ВОФК США.http://www.ach.gov.ru/in/material/m04-06.pdf

Taip pat buvo išnagrinėtos ir naujausios biometrinės technologijos, tokios kaip identifikavimas pagal ausies formą ir kvapą, bet jos dar tik nagrinėjamos ir kol kas nenaudojamos taikomosiose pasienio kontrolės programose.

2 lentelė. Biometrinių duomenų panaudojimas sienos apsaugoje

Technologija	Darbo metodai	Panaudojimas pasienio kontrolėje
Veido bruožų identifikacija	Fiksuoja ir palygina veido struktūrines savybes	Taip
Pirštų atspaudų identifikacija	Fiksuoja ir palygina pirštų antspaudų struktūrines savybes	Taip
Delno geometrija	Nustato ir palygina pirštų ir rankų dydį	Taip (tik patvirtinimui)
Akies rainelės identifikacija	Fiksuoja ir palygina akies rainelės struktūrines savybes	Taip
Tinklainės identifikacija	Fiksuoja ir palygina tinklainės struktūrines savybes	Ne
Parašo identifikacija	Fiksuoja ir palygina parašo ritmo, pagreitinimo ir slėginio judesio struktūrines savybes	Ne
Balso identifikacija	Fiksuoja ir palygina moduliacijos, kalbos tono ir aukščio struktūrines savybes	Ne

Šaltinis: adaptuota pagal „Определение уровня неопределенности при осуществлении проектов в области электронного правительства. Национальный доклад ВОФК США“ http://www.ach.gov.ru/in/material/m04-06.pdf

2.3. E. sienos integruoto valdymo praktinė realizacija, diegimas

Šioje darbo dalyje, bandant apibrėžti e. sienos valdymo praktinę realizaciją, bus orientuojamasi į Šengeno informacinę sistemą (SIS) Lietuvoje, darant prielaidą, jog tokia esminė priemonė visokeriopai praverčia kasdienėje policijos veikloje ir lengvina pasienio kontrolės darbą.

Visų pirma, dera akcentuoti, jog SIS – tai bendra informacijos technologijų ir ryšių sistema, skirta keistis informacija apie ieškomus asmenis ir daiktus. SIS sistemos tikslas – greitai ir veiksmingai tikrinti asmenis, siekiant aptikti nusikaltėlių ir nelegalių imigrantų judėjimą į/iš Šengeno valstybės į kitą.

Šios darbo dalies tikslas – parodyti, kaip veikia SIS ir jos įgyvendinimo kontrolės mechanizmai. Nepaisant to, jog SIS tampa svarbia priemone atliekant kasdienį policijos ir pasienio kontrolės darbą, tačiau vis dar kyla nemažai klausimų, kurie turi būti sprendžiami. Šios problemos yra išsamiai aptartos, SIS veiksmingumo įvertinimas, kaip vidaus ir išorės kontrolės ir apsaugos priemonė.

Analizuojant pirminę informaciją, dera pastebėti, jog Lietuva prie Šengeno informacinės sistemos ir teisėsaugos institucijos, turinčios teisę vykdyti duomenų paiešką ir įvesti duomenis į

Šengeno informacinę sistemą, prisijungė 2007 m. rugsėjo 1 dieną ir sėkmingai atlieka šį darbą[36]. Tokiu būdu Lietuvos pasienyje atvykstančių asmenų duomenys tikrinami ne tik nacionaliniuose registruose, bet ir Šengeno informacinėje sistemoje.

Verta detaliau panagrinėti ir pačią Šengeno informacinę sistemą, akcentuojant pagrindines šios sistemos sudedamąsias dalis, įdiegimo procedūrą ir duomenų modeliavimą.

SIS sudaro du pagrindiniai komponentai:

- nacionalinė sistema, vadinama nacionaline SIS (N.SIS) (yra kiekvienos Šengeno Susitariančiųjų Šalių teritorijose). N.SIS leidžia paskirtą nacionalinės valdžios instituciją atlikti paieškas SIS.

- centrinė techninio palaikymo sistema, vadinama centrine SIS (C.SIS) (įsikūrusi Strasbūre, Prancūzija). C.SIS užtikrina, kad duomenų bylos iš nacionalinių skyrių būtų atnaujinamos ir saugomos identiškai, ir bet kuriuo metu informacija būtų perduodama per tinklą.

SIS yra svarbiausia technologinė kompensacinė priemonė panaikinus vidaus sienas Šengeno erdvėje. Tai yra vienas iš pagrindinių reikalavimų, įgyvendinant Šengeno konvenciją Vidaus reikalų ministerija taipogi laikosi nuomonės, kad SIS atlieka svarbų vaidmenį nusikaltimų prevencijoje ir pasienio kontrolėje. Vadinasi, ši sistema tampa labai svarbiu įrankiu kasdieniniame pasienio kontrolės punktų darbe. Be abejo, SIS dalyvaujančios šalys įgyvendinti įvairius techninių duomenų modeliavimo sprendimus.

Remiantis Lietuvos Respublikos Vidaus reikalų ministro 2007 m. rugsėjo 17 d. įsakymu „Dėl Lietuvos nacionalinės Šengeno informacijos sistemos nuostatų patvirtinimo“, akcentuojama, jog Nacionalinės Šengeno informacijos sistemos (toliau – N.SIS) funkcijos yra:

1) įgyvendinti duomenų mainus tarp Centrinės Šengeno informacinės sistemos (toliau – C.SIS) bei Lietuvos Respublikos valstybės ir žinybinių registrų, nurodytų Nuostatų 12 ir 23 punktuose;
2) kaupti, saugoti ir teikti C.SIS duomenis, esančius nacionalinėje C.SIS duomenų bazės kopijoje, sudaryti sąlygas N.SIS duomenų gavėjams, naudotis C.SIS duomenimis ir vykdyti jų paiešką N.SIS;
3) užtikrinti C.SIS duomenų bazės kopijos reguliarų atnaujinimą ir saugą.

Žemiau yra pateikiama lentelė (3 lentelė) atspindinti nacionalinių registrų ES šalyse narėse sandarą. Registrai yra saugomi nacionaliniuose tinkluose su tikslu apsaugoti duomenis nuo išorinės prieigos. Vienas iš SIS II sistemos tikslų yra užtikrinti tarptautinių mastu registruose saugomos informacijos cirkuliavimą bei spartų registrų duomenų atnaujinimą.

---

[36] Per mažiau nei mėnesį Lietuvos teisėsaugininkai rado 16 ieškomų asmenų. 2 iš jų aptikti Italijoje, 4 – Švedijoje, 2 – Ispanijoje, 1 – Vokietijoje, 5 – Prancūzijoje, 1 – Latvijoje ir 1 – Suomijoje. Šaltinis: Lietuvos vidaus reikalų ministerija. Prieiga per internetą: http://www.vrm.lt/index.php?id=131&backPID=133&begin_at=30&pS=1191186000&pL=2681999&arc=1&tt_news=1356&

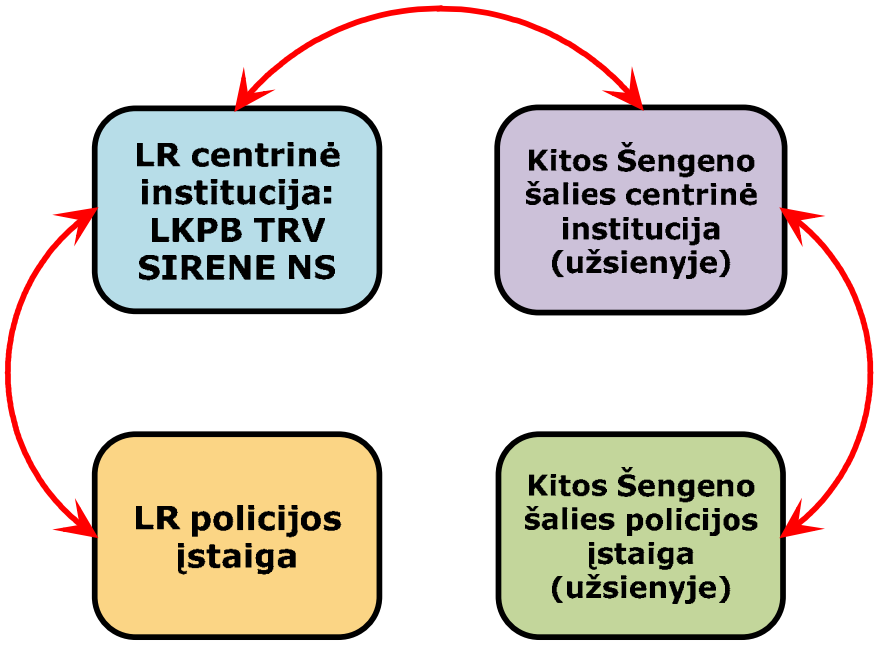
3 lentelė. Informacinės sistemos

1. Nusikalstamų veikų žinybinis registras,
2. Įtariamų, kaltinamų ir teistų asmenų žinybinis registras,
3. Arešto ar terminuoto laisvės atėmimo bausmę atlikusių asmenų atpažinimo žymių žinybinis registras,
4. Ieškomų asmenų žinybinis registras,
5. Civilinėje apyvartoje esančių ginklų žinybinis registras,
6. Ieškomų ginklų žinybinis registras,
7. Valstybinis ginklų registras,
8. Ieškomų transporto priemonių žinybinis registras,
9. Ieškomų numeruotų daiktų žinybinis registras,
10. Policijos registruojamų įvykių žinybinis registras,
11. Policijos registruojamų administracinių teisės pažeidimų žinybinis registras,
12. Gyventojų registras,
13. Muitinės informacinė sistema,
14. Valstybės sienos apsaugos tarnybos prie Vidaus reikalų ministerijos informacinė sistema (VSATIS), nepageidaujamų asmenų sąrašas,
15. Užsieniečių registras, kurio sudėtinė dalis bus Vizų registras.[37]

Sudaryta autorės

Šengeno informacinėje sistemoje veikia informacijos perdavimo, kaupimo, valdymo ir kontrolės mechanizmai. Centrinė Šengeno informacinė sistema užtikrina duomenų tikrumą. Kiekviena nacionalinė SIS perduoda savo užklausimus į Centrinę SIS, kur duomenys būna apdorojami. Vėliau juos įvertina, patikslina ir perduoda tiesiogiai visoms nacionalinėms sistemoms. Nacionalinės sistemos negali keistis duomenimis tiesiogiai tarpusavyje. Tokios procedūros dėka visos nacionalinės sistemos yra tarpusavyje suderintos ir disponuoja vienodo lygio informacija (6 pav.)

[37] Lietuvos Respublikos Vyriausybės 2006 m. birželio 8 d. nutarimas Nr.559 „Dėl Lietuvos Respublikos Vyriausybės 2002 m. liepos 19 d. nutarimo Nr. 1194 "Dėl nacionalinio šengeno acquis priėmimo veiksmų plano pakeitimo" // www.lrvk.lt/teises_aktai/files/2006/06/6666.doc



6 pav. Apsikeitimas informacija: prašymo ir atsakymo pateikimo tvarka Lietuvoje

Šaltinis: Sudaryta autorės, remiantis Europos Sąjungos taryba. Kitos policijos bendradarbiavimo priemonės. Lankstinukas. Prieiga per internetą: http://www.consilium.europa.eu/cms3_fo/showPage.asp?id=1189&lang=lt

Šengeno informacinėje sistemoje yra kaupiami šie duomenys:

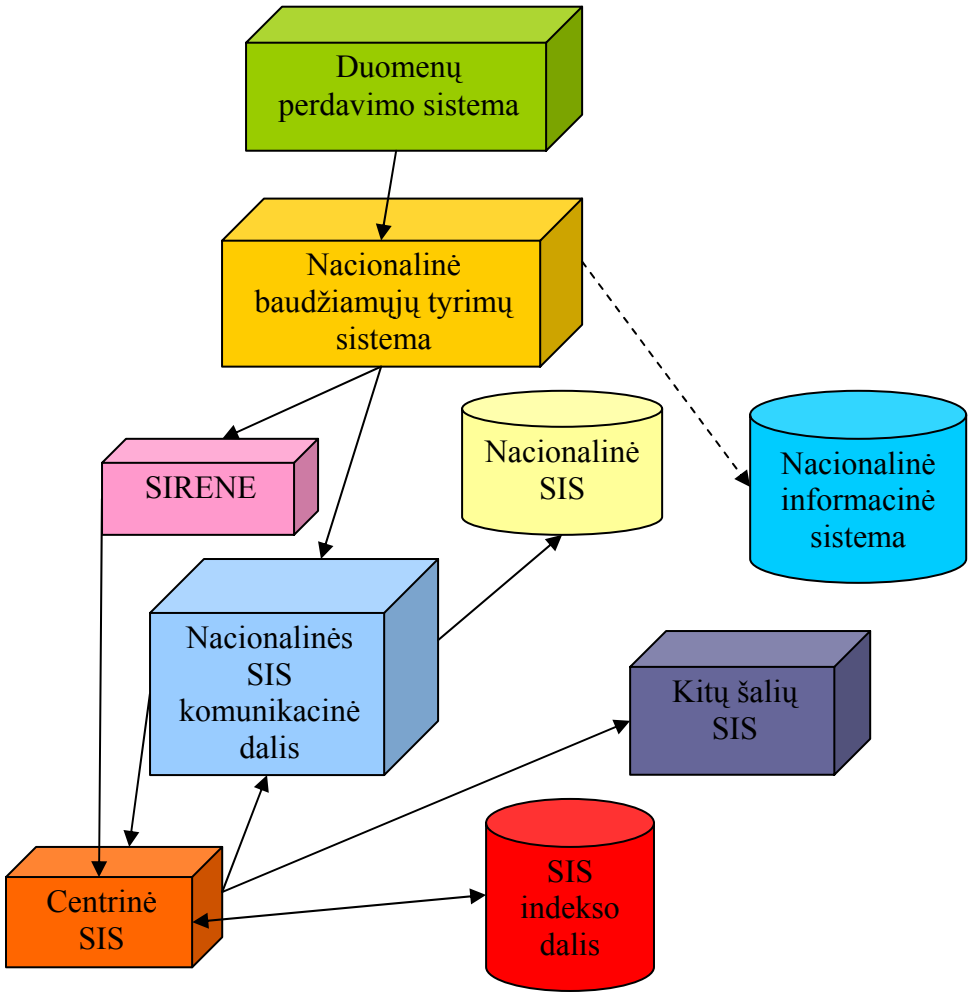
1. Duomenys apie asmenis, dėl kurių yra duotas perspėjimas,
2. Duomenys apie asmenis arba transporto priemones įvedami tam, kad jie būtų atsargiai sekami arba kad būtų atlikti konkretūs tikrinimai. Toks perspėjimas gali būti duodamas siekiant persekioti už nusikalstamas veikas arba neleisti kilti grėsmei visuomenės saugumui, jeigu: yra aiškių įrodymų, kad atitinkami asmenys ketina padaryti arba daro daugelį itin sunkių nusikaltimų; arba jeigu bendras atitinkamo asmens įvertinimas, ypač atsižvelgiant į anksčiau jo padarytas nusikalstamas veikas, leidžia manyti, kad tas asmuo ir ateityje darys itin sunkius nusikaltimus.
3. Duomenys apie asmenis, ieškomus suimti ir išduoti, įvedami prašymą pateikiančios Susitariančiosios Šalies teismo institucijos prašymu.
4. Duomenys apie užsieniečius, kuriems pagal duotą perspėjimą draudžiama įvažiuoti, įvedami remiantis nacionaliniu perspėjimu, kuris grindžiamas kompetentingų administracijos institucijų arba teismų sprendimais pagal nacionalinės proceso teisės normas.
5. Duomenys apie dingusius asmenis arba asmenis, kuriuos dėl jų pačių apsaugos arba siekiant užkirsti kelią grėsmei reikia laikinai perduoti policijai globoti, perspėjimą duodančios Šalies kompetentingos valdžios institucijos ar kompetentingos teismo institucijos prašymu yra įvedami tam, kad policijos įstaigos galėtų pranešti apie tų asmenų buvimo vietą perspėjimą davusiai Šaliai arba galėtų perkelti juos į saugią vietą, siekdamos nutraukti jų kelionę, jei nacionaliniai

teisės aktai leidžia tai daryti. Tai pirmiausia taikytina nepilnamečiams ir asmenims, kurie kompetentingos institucijos sprendimu turi būti internuoti. Duomenys apie dingusį pilnametį asmenį perduodami tik gavus to asmens sutikimą.

6. Duomenys apie liudytojus, asmenis, teisminių institucijų šaukiamus dėl baudžiamųjų bylų atvykti, kad duotų paaiškinimus dėl veikų, už kurias jie yra persekiojami, arba asmenis, kuriems turi būti įteiktas baudžiamasis teismo nuosprendis ar šaukimas atvykti, kad atliktų laisvės atėmimo bausmę, įvedami kompetentingų teisminių institucijų prašymu, kad būtų pranešta apie jų nuolatinę ar laikiną gyvenamąją vietą.
7. Į Šengeno informacinę sistemą įvedami duomenys apie ieškomus daiktus, kad jie būtų konfiskuoti arba panaudoti kaip įrodymai baudžiamojoje byloje. Tokiais daiktais yra laikomos pavogtos, dingusios arba pasisavintos autotransporto priemonės, priekabos, šaunamieji ginklai, oficialių dokumentų blankai, asmens tapatybės dokumentai, banknotai.

Šengeno informacinė sistema yra sukurta pagal 1990 m. Šengeno konvencijos IV dalies nuostatas. Kurioje numatyta, jog konvenciją pasirašiusios šalys sukuria ir išlaiko bendrą informacinę sistemą, toliau vadinamą Šengeno informacine sistema (SIS), kurią sudaro kiekvienos susitariančiosios šalies nacionalinė sekcija ir techninio aptarnavimo tarnyba. Šengeno informacinė sistema leidžia susitariančiųjų šalių paskirtoms institucijoms, naudojantis automatine paieška, prieiti prie perspėjimų dėl asmenų ir daiktų vykdant pasienio kontrolę bei atliekant kitus policijos ir muitinės tikrinimus šalyje pagal nacionalinius teisės aktus. Užsieniečiai, kuriems yra duoti perspėjimai draudžiantis įvažiuoti į Europos Sąjungą yra tikrinami išduodant vizas, suteikiant leidimus gyventi.

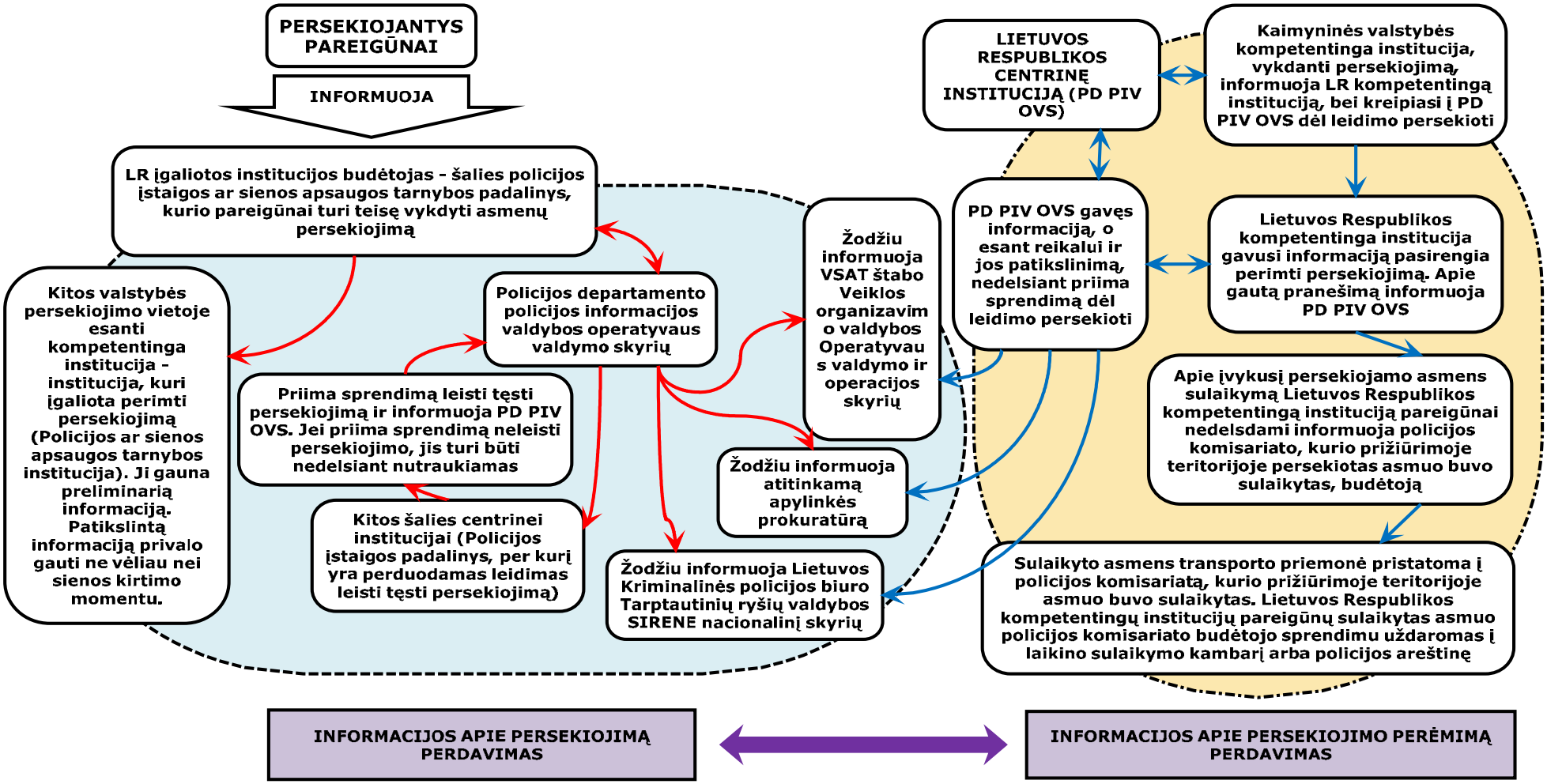
Šiuo metu yra ar kuriamos šios informacinės sistemos, kuriose tvarkomi duomenys, reikalingi nacionalinėms SIS bei SIS II dalims (7 pav.):



7 pav. Lietuva: techniniai aspektai, nacionalinės SIRENE ir SIS veikimas

Šaltinis: Sudaryta autorės, remiantis straipsniu „The Schengen Information System in Austria: An Essential Tool in Day to Day Police and Border Control Work?". Prieiga per internetą: http://www.libertysecurity.org/article165.html

Remiantis 3, 6 bei 7 paveikslais yra atvaizduojami informacijos apie paieškomus asmenis perėmimo bei perdavimo SIS II procesai (duomenis yra saugomi informacijos sistemų registruose 3 lentelė)



8 pav. Informacijos apie persekiojimą ir persekiojimo perėmimą perdavimas

Sudaryta autorės

3. BIOMETRINIO SAUGUMO E-VALDŽIOS ĮGYVENDINIMO ŠENGENO ERDVĖJE PROBLEMOS DIEGIANT E.VALDŽIOS E.SIENOS PASLAUGĄ LIETUVOJE

3.1. Elektroninės valdžios e. paslaugų administravimo aspektai informacinės visuomenės kontekste

Valstybinių institucijų informacinių sistemų (e.paslaugų) valdymas turi būti nagrinėjamas elektroninės valdžios kontekste. Tokiu būdu neišvengiama ir platesnio konteksto, nes nagrinėjamas ir ankstesnių valstybinių procesų įgyvendinimas, ir informacinių sistemų valdymo poreikis bei poveikis tokios sistemos eksploatavimui ir informacinės visuomenės plėtrai.

Labiausiai derėtų orientuotis į Lietuvos Respublikos vidaus reikalų ministeriją, kurios pagrindinis uždavinys ir funkcijos elektroninių viešųjų paslaugų teikimo srityje – vykdyti e.valdžios koncepcijos numatytą elektroninės valdžios projektų valdymo funkciją. Taip pat svarbus Informacinės visuomenės plėtros komitetas prie Lietuvos Respublikos Vyriausybės (toliau – IVPK). Tai institucija, tiesiogiai atsakinga už elektroninės valdžios projektų įgyvendinimo koordinavimą ir stebėseną. Neapsieisime nepaminėję ir Valstybinės duomenų apsaugos inspekcijos (toliau -VDAI), kuri vykdo Lietuvos Respublikos įstatymais ir teisės aktais jai pavestas duomenų apsaugos priežiūros funkcijas. Tačiau visų pirma dera įsigilinti į e. valdžios teikiamų e. paslaugų reikalingumą ir priimtinumą piliečiams visos Europos Sąjungos kontekste.

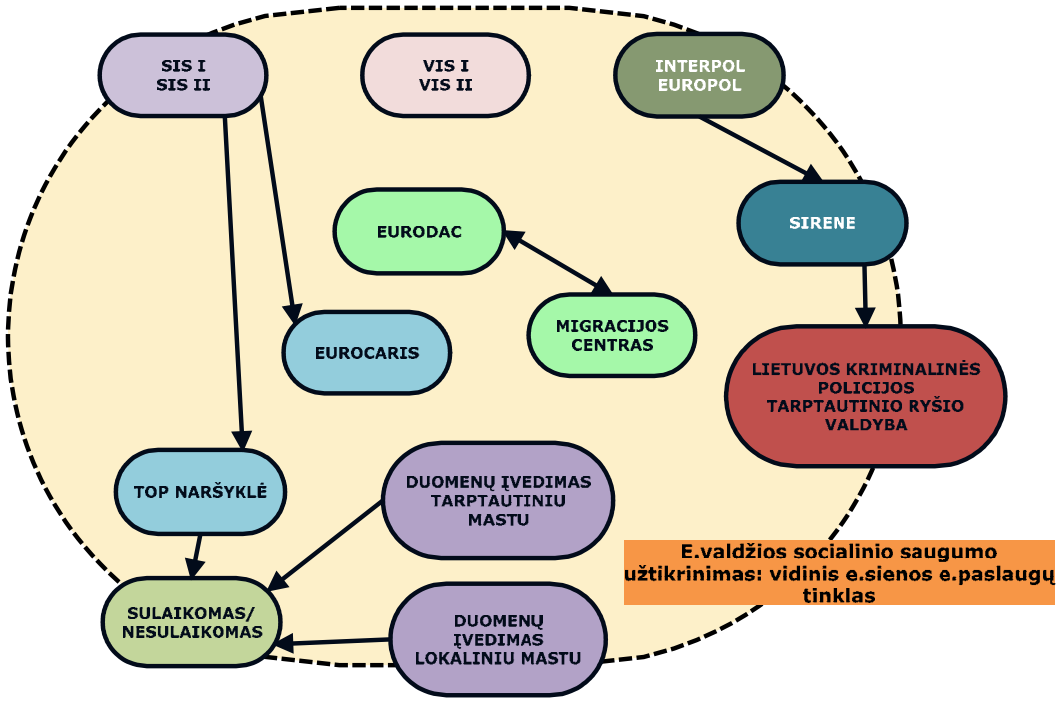
Apgalvojus prieštaringas vizijas ir interesus, supančius Europos vienijimosi procesą, ir atsižvelgus į daugumos šalių piliečių entuziazmo stoką, neįmanoma patikėti, kad integracijos procesas tūkstantmečio pabaigoje yra taip pažengęs į priekį. Šią neįtikėtiną sėkmę iš dalies lėmė tai, kad Europos Sąjunga neišstumia nacionalinių valstybių, o priešingai - tampa pagrindiniu jų išsaugojimo įrankiu, su sąlyga, kad šios atsisakys dalies suvereniteto mainais už didesnę įtaką pasaulio ir vidaus reikaluose globalizacijos amžiuje. Bet tam, kad ši interesų konvergencija taptų veiksni, jai buvo reikalinga institucinė terpė (kuria iš esmės galėtų tapti e.valdžia, teikianti e. paslaugas).

Nesibaigiančios derybos dėl šių institucijų veiklos tarp valstybinio lygmens veikėjų, siekiančių įgyvendinti savas strategijas šių institucijų rėmuose, gali atrodyti sunkios ir neefektyvios. Tačiau būtent šis neapibrėžtumas bei sudėtingumas leidžia Europos Sąjungoje derinti ne tik skirtingų šalių, bet ir skirtingų politinių orientacijų partijų, išrinktų į vyriausybę, įvairius interesus ir besikeičiančias politines platformas. Viena vertus, reikia leisti šalims įgyvendinti savo strateginius e.valdžios sprendimus taip, kad jų negalėtų paralyžiuoti koks nors nepalankus faktorius ar pašalinių įsikišimas.

Tarkime, gynybos, policijos ir valstybės išlaidų reikaluose pirmenybė galėtų būti teikiama konfederacinei ar tarpvyriausybinei [logikai], o pinigų politikos, prekybos, rezidencijos bei kapitalo, prekių ir žmonių judėjimo srityse Sąjunga turėtų funkcionuoti daugiau pagal federalizmo ar viršnacionalinius reikalavimus. Kiti klausimai, pavyzdžiui, užsienio politikos, aplinkosaugos, mokesčių ir imigracijos, turėtų užimti tarpinę poziciją. Būsimojoje, išsiplėtusioje Europos Sąjungoje turėtų būti mažiau vienodumo ir daugiau lankstumo Tokios institucijos, galimas daiktas, labiau panašės į tinklą nei į medį, o politinė teorija dar neturi specialaus termino tokio tipo konfigūracijai pavadinti. Tačiau tai netrukdo tokią sukurti. Vis dėlto nepakanka, kad apsišvietę biurokratai sumanytų tokią e.valdžios instituciją: ją būtinai turi pripažinti ir piliečiai.

Kad pamažu įtvirtintų e.valdžios teisėtumas ir nesusilpnėtų jos gebėjimas formuoti tam tikrą požiūrį į politiką ir jos vykdymą, visos institucijos būtinai turi palaikyti glaudžius ryšius su regionų ir vietinio lygmens valdžia, apgalvotai plėtodamos vientisumo principą, pagal kurį bus ne tik informuojama visuomenė, bet ir teikiamos kokybiškos paslaugos.

Realus Europos relegitimizacijos procesas reiškiasi vietos ir regionų iniciatyvų gausėjimu kuriant e. valdžią, ekonomikos plėtra, taip pat kultūrine raiška bei socialinėmis teisėmis, kurios horizontaliai susisieja viena su kita, taip pat su Europos programomis -tiesiogiai arba per savo nacionalines vyriausybes. Atsižvelgiant į antroje darbo dalyje pateikiamus techninius bei grafinius sprendimus dėl e. sienos integruoto valdymo praktinės realizacijos žemiau darbe yra atvaizduojamas SIS e. valdžios e. paslaugų realizacijos procesas vidiniame e. sienos tinkle akcentuojant specifinius Lietuvos VSAT sistemos ypatumus.



9 pav. ES narių e. paslaugų realizacija e. valdžios sektoriuje

Sudaryta autorės

Svarstydami apie sudėtingėjantį ir lanksčią Europos politinį procesą, kuris šiuo metu gana aktyviai reiškiasi e. valdžios perspektyvoje, įdomi Keo-hane'o ir Hoffmano mintis, kad Europos Sąjunga „iš esmės yra sudaryta kaip tinklas, kuriame suverenitetas yra dalijamas bendrai, o ne deleguojamas aukštesnėms instancijoms“.[27] Ši analizė, kurią teoriškai išplėtojo Waeveris, Europos vienijimąsi leidžia apibūdinti maždaug kaip institucinį naująjį viduramžiškumą - tai yra kaip daugybę vienas kitą papildančių valdžios institucijų, kaip prieš daugelį metų jį apibūdino Hedley'us Bullis, o vėliau atkartojo nemažai Europos tyrėjų.

Nors istorikai gali nesutikti su tokiu sugretinimu, tačiau šis pavyzdys vaizdingai iliustruoja naują valstybės formą, kurią įkūnija Europos institucijos: *tinklo valstybę. Šios valstybės skiriamasis bruožas yra dalijimasis įgaliojimais visame tinkle.* Tinklas pagal apibrėžimą turi mazgus, bet neturi centro. Mazgai gali būti skirtingų dydžių ir susiję asimetriškais ryšiais tinkle - taip, kad tinklo valstybė nesutrukdytų tarpti nelygybei tarp jos narių. Iš tikrųjų Europos tinkle ne visos vyriausybinės institucijos yra lygios. Negana to, kad nacionalinės vyriausybės tebėra sutelkusios didelę dalį sprendimų priėmimo galios į savo rankas, tačiau taip nacionalinių valstybių taip pat esama svarbių galios skirtumų, nors galios hierarchija įvairuoja, nelygu sritis: Vokietija vyrauja kaip ekonomikos supervalstybė, o Britanija ir Prancūzija disponuoja žymiai didesne karine galia ir bent jau ne menkesniais technologiniais pajėgumais. Vis dėlto, nepaisant šios asimetrijos, įvairūs Europos tinklaveikos valstybės mazgai yra priklausomi vieni nuo kitų, todėl nė vienas mazgas, net ir pats stipriausias, sprendimų priėmimo procese negali nepaisyti kitų, net ir pačių mažiausių. Jei kurie nors politiniai mazgai pabandytų taip elgtis, susvyruotų visa sistema. Tuo ir skiriasi politinis tinklas nuo centralizuotos politinės struktūros.

Turimi faktai ir pastarojo meto ginčai politinės teorijos srityje rodo, kad tinklaveikos valstybė, disponuojanti geometriškai įvairuojančiu suverenitetu, yra politinių sistemų atsakas į globalizacijos iššūkius (kaip vienas šių iššūkių yra ir e. valdžios atėjimas į tinklą).

Tačiau galiausiai Europoje suvienyti e. valdžios koncepciją vien tik sumanios politinės inžinerijos nepakaks. Demokratinių visuomenių kontekste susivienyti - įvairiu mastu ir dar įvairiomis formomis - Europa galės tik tuomet, jei to norės jos piliečiai. Atsižvelgiant į trijuose šios knygos tomuose pristatytus socialinių procesų tyrimus, neatrodo, kad toks pritarimas galėtų įvykti vien tik instrumentinio intereso suvaldyti globalizaciją pagrindu, juolab kad toks suvaldymas tikrai neigiamai atsilieps platiesiems gyventojų sluoksniams. Jei prasmė yra susijusi su tapatumu ir jei tapatumas ir toliau bus vien tik tautinis, regioninis ar vietinis, Europos integracija gali neišsilaikyti kitokia, kaip tik bendrosios rinkos forma, analogiška laisvosios prekybos zonoms, įkurtoms kitose pasaulio dalyse. Europos susivienijimui e.valdžios perspektyvoje reikalingas tam tikras piliečių sąmoningumas.

Vis dėlto piliečių sąmoningumo ir bendro sutarimo e. valdžios klausimu samprata yra mažų mažiausiai problemiška. Jis turi būti kuriamas ant demokratijos pamato: pirma, todėl, kad demokratiniai idealai yra pripažįstami visame pasaulyje, o antra, todėl, kad pačią demokratiją šiuo metu yra apėmusi krizė dėl jos priklausomybės nuo nacionalinės valstybės, todėl yra pravartu turėti visiems prieinamą informacinį šaltinį. Informacinė visuomenė tampa vis margesnė. Beje, nebus lengva ginti e. valdžios būtinumą ir reikalingumą, nes dauguma žmonių dar nežino, ką reiškia e. valdžia ir kaip pasinaudoti jos teikiamomis e. paslaugomis? Visuomenėse neįvyks tokia greita ir plati transformacija. Tačiau ją galima sukurti - ne kaip prieštarą tautiniams, regioniniams bei vietiniams įsitikinimams, o kaip jų papildymą. Tam prireiks socialinio konstravimo proceso- tai yra kaip socialinių vertybių bei institucinių tikslų, kuriems galėtų pritarti dauguma piliečių ir kurie nė vieno iš esmės neišskirtų, modelis.

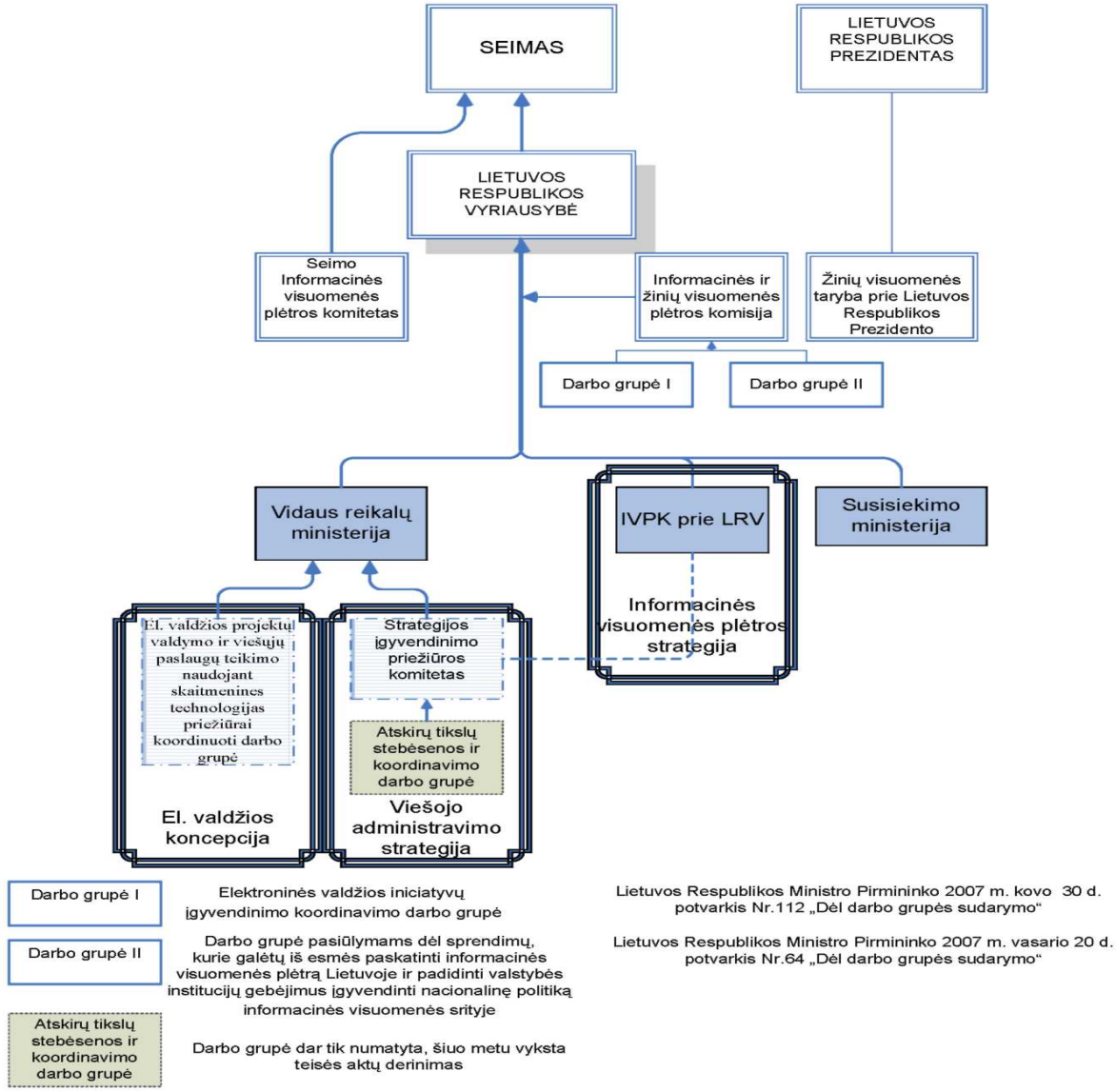
Kokie elementai iš tikrųjų figūruoja globalizacijai ir pilietinių teisių atėmimui oponuojančių, tačiau į bendruomeniškumą nenuslystančių socialinių veikėjų kalboje ir veikloje[2]: laisvė, lygybė, brolybė; gerovės valstybės, socialinio solidarumo, nuolatinio darbo ir darbuotojų teisių gynimas; rūpinimasis visuotinėmis žmogaus teisėmis ir sunkia Ketvirtojo pasaulio padėtimi; demokratijos gynimas ir jos plėtojimas taip, kad ji aprėptų piliečių dalyvavimą vietos ir regionų lygmenimis; istoriškai ir teritoriškai susiformavusių kultūrų gyvybingumas, neretai įgyjantis kalbinę išraiškos formą ir neleidžiantis joms pasiduoti virtualiajai kultūrai. Dauguma Europos piliečių turbūt pritartų šioms vertybėms. Kad būtų įgyvendintos, pavyzdžiui, gerovės valstybės ir nuolatinio darbo vertybės, ekonomikoje ir institucijose turėtų įvykti didžiulės permainos. Tačiau būtent taip ir yra kuriama e.valdžia: kovoje dėl alternatyvių ekonomikos plėtros, visuomeniškumo ir valdymo formų. Jei šios užuomazgos įgaus politinę išraišką, technologinis vystymosi procesas galbūt bus įgyvendintas platesniu mastu.

3.2. Biometrinio saugumo SIS e. valdžios koncepcijos įgyvendinimo Šengeno erdvėje problemos diegiant e. sienos paslaugą Lietuvoje

Kaip jau buvo minėta ankstesnėse darbo dalyse, Šengeno erdvė ir tarpvalstybinis bendradarbiavimas joje sudaro sąlygas panaikinti kontrolę prie valstybių vidaus sienų, taip sudarant galimybes laisvam asmenų judėjimui. Atsivėrus sienoms, pagrįstai kyla nelegalios migracijos klausimas, todėl buvo sukurtos kai kurios prevencinės priemonės, skirtos dalyvaujančioms valstybėms kovoti su neteisėta migracija.

Šios priemonės nutiesia visiškai naujus kelius tarpvalstybiniam teisėsaugos institucijų bendradarbiavimui: sėkmingai pasiekta poreikio skubiai reaguoti į nusikaltimą ir pagarbos nacionaliniam suverenitetui pusiausvyra[38].

Pagal Šengeno konvenciją nustatytos naujos priemonės, tokios kaip **Šengeno informacinė sistema (SIS)** ir **SIRENE** biurai, tapo tarptautinio bendradarbiavimo policijos, baudžiamojo teisingumo ir sienų kontrolės srityse gairėmis. Daugelis šalių pripažįsta jų naudingumą ir aktyviai taiko. Šios dvi paminėtos sistemos – tai pagrindinės priemonės kovojant su nusikalstamumu laisvo judėjimo erdvėje. Jų taikymas sudaro galimybes atlikti ieškomų ir (arba) dingusių asmenų ir objektų tarptautines paieškas. 10 paveiksle pateikiama Informacinių technologijų strategijų vykdomoji organizacinė schema Lietuvoje, kurioje pavaizduoti visos sistemos sudedamosios dalys ir atitinkami ryšiai tarp šių dalių.



10 pav. Informacinių technologijų strategijų vykdomoji organizacinė schema
Šaltinis: Valstybinio audito ataskaita. Valstybinių institucijų informacinių sistemų valdymas e.valdžios kontekste. 2007 rugsėjo 28d. Nr. IA-9000-4-3.

[38] Europos Sąjungos taryba. Šengeno bendradarbiavimas. Prieiga per internetą: http://www.consilium.europa.eu/cms3_fo/showPage.asp?id=1180&lang=lt

Kalbant plačiau, **Šengeno Informacijos Sistema** yra labai svarbi priemonė siekiant įgyvendinti laisvą judėjimą. Iš pradžių tik kelios šalys buvo įtrauktos į bendradarbiavimą, kurios buvo už ES ribų sistemos. Teigiama, kad yra įrodymas, jog laisvas judėjimas veikia, tačiau jis negalėjo veikti be saugumo priemonių, kurių buvo imtasi. SIS buvo labai svarbi priemonė palaikant valstybių narių vidaus saugumą ir kontroliuojant nelegalią imigraciją. Paieška SIS yra veiksminga ir lemia daug teigiamų veiksnių, kurie sustiprina saugumą ir kontroliuoja nusikalstamumą bei nelegalią migraciją į Šengeno erdvę.

Tačiau buvo atkreiptas dėmesys į kai kurias problemas, išsprendus kurias būtų galima pagerinti SIS darbą. Visų pirma, tik apie 10% visos sistemos galimybių yra išnaudojama. Nacionalinės Šengeno valdžios institucijos turi inicijuoti dialogą su teisminėmis institucijomis, stengtis padidinti jų ir sistemos sąveikos supratimą.

Kita problema, susijusi su Šengeno konvencija – labai griežtų duomenų, kuriuos reikia įvesti į SIS, reikalavimas. Buvo įrodyta, kad tai sumažina policijos gebėjimą susidoroti su nusikaltimais, kuriuos lengvai galima buvo išnagrinėti, jei būtų leidžiama operuoti vienokia ar kitokia informacija. Pavyzdžiui, informacijos apie pavogtų automobilių registravimo lenteles įvesti į sistemą negalima, nors informacija apie pavogtus automobilius yra leistina. Tokiu būdu, kuomet automobilio registracijos lentelė vagiama, ji naudojama vogtame automobilyje, su kuriuo vykdomi apiplėšimai ar kiti nusikaltimai. Jeigu būtų įmanoma registruoti lenteles, paprasčiau susekti vogtą automobilį taptų lengviau. Tam reikėtų išplėsti informacijos sąrašą, įvedamą į SIS, o tai gali būti vykdoma tik iš dalies pakeitę konvenciją. Duomenų apsauga Šengeno konvencijoje yra užtikrinama remiantis tam tikromis taisyklėmis ir kontrolės sistemomis. Nors taisyklės yra svarbios duomenų apsaugai ir asmens teisėms, tik praktiškai taikant šias taisykles gali būti vykdoma veiksminga apsauga. Taisyklių taikymo kontrolė yra tai, kas nustato bendrą veiksmingumą praktikoje. Siekiant nustatyti, kaip duomenų apsaugos taisyklės yra taikomos Lietuvoje, bus analizuojamos kontrolės sistemos, kurios yra naudojamos. Dėmesys bus sutelktas į vidaus ir išorės kontrolę.

Vidaus kontrolės nurodo į integruotą apsaugos sistemą, kuria siekiama užtikrinti kokybę ir duomenų saugumą, reikalaujamą pagal Šengeno konvencijos 118 straipsnį. Ji yra **techninės, personalo ir organizacinės kontrolės** derinys.

Techninė kontrolė būna įvairių formų, ir yra atliekama siekiant užtikrinti, kad ši sistema atitiktų duomenų apsaugos taisykles, susijusias su duomenų surinkimu, kokybe ir saugumu. Šengeno informacinė sistema yra atviro ciklo on-line sistema. Pagal Gregorius ir Horn (1963, p16), atviro ciklo on-line sistema panaikina žmogiškąjį faktorių renkant duomenis ar atliekant kontrolės instrukcijas, skirtingai nei „uždarojo ciklo“ sistema, kuri yra visiškai automatizuota visuose etapuose nuo duomenų apdorojimo iki kontrolės įgyvendinimo.

Žmonės vis dėlto lieka svarbia SIS vidaus kontrolės dalimi, visų pirma duomenų inicijavimui (rinkimas, pertvarkymas ir tikrinimas) bei įvedimui. *Organizacinė kontrolė* nurodo į valdymo struktūras ir pareigas tiek valdytojams, tiek ir darbuotojams. Dėl įtikimumo ir aiškumo, aptarsime vidaus kontrolę skirtingais duomenų apdorojimo etapais, pradedant nuo duomenų surinkimo, įrašymo duomenų ir priėjimo prie jų. Techninė kontrolė ir personalas, dalyvaujantis toje kontrolėje bus aptariamas atskirai kiekviename duomenų apdorojimo etape. Organizacinis valdymas, bus aptartas pasibaigus šiam skirsniui, nes jis tęsias visuose duomenų tvarkymo etapuose.

Duomenų genezė apibrėžia tris veiklos rūšis: rinkimą, pertvarkymą ir tikrinimą. Dažniausiai pirmo lygio kriminalistikos policijos pareigūnai renka duomenis įvedimui į SIS programą. Prieigos prie duomenų yra reikalaujama dėl įvairių priežasčių: paieškos, atnaujinimo, koregavimo, pašalinimo, ir atskiro prieigos prašymo (tai bus aptariama vėliau kaip dalis Europos Sąjungos išorės kontrolė). SIS tikslas yra pasiūlyti on-line paieškos galimybės prieigą, nusikaltimų ir imigracijos institucijoms. Taigi paieška yra labiausiai paplitusi prieigos prie SIS forma. Asmuo, kuris gauna prieigą prie duomenų, turi turėti teisėtas priežastis, tokias kaip vykdyti visuomeninę pareigą, kurios iš jo yra reikalaujama.

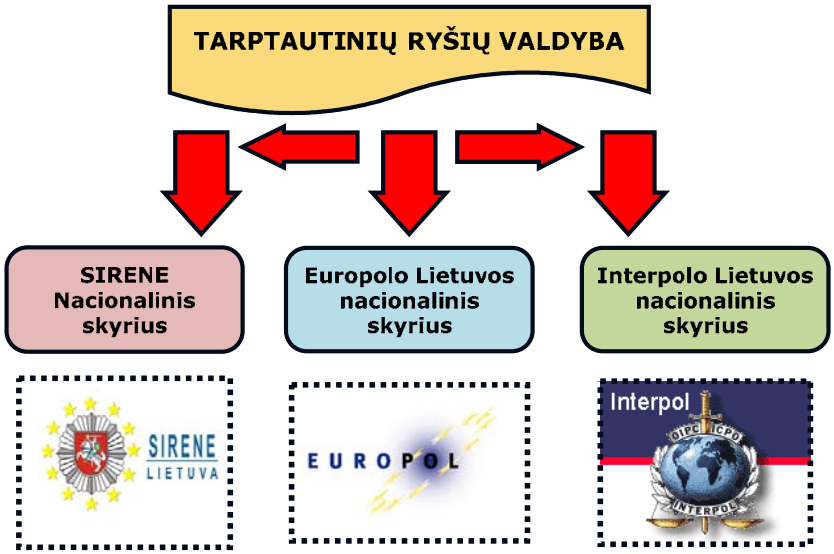
Atsižvelgiant į tai, daroma prielaida, kad paieška yra prieinama beveik visiems pareigūnams, atsakingiems už sienų, nusikalstamumo ir imigracijos kontrolę. Šis skaičius nėra ribojamas ir gali padidėti kai atsiranda poreikis. Tačiau dėl didelio skaičiaus žmonių, turinčių priėjimą, sudaroma galimybė informacijos nutekėjimui.

Kitas svarbus Šengeno aspektas – SIRENE biuras. Tai sudėtinė nacionalinės Šengeno informacinės sistemos dalis. Kiekviena Šengeno valstybė privalo įkurti SIRENE biurus. Lietuvoje SIRENE nacionalinis skyrius yra įsteigtas Lietuvos kriminalinės policijos biuro Tarptautinių ryšių valdyboje.

Remiantis Konvencijos nuostatomis, šis biuras veikia kaip atskiras padalinys. Jis kaupia bei analizuoja informaciją. Tuo tarpu su kitais informaciją kaupiančiais, apdorojančiais, bei analizuojančiais padaliniais, esančias valstybės viduje, biuras gali bendradarbiauti. Jis atsako į užklausimus, apsikeičia reikalinga informacija, be to tą informaciją apdoroja bei paskirsto.
SIRENE biuras veikia 24 valandas per parą, 7 dienas per savaitę.

SIRENE biurą sudaro du skyriai:

1) informacijos priėmimo ir paskirstymo skyrius,
2) analizavimo ir atsakymų į užklausas ruošimo skyrius.



11 pav. Lietuvos kriminalinės policijos biuro Tarptautinių ryšių valdybos schema

Sudaryta autorės, remiantis Europos Sąjungos taryba. Kitos policijos bendradarbiavimo priemonės. Lankstinukas. Prieiga per internetą: http://www.consilium.europa.eu/cms3_fo/showPage.asp?id=1189&lang=lt

Atsižvelgiant į paveiksle pateiktą tarptautinių ryšių valdybos schemą, dera detaliau išanalizuoti, kuo skiriasi SIRENE nuo Europolo ar Interpolo. SIRENE ir Europolas skiriasi tuo, jog „Europolo veikloje didžiausias dėmesys skiriamas tik sunkiam organizuotam nusikalstamumui, kuris susijęs su dviem ar daugiau ES valstybių narių. Europolui leidžiama keistis slapta kriminalinės žvalgybos informacija ir ją tirti. Europolas turi savo personalą, o valstybių narių ryšių palaikymo pareigūnai komandiruojami į Hagą, kur yra Europolo būstinė. Tai yra juridinį statusą turinti ES institucija“[39]. Tuo tarpu SIRENE biurus steigia valstybės narės, siekdamos vykdyti Šengeno bendradarbiavimą. Biurų veikla apima įvairių baudžiamumo klausimų nagrinėjimą, daugiausia dėmesio skiriant paieškoms naudojantis SIS, bendrą keitimąsi informacija ir paramą tarpvalstybinio pobūdžio operacijoms. Europolas turi prieigą prie kai kurių SIS esančių perspėjimų, kad gautų daugiau analitiniam darbui reikalingos informacijos.

Kitas klausimas – SIRENE ir Interpolo sąsaja. Interpolas yra pasaulinio lygio organizacija, kurios veikla grindžiama tarpvyriausybiniu susitarimu. Interpolas sudaro galimybes keistis informacija, tačiau bendradarbiavimas visiškai priklauso nuo valstybių narių. Jis taip pat turi duomenų apie ieškomus asmenis, transporto priemones ir kitą turtą, bazę, tačiau valstybės narės neprivalo teikti informacijos, o gatvėse patruliuojantys policijos pareigūnai daugelyje šalių neturi tiesioginės prieigos prie tos duomenų bazės[40]. SIRENE, dera akcentuoti, vykdo veiklą tik Šengeno teritorijoje, kur ši veikla pakeičia bendradarbiavimą per Interpolą. Kadangi Interpolo nacionalinių centrinių biurų ir SIRENE biurų veikla yra gana panaši, kai kurios valstybės narės juos sujungė į vieną.

[39] Europos Sąjungos taryba. Šengenas. Prieiga per internetą: http://www.consilium.europa.eu/cms3_fo/showPage.asp?id=1187&lang=lt
[40] Europos Sąjungos taryba. Šengenas. Prieiga per internetą: http://www.consilium.europa.eu/cms3_fo/showPage.asp?id=1187&lang=lt

Tokioje sistemoje kaip SIS, kur asmenims yra ribojama arba nesuteikiama jokia prieiga prie jų asmeninės informacijos, tik vidaus ir išorės kontrolės mechanizmai gali užtikrinti tinkamą individualią apsaugą. Imperatyvu tampa tai, kad tie, kurie atsako už sistemos funkcionavimą, turi užtikrinti ir tinkamus vidaus kontrolės mechanizmus. Kita vertus, kad būtų pagerinta bendra individualioji duomenų apsauga, veiksminga išorės kontrolė turėtų papildyti vidaus kontrolę. Tiek SIS vidaus kontrolės, tiek ir išorės kontrolės mechanizmai reikalauja gero suderinamumo, siekiant užtikrinti, kad nekalti asmenys netaptų aukomis tos sistema, kuri buvo numatyta juos apsaugoti.

Dėmesys turėtų būti sutelktas į duomenų surinkimą ir įrašymą, prieigos kontrolę, viešąjį visuomenės informavimą ir švietimą, tiek nacionaliniame, tiek ir bendros priežiūros kontekste. Reikalavimas turėti išsamų visų Šengeno sistemų duomenų įvertinimą gali būti perspektyvus sprendimas, pagerinantis individualią apsaugą.

Organizacinė kontrolė. Organizacinė sistemos kontrolė apima personalą ir procedūras. Kaip buvo pažymėta anksčiau, SIS yra atvira sistema, naudojanti žmones jos kontrolės funkcijoms atlikti. Todėl personalas yra labai svarbi sudedamoji vidaus kontrolės sistemos dalis. Kaip jau buvo aptarta anksčiau, pirmojo lygio pareigūnai yra atsakingi už duomenų rinkimą, o antrojo lygio pareigūnų pareiga – patikrinti ir įvesti duomenis juos į SIS. Be to, Vidaus reikalų ministerija paskiria asmenį, atsakingą už duomenų apsaugą ir saugumą nacionalinėje sistemoje. Šis asmuo taip pat atsako už duomenų apsaugą ir saugumą SIS. Be to, atsakomybė už duomenų apsaugą policijos sistemose yra decentralizuota kiekvienai policijos apygardai, kurių kiekviena turėtų turėti po asmenį, atsakingą už duomenų apsaugą ir saugumą. Ministerija taip pat skiria asmenį, atsakingą už saugumo ir duomenų apsaugą SIRENE sistemose. Šis asmuo atsiskaito už bendrą duomenų apsaugą Vidaus reikalų ministerijos pareigūnui.

Individuali kontrolė: subjekto teisė susipažinti su duomenimis. Pagal Šengeno konvenciją, kur duomenų registracijos yra reikalaujama pagal įstatymus, ir asmuo neturi sutikimo teisės (kad duomenys būtų registruojami be fizinio asmens žinios), individualios kontrolės veiksmas priklauso nuo prieigos prie duomenų teisės. Teoriškai, asmuo turi galią kontroliuoti teisę į prieigą (109 straipsnis), teises į duomenų pataisymą ar panaikinimą (110 straipsnis), ir prašymą patikrinti duomenis per nacionalines duomenų apsaugos institucijas (114 straipsnis). Akivaizdu, kad viena svarbiausių teisių yra teisė į prieigą. Nesant šios teisės, naudojimasis kitomis teisėmis gali neturėti pakankamo pagrindo. Deja, prieigos teisė pagal Šengeno konvenciją yra griežtai apribotas. Tokiais atvejais, asmuo negali vykdyti jokios kontrolės.

Akcentuojant teisminę kontrolę, reikia pabrėžti, jog teisminė kontrolė, ypač tarptautinė ar bendros prieigos, niekada nebuvo stiprioji Šengeno bendradarbiavimo vieta. Šengeno konvencija visiškai apeina bendros teisminės kontrolės idėją. Tačiau Šengeno įtraukimas į ES teisinę struktūrą pripažino ribotą Europos Bendrijų Teisingumo Teismo jurisdikciją. Tai gali išgelbėti situaciją. Nepaisant bendros teisminės kontrolės trūkumų, Susitariančių Šalių nacionaliniai teisminiai aparatai

ir toliau lieka perspektyviausi teisminės kontrolės organai Šengeno erdvės klausimais. Pavyzdžiui, Prancūzijoje, Vokietijoje, Beneliukso šalyse, kur SIS buvo tam tikrą laiko tarpą eksploatuojama, nemažai bylų nukeliavo iki teismų.

Nors Šengeno sistemai trūksta bendros teisminės kontrolės išplečiant nacionalinę teisminę kontrolę, Europos Žmogaus Teisių Teismas (EŽTT) yra ta institucija, kuri kontroliuoja kreipimusis, kilusius iš Šengeno Susitariančiųjų Šalių.

Taigi teisminė kontrolė yra svarbi, o ypač sprendžiant platesnius klausimus dėl žmogaus teisių ir aiškinant Šengeno konvenciją. Keletas nacionalinių teismų sprendimų parodė, kad Šengeno sistemai trūksta aiškios registracijos ir paieškos kriterijų, kuriais remiasi Susitariančiosios Šalys. Prancūzijoje, Rumunijos piliečio byloje, teismas kritikavo registracijos praktiką Vokietijoje. Čia valdžios institucijos registruoja duomenis apie asmenis, kurių prieglobsčio prašymas buvo atmestas. Prancūzijos teismas teigė, kad tokia praktika prieštarauja Šengeno susitartiems 96 straipsniui.

Reikia akcentuoti, kad Šengeno konvencijoje informacijos sistemos priežiūra numatyta dviem lygiais: nacionaliniu (114 straipsnis) ir bendru (115 straipsnis). Kalbant apie *nacionalinę priežiūrą,* Šengeno konvencija reikalauja, kad kiekviena Susitariančioji Šalis paskiria nacionalinę instituciją, kuri vykdo nacionalinės sekcijos SIS priežiūrą, nepriklausomai ir pagal nacionalinės teisės aktus.

Sekančiame darbo poskyriuje bus pateikiamas tyrimas kurio tikslas yra ištirti Lietuvos gyventojų pozicija Valstybės sienos apsaugos tarnybos pasirengimo ES išorės sienos apsaugos klausimu. Tokiu būdu bus bandoma ištirti biometrinio saugumo SIS e. valdžios koncepcijos įgyvendinimo Šengeno erdvėje aspektus diegiant e. sienos paslaugą Lietuvoje efektyvumą, bei poveikį visuomenei; pažymėtina jog bus vykdomas netiesioginis anketinis tyrimas.

3.3. VSAT valstybės sienos apsaugos įvertinimo netiesioginis tyrimas

Pagrindinis šio tyrimo tikslas: - ištirti, kaip Lietuvos gyventojai vertina Valstybės sienos apsaugos tarnybos pasirengimą ES išorės apsaugai.

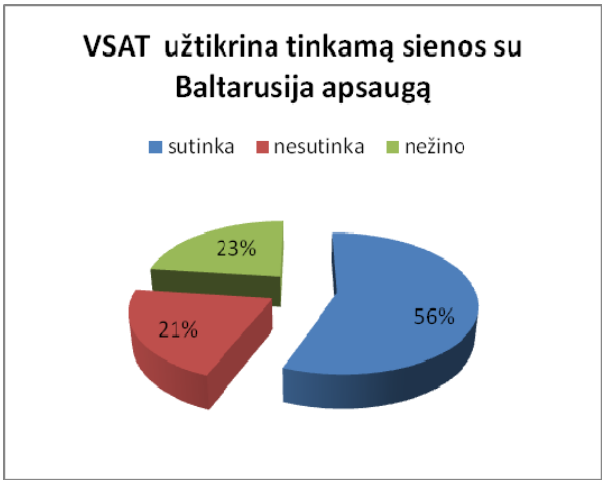
Tyrimo uždaviniai: – pasinaudojant empiriniu kokybiniu metodu, įvertinti VSAT darbuotojų pasirengimą ES sienos apsaugai. Remiantis respondentų atsakymų kokybiniu įvertinimu siekiama pateikti esamos situacijos analizę.

Tyrimo laikas: – 1 savaitė

Apklausos atlikimo metodas: – anketą užpildyti buvo prašoma piliečių, kertančių pasienio kontrolės punktus su Baltarusijos siena. Respondentų buvo prašoma atsakyti į esminius anketos klausimus tiesiogiai pasienio kontrolės punktuose. Respondentų skaičius varijuoja priklausomai

nuo kertančių sieną Lietuvos piliečių, bei nėra galimybės nustatyti apytikrio skaičiaus respondentų, kertančių sieną vienai dienai.

Imties skaičius: Atsižvelgiant į galimybės stoką išskirti imties amplitudę, buvo pasirinktas kokybinis empirinis tyrimas su esminiais klausimais.

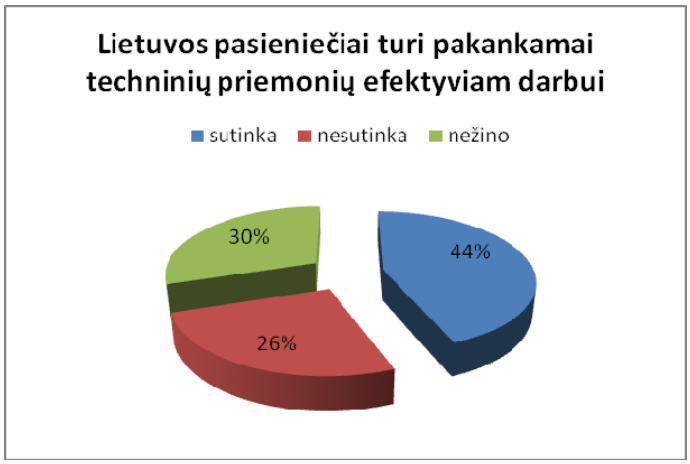


12 pav. Lietuvos piliečių vertinimas dėl tinkamos sienos su Baltarusija apsaugos

Daugiau nei pusė (56%) Lietuvos gyventojų mano, kad VSAT užtikrina tinkamą sienos su Baltarusija apsaugą. Penktadalis (21%) šalies gyventojų su tuo nesutinka, o ketvirtadalis (23%) neturėjo nuomonės šiuo klausimu. Aukščiau įvardinti duomenis leidžia teigti, jog VSAT veikla, užtikrinant e.sienos saugumą, yra pakankamai efektyvi, todėl teigiama, jog šiame regione yra užtikrinama pakankama perimetro kontrolė.

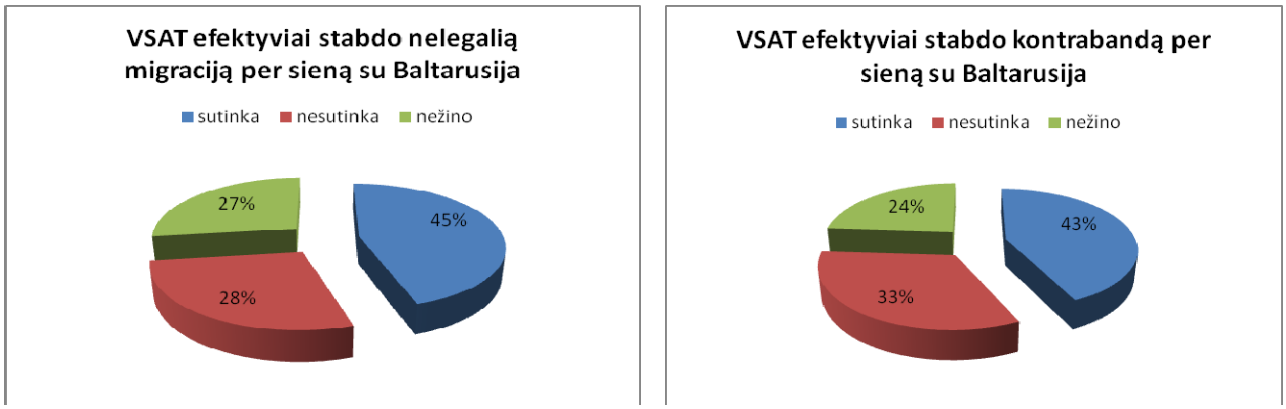
13 pav. Lietuvos piliečių vertinimas dėl PKP tinkamo įrengimo

Kas antras (49%) Lietuvos gyventojas mano, kad pasienio kontrolės punktai prie ES išorės sienų Lietuvoje yra tinkamai įrengti. Su tuo nesutinka apie šeštadalis (17%) respondentų, o trečdalis (34%) negalėjo to įvertinti. Dauguma Lietuvos gyventojų sutinka, jog pasienio kontrolės punktai prie sienos su Baltarusija yra tinkamai įrengti.



14 pav. Lietuvos piliečių vertinimas dėl pasieniečių techninio aprūpinimo

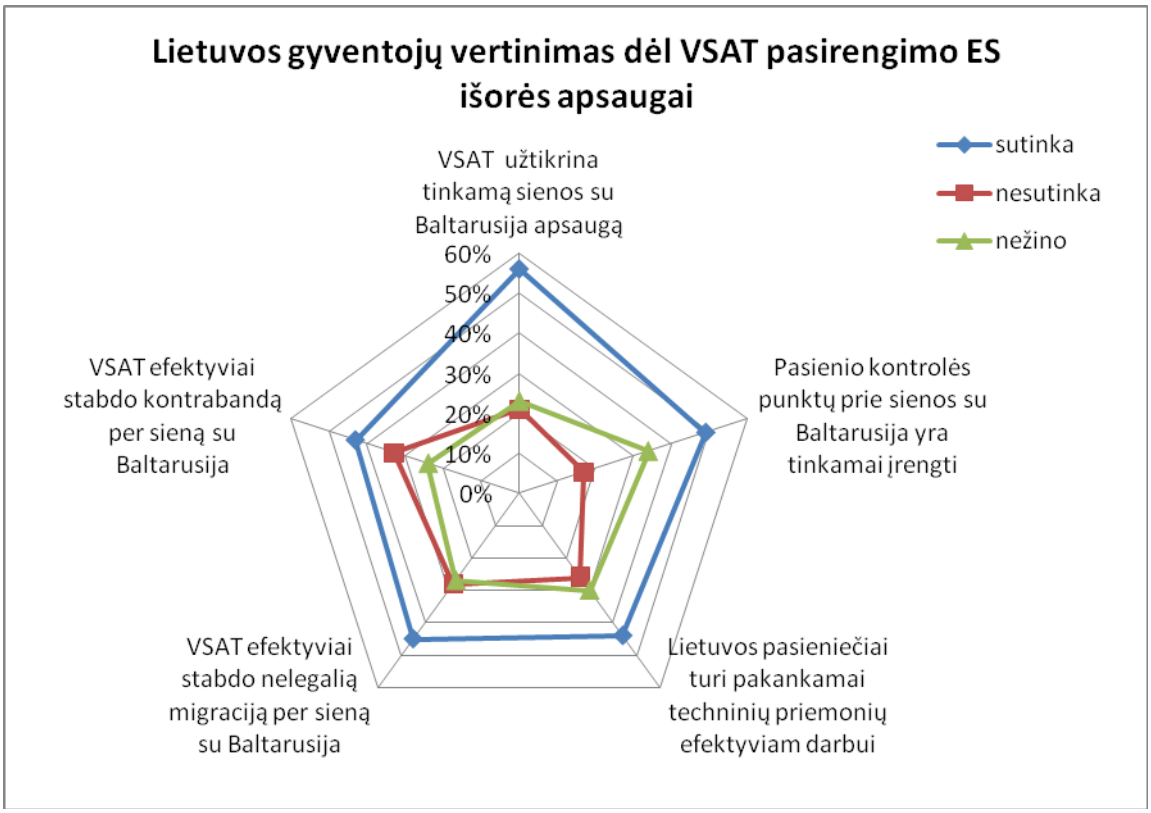
Daugiau nei keturi iš dešimties (44%) Lietuvos gyventojų mano, kad mūsų pasieniečiai turi pakankamai techninių priemonių efektyviam darbui (turi pakankamai automobilių, sraigtasparnių, laivų, ryšio ir stebėjimo priemonių). Su tuo nesutinka ketvirtadalis (26%) suaugusių šalies gyventojų, o trys iš dešimties (30%) neatsakė į šį klausimą. Pastebima, kad trečdalis Lietuvos gyventojų nėra susipažinę su Lietuvos pasieniečių veikla.



15 pav. Lietuvos piliečių vertinimas dėl nelegalų ir kontrobandos stabdymo efektyvumo

45% suaugusių šalies gyventojų sutinka, kad VSAT efektyviai stabdo nelegalią migraciją per sieną su Baltarusija, beveik trys iš dešimties (28%) su tuo nesutinka, o ketvirtadalis (27%) neturėjo nuomonės šiuo klausimu. Pastebima, jog Lietuvos gyventojai nedisponuoja pakankamu žinių kiekiu šiuo klausimu.

Keturi iš dešimties (43%) 15 – 74 metų Lietuvos gyventojų mano, kad VSAT efektyviai stabdo kontrabandą per sieną su Baltarusijos, o trečdalis (33%) su tuo nesutinka. Tai leidžia teigti, jog pasienyje egzistuoja saugumo užtikrinimo spragos.



16 pav. Lietuvos gyventojų vertinimas dėl VSAT pasirengimo ES išorės apsaugai

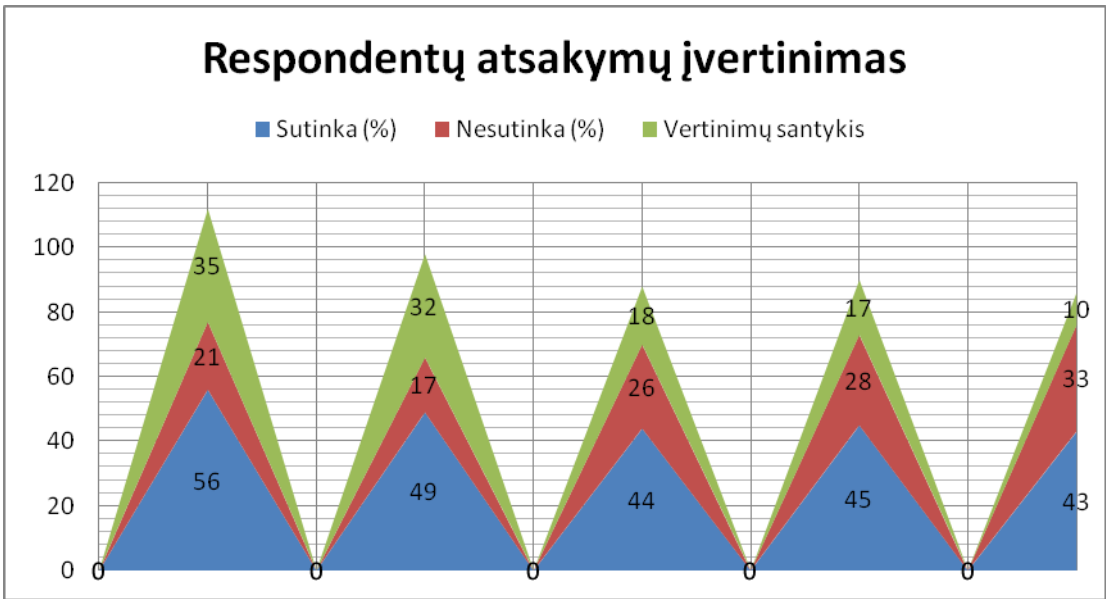
Tyrimo rezultatai: - Remiantis aukščiausius respondentų įvertinimus pelniusiais VSAT veiklos rodikliais, gaunami tokie rezultatai:

1. VSAT užtikrina tinkamą sienos su Baltarusija apsaugą pasienio kontrolės punktuose.
2. VSAT Užtikrina tinkamą sienos su Baltarusija perimetro saugumą.
3. Prie sienos su Baltarusija yra tinkamai įrengti kontroliniai postai.

Su kiekvienu iš šių teiginių sutinka pusė ar daugiau nei pusė respondentų, o su tuo nesutinka vienas iš penkių apklaustųjų.

Kiek mažiau nei pusė šalies gyventojų sutinka ir kas ketvirtas nesutinka, kad Lietuvos pasieniečiai turi pakankamai techninių priemonių efektyviam darbui bei su tuo, kad VSAT efektyviai stabdo nelegalią migraciją per sieną su Baltarusija. Santykinai mažiausia dalis šalies gyventojų sutinka su tuo, kad VSAT efektyviai stabdo kontrabandą per sieną su Baltarusija (su tokiu teiginiu nesutinka trečdalis apklaustųjų), nors bendrai kiek didesnė dalis šalies gyventojų mano, kad VSAT efektyviai stabdo kontrabandą.

Šis tyrimas parodo, kad dabartiniu metu Lietuvos gyventojai nejaučia nepatogumų kertant sieną su Baltarusija. Jie patenkinti VSAT darbu, o taipogi pasitiki pasieniečiais. Nuomonės, kad VSAT efektyviai stabdo nelegalią migraciją ir kontrabandą per sieną, rodo, jog kol kas nėra didelio būtinumo reorganizuoti pasienio kontrolės punktų struktūrą.

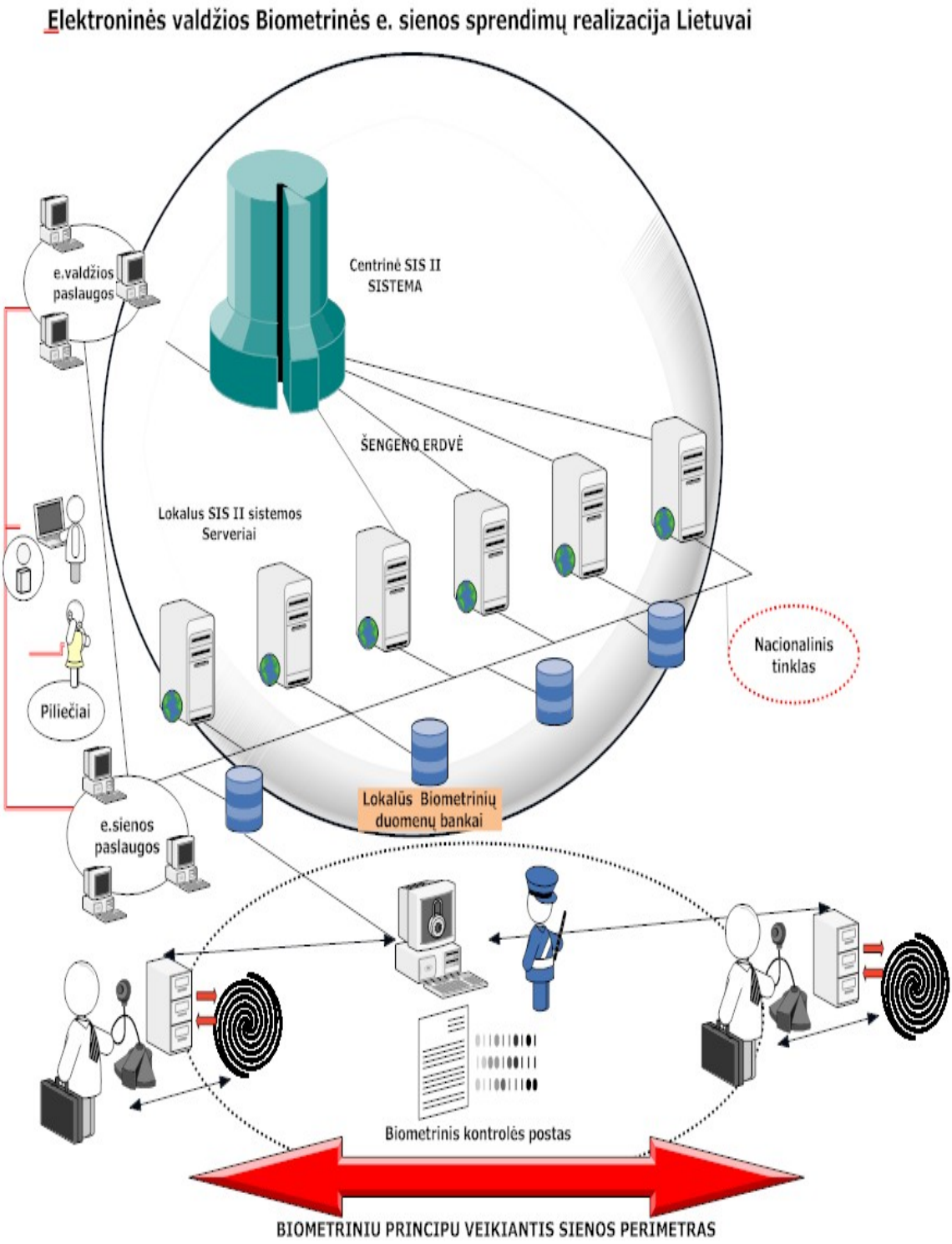


17 pav. Respondentų atsakymų įvertinimas

Iš atlikto respondentų atsakymų įvertinimo galima spręsti, kad Lietuvos gyventojai teigiamai vertina VSAT veiklą, nepaisant naujos vykdomos Šengeno erdvės biometrinio saugumo politikos, kurios realizavimo kontekste Lietuva smarkiai atsilieka. Atsižvelgus į ganėtinai aukštą respondentų atsakymų santykį, suformuojama prielaida, jog apklaustieji respondentai yra labai mažai informuoti apie geopolitinio saugumo užtikrinimo sprendimus, priimamus bendru ES mastu. Daroma prielaida, jog Lietuvos visuomenėje yra nepakankamai kalbama apie kompleksišką biometrinio saugumo problemą: Šengeno erdvės struktūros veiklą, galimybes ir privalumus. Taigi galima teigti, kad respondentų nuomonė VSAT išorės sienos apsaugos klausimu gali būti klaidinga. Dėl to būtina keisti sienų apsaugos struktūrą, ją tobulinti, stiprinti ir panaudoti integruotame sienų valdyme visas naujas technologijas, kurios buvo aptartos antroje darbo dalyje.

Tyrimo išvada: Lietuvos gyventojai vertina Valstybės sienos apsaugos tarnybos pasirengimą tinkamai užtikrinti ES išorės sienos apsaugą pozityviai, tačiau atsižvelgus į atliktą respondentų atsakymų kokybinį įvertinimą, patvirtinama, jog Lietuvos piliečiai nėra tinkamai informuoti, arba stokoja informacijos apie biometrinius pasus bei Šengeno informacinę sistemą. Kadangi įstojimas į Šengeno erdvę iškėlė naujus uždavinius Lietuvos VSAT bei komplikavo sienos apsaugos kontrolės procesą, daroma prielaida, kad Lietuvoje vertėtų prioritetine tvarka įdiegti e. valdžios biometrinės e. sienos sprendimus.

Išnagrinėję valstybės kontrolės audito ataskaitas, atlikę anketinį tyrimą bei išstudijavę Šengeno sistemos raidos bei išsivystymo galimybes, siūlome būtent tokią e.sienos sprendimo realizaciją Lietuvai (18 pav.).



18 pav. E. valdžios biometrinės e. sienos sprendimų realizacija Lietuvai

Sudaryta autorės

Pagrindinis superkompiuteris – centrinė SIS II sistema, prie jos yra prijungti lokalūs SIS II sistemos serveriai ir kai kuriuose valstybėse veikiantys SIS I serveriai. Apskritimas apibūdina Šengeno erdvę, į kurią patenka lokalios sistemos ir globali sistema. Faktiškai, e.valdžios paslaugos realizuojamos tiesiogiai stebint centrinę SIS sistemą. Vykdomoji valdžia – valdžios organai – tarpusavyje pasikeičia informacija, taip sukurdami e.valdžios gyvavimo prielaidą, kuri turi tam tikrų demokratinių bruožų.

Esamoje schemoje mes galime pamatyti **du esminius dalykus**:

1) e. valdžios paslaugas;

2) e. sienos paslaugas.

E. valdžios paslaugos tiesiogiai realizuojasi įskiepijant centrinę SIS II sistemą, nes nacionalinis tinklas, kuriame egzistuoja lokalūs biometrinių duomenų bankai, yra nacionalinis bei priklauso vyriausybei, ir tiesioginę kontrolę vykdo VRM. Prie nacionalinių duomenų prieigą turi tik tam tikri piliečiai ir, vėl gi, ne prie visų, o tik prie tam tikrų pogrupių.

E. sienos paslaugos realizuojamos taip: pilietis, užsisakęs pažymą arba paskambinęs telefonu, gauna tam tikrą informaciją elektroniniu būdu arba automatiniu registravimo būdu.

Faktiškai, mes nagrinėjame paslaugas, kurios turi praktinį pritaikymą ir realų pagrindimą. Todėl mes nagrinėjame tos pačios sistemos sukūrimo modelį ir kokiu būdu jis veikia. Jeigu mes nagrinėsime biometriniu principu veikiantį sienos perimetrą, tai matome, kad ateina individas, nuskanuojami jo pirštų antspaudai, akies rainelė. Šie duomenys keliauja į automatinio nuskaitymo sistemą, kuri yra tiesiogiai sujungta su kompiuteriu, prie kurio sėdi budintis pareigūnas. Nuskaičius duomenis, jie keliauja į lokalią biometrinių duomenų bazę, nes poste yra tik atskiras kompiuteris su apsaugotu ryšiu. Iš lokalaus biometrinių duomenų banko medžiaga keliauja į lokalų SIS sistemos serverį. Lokalus biometrinių duomenų bankas gali būti tam tikroje VSAT rinktinėje. Iš rinktinės duomenys keliauja į centrinės būstinės serverį, kuris yra tiesiogiai sujungtas su Lietuvos VRM sistema. Iš ten keliauja į SIS. Tai yra tiesioginis priėjimas ir visas procesas vyksta per kelias sekundes.

Esamos sistemos trūkumas, lyginant su siūlomų biometriniu e.sienos modeliu, Lietuvai yra toks, kad informacija apie duomenis yra užklausiama žodiniu būdu, o biometriniai duomenys persiunčiami ne pagal automatizuotą sistemą ir patikrinimas vyksta tik „EURODAC“ sistemoje. Siūlomo modelio privalumas yra tai, kad „EURODAC“ sistema persiunčia pabėgėlių bei nusikaltėlių duomenis, t.y. jų biometrinius duomenis iš/į lokalius biometrinius bankus, tarpininkaujant lokaliems SIS II sistemos serveriams - taip užtikrinamas aukščiausio lygio duomenų verifikacijos procesas bei padidinamas nacionalinių pasienio kontrolės postų sutikrinamų duomenų srautų našumas (kiekis). Biometrinio paso duomenų cirkuliavimas vyksta analogiškai.

Siūlomi sprendimai įgalina automatizuoti biometrinių duomenų nuskaitymo procesą, realizuoti biometrinio saugumo e. sienos koncepciją Lietuvoje užtikrinant e. valdžios nacionalinio tinklo viešojo administravimo efektyvumą.

IŠVADOS

Magistro darbe buvo nagrinėjamos biometrinio sienų saugumo e. sienos sudedamosios dalys, akcentuojant besiformuojančią Lietuvos e. valdžios biometrinės sistemos e. sienos koncepciją.

Užfiksuoti trūkumai e.sienos, biometrinio saugumo realizavimo (SIS bei nacionalinių registrų valdymo bei kontrolės) srityje, atskleidžiant SIS II bei nacionalinių pasienio kontrolės punktų informacinių duomenų filtravimo sistemų neefektyvumą, siekiant apibrėžti bei ištirti biometrinio sienų saugumo vaidmenį formuojant automatizuotą biometrinių duomenų nuskaitymo sistemą bei realizuoti biometrinio saugumo e. sienos koncepciją Lietuvoje, sukuriant e. valdžios nacionalinio tinklo viešojo administravimo kontrolės mechanizmą (18 pav.)

1. Atlikus e.valdžios tyrimus, nėra pakankamai aiškiai apibrėžiami pagrindiniai veiklos vertinimo kriterijai, neatsižvelgiama į veiklos efektyvumą ir rezultatyvumą, nes viešųjų e.paslaugų kokybė nėra sistemingai stebima ir koreguojama, jų pridėtinė vertė nėra sistemingai matuojama, verslas į elektroninių paslaugų kūrimo procesą nėra įtraukiamas, jo kompetencija, finansiniai pajėgumai ir motyvacija nėra išnaudojami.
2. Neegzistuoja vientisos standartizacijos sistemos, kas savo ruožtu užkerta kelią realizuoti globalią integruotą e. sienos paslaugą pasaulyje, nes egzistuoja biometrinių duomenų kodavimo bei perdavimo standartų skirtumai.
3. Kai kurios e. valdžios koncepcijos nuostatos yra pasenusios ir neatitinka tikrovės, todėl negalimas efektyvus biometrinių sienų saugumo įgyvendinimas.
4. Tam, kad būtų išlaikomas informacinės visuomenės plėtros politikos vientisumas ir nuoseklumas, būtini konkretūs e.valdžios strateginių dokumentų įgyvendinimo planai, atsižvelgiant į Šengeno srities strateginius dokumentus bei plėtojamą e. sienos koncepciją.
5. Elektroninės valdžios koncepcijoje stebėjimo ir valdymo funkcijos priskirtos skirtingoms institucijoms, o tai komplikuoja e. valdžios e. paslaugų įgyvendinimo kontrolę bei neužtikrina efektyvaus biometrinių sienų saugumo.
6. Nesant objektyvios stebėsenos mechanizmų, nevykdomas informacinių technologijų procesų valdymo etapas - esamos būklės stebėjimas ir įvertinimas, o įvertinimo procesas reikalingas vadovybei įsitikinti, jog suplanuoti procesai vyksta numatyta linkme ir numatytu laiku. Jei nustatytų tikslų nepasiekiama, vadovybė turėtų imtis priemonių ištaisyti susiklosčiusią padėtį (nukrypimus).
7. Nustatytas menkas žmonių informuotumas apie biometrinių domenų rinkimą, saugojimą bei panaudojimą. Nepaisoma biometrines koncepcijos svarbos, siekiant stiprinti biometrinį saugumą.

Kokybiniai e.valdžios vertinimai yra aktualūs visos Europos mastu, nes aktualios informacijos teikimas, kiekybinis vertinimas, lyginamoji analizė, matavimas ir poveikio bei naudos lyginimas yra labai svarbūs e. valdžios paslaugoms populiarinti. Todėl 4 lentelėje pateikiami e. sienos rekomendacinės diegimo gairės Lietuvoje.

Biometrinio e. sienos saugumo formavimo rekomendaciniai veiksniai Lietuvoje

4 lentelė. E. sienos rekomendacinės diegimo gairės Lietuvoje

E. sienos degimo Lietuvoje gairės	Gairių aprašymas
Implementuojama sistema turi būti tiksli	Biometrinės technologijos iš esmės turėtų padidinti jau naudojamų asmens identifikavimo priemonių tikslumą, plėsti jų pritaikomumo spektrą modifikuojant tiesiogiai teikiamas e. valdžios paslaugas.
Pažangus atpažinimo metodai, yra būtini siekiant įgyvendinti e. valdžios koncepciją. Biometrinės technologijos, tai būtina autentifikavimo priemonė	Neatskiriamu elementu teikiant naudingąsias e. valdžios vidaus naudojimo e. paslaugas pasienyje yra patikima bei veiksminga autentiškumo patvirtinimo procedūra.
Biometriniai duomenys yra svarbi sudėtinė dalis numatomu teikti e. valdžios paslaugų	Biometrinės technologijos yra itin svarbios siekiant veiksmingos sąveikos tarp piliečių ir valstybės, kurios paskirtis apsiriboja saugų duomenų tvarkymu bei e. valdžios e. paslaugų vykdymu. Biometrinės tapatybės nustatymo priemonių taikymas taip pat tinka vykdyti kitoms programoms, pavyzdžiui, vairuotojo pažymėjimų gavimas bei informacijos apie subjekto sveikatos duomenų gavimas.
Biometrinės diegiamos paslaugos e. valdžioje buti orientuotos į privatumo didinimą bei įgauti piliečių pasitikėjimą	Biometrinės sistemos negali tapti asmeninės autorizacijos defaktiniu standartu identifikuojant asmens duomenis bei formuojant piliečių požiūrį apie e. sieną bei e. saugumą be skaidriai suformuluoto piliečių požiūrio į galimus e. sienos, biometrinių duomenų pažeidimus bei privatumą. Diegiant potencialios biometrinės elektroninės valdžios paslaugas, reikėtų naudoti sistemą, kuri pateisina privatumo ir pasitikėjimo lūkesčius yra centralizuota bei efektyviai apdorojanti gaunamus bei siunčiamus duomenis.
Lietuvos vyriausybė turi būti informuota apie tarptautinio masto geopolitinius išorinius faktorius, tiesiogiai įtakojančius pažangių biometrinių sistemų dislokavimą aqua geo bei aero sąlyčio taškus.	Priėmimas ir naudojimasis įvairiomis biometrinėmis saugumo priemonėmis, yra smarkiai įtakotas tarptautinės politikos. Imigracijos, terorizmo bei kontrabandos ir pabėgėlių grėsmėms likviduoti reikalinga tiksli naudotojų identifikacija. Lietuvos vyriausybei būtina suvokti biometrinės raidos etapus kitose šalyse, todėl, kad vertinant Lietuvos nacionalinio tinklo veiklos efektyvumą remiantis valstybės kontrolės ataskaitomis buvo nustatyta, jog lygiaverčių tarptautinių biometrinio saugumo priemonių taikymas e. sienoje atsilieka - Lietuva neturi biometrinės tapatybės identifikuojančiu prietaisų o jų sistemos degimas "atsilieka". Be to, Lietuvos vyriausybė turi būti informuota apie technologijų pažangą įgyvendinant kai kurias formas biometrinių technologijų, formuojant informacinių standartų suderinamumą, kurie galėtų turėti įtakos formuojant metodus ir priemones, taikomas Lietuvoje teikiant elektroninės valdžios e. sienos paslaugas.

Sudaryta autorės

Atsižvelgiant į pateiktą lentelę, teigiama, jog šioje lentelėje numatoma sukurti e.sienos poveikio matavimo sistemą, kuri gali būti papildoma priemonė, padėsianti nustatyti duomenų naudojimo būdus, pvz., nustatyti e.valdžios investicijų ir produktyvumo santykį arba e.valdžios politikos bei programų poveikį visai Lietuvos informacinei visuomenei.

Bendri rekomendaciniai veiksmai

1) Siekiant užtikrinti informacinės ir žinių visuomenės plėtros politikos vientisumą ir nuoseklumą, taip pat Šengeno erdvės nuostatuose numatytų pagrindinių uždavinių įgyvendinimo kontrolę e.sienos klausimu, didesnis dėmesys turėtų būti skiriamas biometriniam sienų saugumo ir jų techninių charakteristikų plėtojimui, atsižvelgiant ne tik į lėšų informacinėms technologijoms pagrįstumą, bet ir projektų įgyvendinimo laiko pagrįstumą bei įgyvendinimo galimybes.
2) e.valdžios projektų vertinimai turi būti atliekami nuolat ir visapusiškai, vertinant ne tik patį e.valdžios projektų įgyvendinimo faktą, bet ir jų įgyvendinimo efektyvumą ir rezultatyvumą.
3) VRM ir IVPK turėtų naudotis atliktų tyrimų ir apklausų rezultatais e. valdžios projektų įgyvendinimo efektyviam valdymui ir stebėjimui užtikrinti ir pateikti juos Informacinės ir žinių visuomenės plėtros komisijai susipažinti, kad ji priimtų teisingus sprendimus.

LITERATŪRA

Norminiai teisės aktai

1. Lietuvos Respublikos Vidaus reikalų ministro 2007 m. rugsėjo 17 d. įsakymas „Dėl Lietuvos nacionalinės Šengeno informacijos sistemos nuostatų patvirtinimo“ [PDF HTML kopija].http://www.vrm.lt/fileadmin/Image_Archive/IRD/teises_aktai/D_L_LIETUVOS_NACIONALIN_S__ENGENO_INFORMACIN_S_SISTEMOS_NUOSTAT__PATVIRTINIMO.pdf [žiūrėta 2008 11 12]
2. Komisijos sprendimas 2006/VI/28 nustatantis valstybių narių išduodamų pasų ir kelionės dokumentų apsauginių savybių ir biometrikos standartų technines specifikacijas. http://www.ec.europa.eu/justice_home/doc_centre/freetravel/documents/doc/c_2006_2909_lt.pdf [žiūrėta 2008 11 22]
3. Lietuvos Respublikos Vyriausybės 2002 m. gruodžio 31 d. nutarimas Nr. 2115 „Dėl Elektroninės valdžios koncepcijos patvirtinimo”. http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=198184 [žiūrėta 2008 10 03]
4. Tarybos reglamentas dėl antros kartos Šengeno informacinės sistemos (SIS II) sukūrimo (EB) Nr. 2424/2001 2001 m. gruodžio 6 d. http://www.policija.lt/tarp_bendradarbiavimas/sengeno_teisynas/SIS%20SIRENE/Tarybos%20reglamentas%202424_2001.doc [žiūrėta 2008 11 05]
5. Direktyvos 95/46/EB 29 str. darbo grupės 2001 m. rugsėjo 13 d. Darbinis dokumentas Nr. 12168/02, WP 80 „Dėl biometrinių duomenų“. http://www.ada.lt/images/cms/File/WP80.pdf [žiūrėta 2008 04 02]
6. Europos parlamento ir tarybos direktyva (95/46/EB) 1995 m. spalio 24 d. dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (OL L 281, 23.11.1995, p. 31). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1995L0046:20031120:LT:PDF [žiūrėta 2008 06 05]
7. Europos Parlamento Ir Tarybos Direktyva 2002/58/EB 2002 m. liepos 12 d. „Dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių)“. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:LT:HTML [žiūrėta 2008 11 12]
8. Valstybinio audito ataskaita. Valstybinių institucijų informacinių sistemų valdymas e.valdžios kontekste. 2007 rugsėjo 28d. Nr. IA-9000-4-3.

9. Nuomonė 3/2005 dėl 2004 m. gruodžio 13 d. Tarybos reglamento (EB) Nr. 2252/2004 „Dėl valstybių narių išduodamų pasų ir kelionės dokumentų apsauginių savybių ir biometrikos standartų įgyvendinimo“. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp112_lt.pdf [žiūrėta 2008 11 30]
10. Nuomonė Nr. 3/2007 dėl pasiūlymo dėl Europos Parlamento ir Tarybos reglamento, iš dalies keičiančio diplomatinėms atstovybėms ir konsulinėms įstaigoms skirtas Bendrąsias konsulines instrukcijas dėl vizų atsižvelgiant į biometrinių duomenų įdiegimą, įskaitant nuostatas dėl prašymų išduoti vizą priėmimo ir nagrinėjimo organizavimo (COM (2006) 269 galutinis). http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp134_lt.pdf [žiūrėta 2008 11 22]
11. Darbo dokumentas Nr. 1dėl Komisijos komunikato COM(2008) 0069 Pasirengimas kitiems Europos Sąjungos sienų valdymo etapams. Piliečių laisvių, teisingumo ir vidaus reikalų komitetas: http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dt/744/744600/744600lt.pdf [žiūrėta 2008 10 06]
12. Council framework decision on the use of Passenger Name Record (PNR) for law enforcement purposes. Brussels, 6.11.2007. COM(2007) 654 final. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0654:FIN:EN:PDF [žiūrėta 2008 11 12]
13. Europos parlamento ir tarybos direktyva (95/46/EB),1995 m. spalio 24 d. dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo.(OL L 281, 23.11.1995, p. 31). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1995L0046:20031120:LT:PDF [žiūrėta 2008 11 30]

Specialioji literatūra

14. **Dessimoz D., Richiardi J., Champod C., Drygajlo A.** Multimodal Biometrics for Identity // State-of-the-Art Research Report PFS 341-08.05 (Version 2.0). http://www.europeanbiometrics.info/images/resources/90_264_file.pdf [žiūrėta 2008 11 22]
15. ID management lifecycle and eGovernment. Made in Germany - Deutschlands Engagement in der Welt. Version Deutschlands Engagement in der Welt 1, 23.01.2008. http://www.germanyandafrica.diplo.de/Vertretung/pretoria__dz/en/03__Business__und__Development/Downloaddateien/download__element__3,property=Daten.pdf [žiūrėta 2008 11 12]

16. **Kajevic B., Sjoberg T., Muus P.** Biometrics: A New Mean of Surveillance and Migration Control// Malmo University IMER 41-80 2006-06-02. http://dspace.mah.se:8080/bitstream/2043/4924/1/masterthesis.pdf [žiūrėta 2008 11 12]
17. Most M.Biometrics and Border Control Beyond US-VISIT http://magazine.digitalidworld.com/Sep04/Page18.pdf [žiūrėta 2008 11 30]
18. Darbinis dokumentas Nr. 12168/02, WP 80 „Dėl biometrinių duomenų“. http://www.ada.lt/images/cms/File/WP80.pdf [žiūrėta 2008 11 12]
19. Border Management in the New Century - Emerging Trends and Best Practices IBM Global Business Services. http://www-03.ibm.com/industries/global/files/Border_Management_in_the_New_Century.pdf?re=government&sa_message=title=border_management_in_the_new_century [žiūrėta 2008 10 06]
20. **Dr Frank P.** Biometric borders // 4TH Ministerial e-government conference, 2007
21. IBM Institute for Business Value. Expanded borders, integrated controls. Achieving national prosperity and protection through integrated border management. http://www-935.ibm.com/services/us/imc/pdf/g510-6218-expanded-borders.pdf [žiūrėta 2008 11 30]
22. Securing and Speeding the Global Movement of People. Customs, Ports and Borders Candidate and Visitor Screening. http://t1d.www-03.cacheibm.com/industries/government/doc/content/bin/Candidate_and_Visitor_Screening_Brief.pdf [žiūrėta 2008 11 12]
23. Advanced Customs & Border ControlAccess System - RIMCO XXI ApplicationNote# 0823. August 23, 2005. http://www.rimco.ru/_files/AN0823.pdf [žiūrėta 2008 11 25]
24. e-Government Solutions - ACCESS secure identity, 2008 Creating a world with more security, efficiency and freedom, all at the same time. http://www.hidglobal.com/documents/egov_solutions_broch_en.pdf [žiūrėta 2008 11 25]
25. Leveraging Biometric Technology for Border Control, Immigration Management and the Transportation Industry – Daon *September 2005*.
26. Border Control System for Lithuania - A milestone on the road to the European Union. Siemens IT Solutions and Services. http://www.it-solutions.siemens.com/b2b/it/en/global/Documents/References/Lithuania_BorderControlSystem_PDF_e.pdf [žiūrėta 2008 11 12]
27. Department of Homeland Security Office of the CIO E-Government Act Report 2007. http://www.dhs.gov/xlibrary/assets/cio_egov_annual_report_2007.pdf [žiūrėta 2008 11 12]
28. Leveraging Biometric Technology for Border Control, Immigration Management and the Transportation Industry. http://www.europeanbiometrics.info/images/resources/27_560_file.pdf [žiūrėta 2008 11 12]

29. Digital Identities Security and Privacy - Institute for the Protection and Security of the Citizen. http://ipsc.jrc.ec.europa.eu/showdoc.php?doc=promotional_material/leaf-biometrics_red-04.pdf&mime=application/pdf [žiūrėta 2008 11 30]
30. IBM Public Sector. Biometrics for secure border management.http://www-03.ibm.com/industries/government/doc/content/bin/Border_Management_Biometrics_July05_2.pdf [žiūrėta 2008 11 12]
31. Support to and Coordination of Integrated Border Management Strategies. Contract No. 81242. Inter-agency Training Manual. http://gfptt.org/uploadedFiles/7488d415-51ca-46b0-846f-daa145f71134.pdf [žiūrėta 2008 11 25]
32. UK Border Agency. FAQ e-Borders. http://www.bordercontrolrecruitment.co.uk/faqs.asp [žiūrėta 2008 11 12]
33. Coesys eBorder Solutions for National Security - Providing effective border control. Helping citizens to travel freely and securely, 2007. http://www.gemalto.com/brochures/download/coesys_border.pdf [žiūrėta 2008 11 12]
34. Kuriami svetingi ir saugūs Lietuvos pasienio ruožai, 2006 08 03. http://www.vrm.lt/index.php?id=644 [žiūrėta 2008 09 21]
35. **Kochems A., Schwartz A.** Biometric Technologies: Security, Legal, and Policy Implications by Paul Rosenzweig. http://www.heritage.org/Research/HomelandSecurity/upload/65326_1.pdf [žiūrėta 2008 11 12]
36. Ryšių su visuomene agentūra „MEDIA Baltijos verslas"; Šengeno erdvės aktualijos. http://www.mediabv.lt/res_all.php?id=213[žiūrėta 2008 11 30]
37. Biometriniai duomenys ir skaitmeninis sertifikatas – neatskiriami. http://www.5ci.lt/Default.asp?DL=L&TopicID=82&NewsID=90097&ArcMonth=&ArcYear= [žiūrėta 2008 11 12]
38. Nelegali migracija: būtina glaudi partnerystė. http://www.europarl.europa.eu/sides/getDoc.do?language=LT&type=IM-PRESS&reference=20060717STO09891&secondRef=0 [žiūrėta 2008 11 06]
39. Lietuvos Respublikos Valstybės sienos apsaugos tarnyba. http://www.pasienis.lt [žiūrėta 2008 11 12]
40. 2005 m. rugsėjo 16 d rezoliucija priimta.27-ojoje Tarptautinėje duomenų apsaugos ir privatumo įgaliotinių konferencijoje Montreux "Dėl biometrijos naudojimo pasuose, identifikavimo kortelėse bei kelionės dokumentuose“. http://www.ada.lt/images/cms/File/rezoliucija_konferencijos_medz.pdf [žiūrėta 2008 11 12]
41. Kad neliktų vidaus kontrolės, būtina stiprinti išorinę. Verslo žinios, 2006 01 24, Nr. 16, 10p. http://archyvas.vz.lt/news.php?id=252388&strid=1002&rs=0&ss=&y=2006%2001%2024 [žiūrėta 2008 11 12]

42. **Wayman J., Jain A., Maltoni D., and Maio D**. An introduction to biometric authentication systems, in Biometric Systems // Technology, Design and Performance Evaluation, Eds. London: Springer-Verlag, 2005, 1 d., p. 1–20.
43. **Clarke R.** Human identification in information systems: Management challenges and public policy issues. // Information Technology and People, p. 6–37, 1994.
44. Šengeno erdvė – Europa be sienų – saugumo garantas. http://www.kalvarija.lt/Naujienos/dsp_newsr.php?Title=&From=&To=&Page=2&list=10 [žiūrėta 2008 09 02]
45. Biometric Technology Today, "Part 1: Biometrics and ePassports," Biometric Technology Today, Nr. 6, p. 10–11, 2005.
46. Методология интегрированного управления границами.PS-Форум,Москва, 23 марта 2006 г. http://www.ibm.com/ru/events/presentations/ic06/public/kouwenhoven.pps [žiūrėta 2008 11 30]
47. Lietuva ir Europos Sąjunga. Šengeno erdvė. http://www.euro.lt/lt/apie-lietuvos-naryste-europos-sajungoje/lietuva-ir-europos-sajunga/sengeno-erdve/ [žiūrėta 2008 11 12]
48. Биометрический паспорт Европы: какому варианту отдать предпочтение?. http://www.goethe-bytes.de/dw/article/0,2144,1011523,00.html [žiūrėta 2008 11 12]
49. Российский биометрический портал. http://www.biometric.ru/document.asp?group_id=50&nItemID=805&sSID=3.53 [žiūrėta 2008 11 12]
50. Стандарты биометрии. http://www.guardinfo.ru/tech/normatives/reglament/reglament_3293.html [žiūrėta 2008 04 02]
51. Реорганизация американской иммиграционной системы (2002-2004 гг.) http://demoscope.ru/weekly/2005/0207/analit04.php [žiūrėta 2008 11 12]
52. Определение уровня неопределенности при осуществлении проектов в области электронного правительства. Национальный доклад ВОФК США. http://www.ach.gov.ru/in/material/m04-06.pdf [žiūrėta 2008 11 30]
53. Биометрические технологии призваны укрепить безопасность американских границ – и обогатить американских инвесторов. http://www.k2kapital.com/analytics/reviews/93687.html [žiūrėta 2008 11 12]
54. Biometric border solution. Prieiga per internetą: http://www.csg.org/pubs/Documents/sgn0205BiometricBorder.pdf [žiūrėta 2008 11 12]

Krasauskaitė V. Biometrinis sienų saugumas: e. siena ir Lietuva Šengeno erdvėje / Viešojo administravimo magistro baigiamasis darbas. Vadovas prof. dr. A. Augustinaitis. – Vilnius: Mykolo Romerio universitetas, Ekonomikos ir finansų valdymo fakultetas, 2008. – 86 p.

ANOTACIJA

Magistro baigiamajame darbe išanalizuota ir įvertinta e. valdžios koncepcija, užtikrinant sienų saugumą, analizuojant biometrinių duomenų naudojimo aspektus bei jų sąsajas su duomenų apsaugos reikalavimais, iškeltos integruoto sienų valdymo įdiegimo strategijos, asmens identifikavimo problemos bei pateikti pasiūlymai, kaip šias problemas spręsti. Pirmoje darbo dalyje teoriniu aspektu tiriamas ES elektroninės valdžios integruotų e. sienų valdymo ir biometrinio saugumo aspektai, akcentuojama informacinės visuomenės svarba. Antroje dalyje tiriama e. sienos integruoto valdymo praktinė realizacija bei biometrinių perimetro saugos sistemų realizavimo ypatumai ES bei pasaulio šalių praktikoje. Trečioje dalyje aptariamos biometrinio saugumo e. valdžios įgyvendinimo Šengeno erdvėje problemos diegiant e. valdžios e. sienos paslaugą Lietuvoje.

Pagrindiniai žodžiai: e. valdžia, e. siena, biometrinis saugumas, integruotas e. sienų valdymas, Šengeno erdvė.

Krasauskaitė V. Biometric border security: e-border and Lithuania in the Schengen area / Master's Work in Public administration. Supervisor prof. dr. A. Augustinaitis. - Vilnius: Faculty of Economics and Finance Management, Mykolas Romeris University, 2008. – 86 p.

ANOTATION

Master work reviewed and assessed the concept of e - government, ensuring border security in the analysis of the use of biometric data elements and their interrelationships with data protection requirements, bringing the introduction of integrated border management strategy, identification problems and proposals to solve these problems. The first work in theoretical aspects studied in the EU e-government integrated e - border management and biometric security elements, stressing the importance of the information society. The second part of the examined integrated e-border management and the practical implementation of biometric perimeter security systems realization peculiarities of the EU and the countries of the world in practice. The third part deals with biometric

security e - government in the implementation of the Schengen area of installation problems e-government e-border service in Lithuania.

Key Words: e. government, e. border, biometric security, integrated e.-border management, Schengen area.

Krasauskaitė V. Biometrinis sienų saugumas: e. siena ir Lietuva Šengeno erdvėje / Viešojo administravimo magistro baigiamasis darbas. Vadovas prof. dr. A. Augustinaitis. – Vilnius: Mykolo Romerio universitetas, Ekonomikos ir finansų valdymo fakultetas, 2008. – 86 p.

SANTRAUKA

Viešojo administravimo magistro baigiamojo darbo tema yra aktuali, nes darbe buvo nagrinėjami biometrinio sienų saugumo e. sienos sudedamieji akcentuojant besiformuojančią Lietuvos e. valdžios biometrinės sistemos e. sienos koncepciją. Užfiksuoti e. sienos, biometrinio saugumo realizavimo (SIS bei nacionalinių registrų valdymo bei kontrolės srityje) trūkumai, atskleidžiant SIS II bei nacionalinių pasienio kontrolės punktų informacinių duomenų filtravimo sistemų neefektyvumą su tikslu apibrėžti bei ištirti biometrinio sienų saugumo vaidmenį, formuojant automatizuotą biometrinių duomenų nuskaitymo sistemą bei realizuoti biometrinio saugumo e. sienos koncepciją Lietuvoje, sukuriant e. valdžios nacionalinio tinklo viešojo administravimo kontrolės mechanizmą. Buvo nagrinėjami ES elektroninės valdžios integruotų e. sienų valdymo ir biometrinio saugumo aspektai, akcentuojama informacinės visuomenės svarba.

Detaliau aptarta integruota Europos sienų valdymo strategija bei išplėstas integruotas sienų valdymas: nacionalinio tinklo įtaka sienos vadybai, rizikos valdymas. Išskirtinis dėmesys buvo skiriamas Lietuvos Šengeno erdvėje pozicijai įstirti. Plačiau apžvelgiamas Šengeno (acquis) teisynas, informacinė sistema ir jos paskirtis, “ EURODAC“ bei vizų informacinės sistemos (VIS) analizė bei biometriniai pasai bei jų taikymo problemos Lietuvoje.

Darbe aptariama e. sienos integruoto valdymo praktinė realizacija, biometrinių perimetro saugos sistemų realizavimo ypatumai ES bei pasaulio šalių praktikoje. Išanalizuojamas efektyvios sienos kontrolės užtikrinimo projektas detaliau aptariant e-sienos paskirtį bei vaidmenį, užtikrinant biometrinį perimetro saugumą e. sienos kontrolės kontekste. Atliekama biometrinės sistemos analizė, išanalizuojamos biometrinės operacijos, duomenų apdorojimo etapai, ištiriamas biometrijos sistemų funkcionalumas ir efektyvumas; pritaikomumas pasienio kontrolėje. Nagrinėjamos biometrinio saugumo e-valdžios įgyvendinimo Šengeno erdvėje problemos diegiant e. valdžios e. sienos paslaugą Lietuvoje. Apžvelgiami elektroninės valdžios e. paslaugų administravimo aspektai informacinės visuomenės kontekste bei pateikiami sprendimai dėl biometrinės saugumo SIS e. valdžios koncepcijos įgyvendinimo Šengeno erdvėje problemos. Diegiant e. sienos paslaugą Lietuvoje atliekamas VSAT valstybės sienos apsaugos įvertinimo netiesioginis tyrimas bei pateikiamai e. valdžios biometrinės e. sienos sprendimų realizacija Lietuvai pasiūlymai bei rekomendacijos.

Siūlomi sprendimai įgalina automatizuoti biometrinių duomenų nuskaitymo procesą, realizuoti biometrinio saugumo e. sienos koncepciją Lietuvoje, užtikrinant e. valdžios nacionalinio tinklo viešojo administravimo efektyvumą.

SUMMARY

Krasauskaitė V. Biometric border security: e-border and Lithuania in the Schengen area / Master's Work in Public administration. Supervisor prof. dr. A. Augustinaitis. - Vilnius: Faculty of Economics and Finance Management, Mykolas Romeris University, 2008. – 86 p.

Public administration master's final work is a constant theme because of the work was considered a biometric border security e-border constituent emphasis on the emerging Lithuania biometric e-government system e-border concept. Fixed the outlets deficiencies of e-border, biometric security (SIS and national registers of management and control) identified in the SIS II and the national border control points of information filtering systems, the ineffectiveness of purpose to define and explore a biometric border security role in the formation of an automated biometric data scanning systems and realize the biometric security the concept of the e-border in Lithuania, creating e-government in a national network of public administration control mechanism. The EU has been dealt with e-government integrated e - border management and biometric security elements, accented the importance of the information society.

Details discussed in the integrated European border management strategy and advanced integrated border management: a national network of influence in border management, risk management. Particular attention was given to Lithuania's position in the Schengen area studied. More overview of the Schengen (acquis) legislation, information system and its purpose, "Eurodac" and the Visa Information System (VIS) analysis, also biometric passports and their problems in Lithuania.

In the master’s work discussed the integrated e-border management and practical implementation particularities to realization of biometric perimeter security systems of the EU and the countries of the world in practice. Effective border control to ensure analyzed a more detailed discussion of the draft e-border mission and role, providing perimeter security of biometric e-border control context. Pending biometric security e-government implementation of the Schengen area of installation problems e-government e-border service in Lithuania. Overview of e-government e - service administration aspects of the information society context, and made decisions on the biometric security of SIS e-government in the implementation of the Schengen area, the concept of the problem. The introduction of Lithuania e-border service performed State Border Guard Service border guards indirect assessment of the investigation and provided the biometric e-government e - border sales of Lithuania to offer solutions and recommendations.

Proposed solutions enable biometrics to automate the scanning process, the realization of biometric security Lithuania e-borders the concept of providing e-government in a national network of public administration efficiency.

.

1 PRIEDAS

APKLAUSOS ANKETA

Anketa

Anketos numeris

Anketos tikslas – ***ištirti kaip Jūs vertinate Lietuvos valstybės sienos apsaugos tarnybos (pasieniečių) pasirengimą ES išorės sienų apsaugai?***

Pildymo instrukcija: prašom įvertinti kaip Jūs sutinkate ar nesutinkate su kiekvienu teiginiu pažymėdami atitinkamą variantą.

	Visiškai sutinku	Greičiau sutinku	Greičiau nesutinku	Visiškai nesutinku	Nežino, neatsakė
1. VSAT užtikrina tinkamą sienos su Baltarusija apsaugą					
2. Pasienio kontrolės punktai prie sienos su Baltarusija yra tinkamai įrengti					
3. VSAT efektyviai stabdo nelegalią migraciją per sieną su Baltarusija					
4. Lietuvos pasieniečiai turi pakankamai techninių priemonių efektyviam darbui (automobilių, sraigtasparnių, laivų, ryšio ir stebėjimo priemonių)					
5. VSAT efektyviai stabdo kontrabandą per sieną su Baltarusija					

2 PRIEDAS

ANKETINĖS APKLAUSOS VERTINIMO SANTYKIS

	Sutinka (%)	Nesutinka (%)	Vertinimų santykis
1. VSAT užtikrina tinkamą sienos su Baltarusija apsaugą	56	21	+ 35
2. Pasienio kontrolės punktai prie sienos su Baltarusija yra tinkamai įrengti	49	17	+ 32
3. Lietuvos pasieniečiai turi pakankamai techninių priemonių efektyviam darbui (automobilių, sraigtasparnių, laivų, ryšio ir stebėjimo priemonių)	44	26	+ 18
4. VSAT efektyviai stabdo nelegalią migraciją per sieną su Baltarusija	45	28	+ 17
5. VSAT efektyviai stabdo kontrabandą per sieną su Baltarusija	43	33	+ 10