Mykolo Romerio universitetas
Viešojo administravimo fakultetas
Informatikos ir statistikos katedra

MARTYNAS DAMKUS
Elektroninės valdžios administravimas

Informacijos saugumas elektroninės valdžios infrastruktūros kūrime

Magistro baigiamasis darbas

Vadovas:
Profesorius, daktaras
Rimantas Petrauskas

Vilnius, 2006

TURINYS

ĮVADAS

2006 gegužės 31 dieną Europos Komisija priėmė saugios informacinės visuomenės strategijos komunikatą „Dialogas, partnerystė ir teisių suteikimas“[1] [20], kurio pagrindinis tikslas – atgaivinti 2001 metų Europos Komisijos saugumo strategiją, pateiktą komunikate „Tinklų ir informacijos saugumas. Pasiūlymas dėl Europos politikos požiūrio“[2] [26]. Tai dar kartą pabrėžė Europos Sąjungos požiūrį ir teikiamus prioritetus informacijos saugai.

2006 vasario 13 dieną Europos Komisija paskelbė komunikatą „Tarpusavio sąveika pan-Europinėms e.valdžios paslaugoms“[3] [22, 2], kurio pagrindinis tikslas yra atkreipti šalių-narių dėmesį į elektroninės valdžios paslaugų *tarpusavio sąveikos* (angl. *Interoperability*), pan-Europiniu lygmeniu, skatinimą.

Šiuo dokumentu pabrėžiamas elektroninės valdžios, kaip kertinio akmens, vaidmuo skatinant Europos ekonomikos konkurencingumą ir inovacijas: siūloma vystyti tarpvalstybines elektronines paslaugas, kurios padidintų tarpusavio sąveikos laipsnį. Tokio tikslo pasiekimas neįmanomas be glaudaus šalių-narių administracijų bendradarbiavimo paremto informacinėmis technologijomis. Naujajame komunikate pabrėžiama, jog moderni viešojo administravimo sistema gali būti sukurta tik pažangios, bei patikimos informacinių ir komunikacinių technologijų infrastruktūros, o taip pat aiškių elektroninės valdžios procesų pagrindu.

2005 metų eEuropos veiksmų plane[4] [24, 3] elektroninės valdžios paslaugų pan-Europinė sąveika buvo įvardinama kaip pirminė jų teikimo sąlyga. eEuropos veiksmų planas remiasi dviejų tipų veiksmų grupėmis: viena iš jų apima paslaugas, jų taikymą ir turinį, o kita – plačiajuostę infrastruktūrą ir saugumo klausimus. Vienas iš svarbiausių veiksmų plano tikslų, kuris įtakoja ir kitų tikslų pasiekimą – saugios informacinės infrastruktūros sukūrimas.

Informacinės infrastruktūros patikimumas ir saugumas – viena svarbiausių elektroninės valdžios paslaugų teikimo sąlygų. Turimos ar perduodamos informacijos saugumo klausimų

[1] Communication from the Commission to the Council and the European Parliament. Dialogue, partnership and empowerment: A Strategy for a Secure Information Society. 2006-05-31 // http://europa.eu.int/information_society/newsroom/cf/itemlongdetail.cfm?item_id=2766; prisijungimo laikas: 2006-02-15

[2] Communication from the Commission to the Council and the European Parliament. Network and Information Security: Proposal for A European Policy Approach. 2001 // http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52001DC0298:EN:HTML; prisijungimo laikas: 2006-02-15

[3] Communication from the Commission to the Council and the European Parliament. Interoperability for Pan-European eGovernment Services. 2006-02-13 // http://ec.europa.eu/idabc/servlets/Doc?id=24117; prisijungimo laikas: 2006-02-15

[4] Communication from the Commission to the Council and the European Parliament. eEurope 2005: An information society for all. 2002-05-28 // http://europa.eu.int/information_society/eeurope/2005/all_about/action_plan/index_en.htm; prisijungimo laikas: 2006-05-05

sprendimas reikalauja daug lėšų ir laiko sąnaudų: proceso eigoje buvo kuriami saugios infrastruktūros projektai, juos reglamentuojantys dokumentai.

Pirmoji, tarpusavio sąveiką ir pan-Europinio lygmens elektroninės valdžios paslaugas skatinanti, iniciatyva buvo IDA (Interchange of Data between Administrations) programa, kuri pasiūlė bendrąsias pan-Europinių elektroninių paslaugų teikimo gaires. Prie šios programos kuriamų saugumo projektų ketinama prijungti ir Lietuvos viešųjų struktūrų sistemas.

Darbo tikslas – ištirti ir užtikrinti informacijos saugumą elektroninės valdžios infrastruktūroje, teorinį ir praktinį saugios sistemos pagrindimą.

Darbo uždaviniai:

1. Išanalizuoti elektroninės valdžios ir informacijos saugumo reglamentavimą.
2. Išnagrinėti svarbiausius Europos Sąjungos ir Lietuvos Respublikos teisinius dokumentus, reglamentuojančius informacijos saugą.
3. Ištirti saugios informacijos perdavimo infrastruktūros kūrimą.
4. Atlikti informacijos saugos Lietuvos elektroninės valdžios infrastruktūroje tyrimą.

Darbo objektas:

Techninės, organizacinės ir teisinės informacijos saugumo priemonės kuriamoje e.valdžios infrastruktūroje.

Darbo metodika:

Elektroninės valdžios infrastruktūros ir informacijos saugumo reikšmingumo joje įvertinimas, teisinis saugumo reglamentavimas.

Analizuojant informacijos saugumo sistemos kūrimą teoriniu lygmeniu atsižvelgiama į rizikos analizės svarbą, visa apimančios saugumo politikos vystymą.

Iškeltam darbo tikslui pasiekti atliekamas kokybinis tyrimas. Jo metu tiriamas informacijos saugos reglamentavimas ir taikymas viešojo administravimo įstaigose.

Atlikus darbą pateikiamos konkrečios praktinės išvados ir rekomendacijos, kurios apibendrina ir įvardina darbo ir tyrimo metu pastebėtus trūkumus, siūlo galimus situacijos gerinimo variantus.

Darbo sandara:

Darbas sudarytas iš įvado, trijų dėstymo dalių ir išvadų.

Įvade aptariama darbo tema, jos aktualumas, numatomas darbo tikslas ir jo uždaviniai, trumpai aptariama darbo atlikimo metodika ir jo sandara.

Pirmojoje dalyje nagrinėjama elektroninės valdžios sąvoka, ir informacijos saugumo užtikrinimas Lietuvos elektroninės valdžios infrastruktūroje, atliekama svarbiausių Europos Sąjungos teisinių dokumentų, reglamentuojančių informacijos ir tinklų saugumą, o taip pat ir elektroninės valdžios įgyvendinimą, analizė, detaliai išnagrinėjamas IDA - TESTA informacijos saugumo projektas Europos ir Lietuvos lygmenimis.

Antrojoje dalyje analizuojama ir apibendrinama informacijos saugumo teorija. Pateikiami saugumo politikos vystymo principai, nagrinėjami organizaciniai ir technologiniai informacijos saugos aspektai. Aprašomas informacijos saugos ir rizikos vertinimas, kylančios grėsmės ir galima žala, informacijos saugos sistemos kūrimas.

Trečioji dalis – susideda iš trijų poskyrių, kuriuose pateikiama statistinės informacijos e.valdžios ir saugumo temomis analizė; analizuojami svarbiausi informacijos saugos aspektus Lietuvoje reglamentuojantys teisiniai aktai; aprašomas atliktas viešojo administravimo įstaigų informacijos saugumo ir jo reglamentavimo tyrimas, tarpusavio palyginimas.

Paskutinė dalis susideda iš išvadų ir rekomendacijų. Pateikiamos baigiamosios darbo išvados, apibendrinančios tiriamojo darbo ir kokybinio tyrimo rezultatus. Remiantis išvadomis pateikiamos dalykinės rekomendacijos.

Darbo pabaigoje patiekiamas naudotos literatūros bibliografinis sąrašas, santraukos lietuvių ir anglų kalbomis.

1. ELEKTRONINĖ VALDŽIA IR SAUGUMO REGLAMENTAVIMAS

Informacinių ir komunikacinių technologijų plėtra ir diegimas, integracija įvairiose gyvenimo srityse, o taip pat ir pastovus vartotojų rato didėjimas leidžia valstybei išnaudoti vis parankiau besiklostančią situaciją elektroninės valdžios idėjos įgyvendinimui.

Elektroninė valdžia tai ne tik informacija valdžios institutų portaluose, tačiau taip pat ir galimybė greitai ir efektyviai, maksimaliai sumažinant laiko ir pinigines sąnaudas pasinaudoti viešosiomis paslaugomis, įtakoti valstybėje daromus sprendimus, dalyvauti demokratiniuose valstybės valdymo procesuose, interaktyviai spręsti jiems kylančias problemas.

Be abejonės – svarbiausias tokios IKT paremtos sistemos reikalavimas – naudojamos informacijos saugumas. Tik patikima ir saugi sistema gali sėkmingai veikti, teikti paslaugas ir siekti užsibrėžtų tikslų.

1.1 E.valdžios sąvoka ir saugumas

2003 metais Europos Komisijos paskelbtame komunikate elektroninė valdžia (*electronic government*) apibrėžiama kaip „informacinių ir komunikacinių technologijų panaudojimas viešajame administravime apjungiant jas su organizaciniais pokyčiais bei naujais įgūdžiais siekiant patobulinti viešąsias paslaugas ir demokratinius procesus, o taip pat sustiprinti viešųjų politikų paramą“[5] [23, 7].

Elektroninė valdžia sudaro galimybę patogiai ir efektyviai naudotis viešosiomis elektroninėmis paslaugomis, sumažinti laiko ir finansines sąnaudas. Sėkmingo valdymo ir elektroninės demokratijos siekianti elektroninės valdžios sistema siekia[6] [18]:

- Tobulesnių valdžios institucijų sprendimų,
- Didesnio piliečių pasitikėjimo valdžios institucijomis,
- Geresnio valdžios atskaitingumo ir skaidresnio valdymo,
- Sudaryti galimybę įgyvendinti piliečių valią,

[5] Communication from the Commission to the Council and the European Parliament. The Role of eGovernment for Europe's Future. 2003-09-26. // http://europa.eu.int/information_society/eeurope/2005/doc/all_about/egov_communication_en.pdf; prisijungimo laikas: 2006-06-08

[6] Clift S. E-Democracy, E-Governance and Public Net-Work. 2003 September // http://www.publicus.net/articles/edempublicnetwork.html; prisijungimo laikas: 2006-06-08

- Įtraukti piliečius, verslo atstovus, nevyriausybines organizacijas ir kitas interesų grupes į visuomenei svarbių iššūkių priėmimą ir sprendimų ieškojimą.

Norint įvykdyti pagrindinius elektroninės valdžios sistemos siekius, jos kūrime galima išskirti keturis centrinius aspektus[7] [32, 17]:

- Piliečių poreikių supratimas.
- Bendra visai valdžiai integruota politika ir strategija.
- Aktyvus modernių paslaugų teikimas.
- Paprasto priėjimo prie paslaugų vietiniu ir centriniu lygmenimis sukūrimas.

Išskiriamos trys paslaugų teikimo ir bendravimo kryptys[8] [18]: G2C (*government to citizen*) – valdžia piliečiams, G2B (*government to business*) – valdžia verslui ir G2G (*government to government*) – valdžia valdžioms institucijoms. Fiziniai ir juridiniai asmenys yra potencialūs „išoriniai“ šių paslaugų vartotojai. Tuo tarpu kitos valdžios institucijos yra „vidiniai“ vartotojai.

2002 metais Seimo priimtoje elektroninės valdžios koncepcijoje minimos 20 viešųjų paslaugų (12 skirtų gyventojams ir 8 verslo subjektams)[9] [16].

Šių viešųjų paslaugų teikimas skirstomas brandos lygmenimis, kurie nurodo tokios viešosios paslaugos galimybes ir jos veikimo principą. Kai kurios paslaugos negali pasiekti aukščiausio jos teikimo lygmens dėl savo specifikos.

Informacinės visuomenės plėtros komitetas prie Lietuvos Respublikos Vyriausybės skiria keturis viešųjų paslaugų teikimo Internetu brandos lygmenis[10] [33]:

- Pirmasis lygis – informacinio pobūdžio viešosios paslaugos. Institucija pateikia viešąją informaciją Internetu.
- Antrasis lygis – vienkryptis interaktyvumas. Institucija pateikia vartotojui savo tinklalapiuose iš dalies automatizuotas formas ir anketas, kurias užpildęs ir išspausdinęs vartotojas gali jomis naudotis (pvz.: pateikti institucijai duomenis).
- Trečiasis lygis – dviejų krypčių interaktyvumas. Vartotojo tapatybė nustatoma sistemoje. Jis gali pateikti paklausimus, ir institucija elektroninio paklausimo

[7] eGovernemnt, more that as automation of government services. 2003 October // www.isc.ie/downloads/egovernment.pdf; prisijungimo laikas: 2006-06-08
[8] Clift S. E-Democracy, E-Governance and Public Net-Work. 2003 September // http://www.publicus.net/articles/edempublicnetwork.html; prisijungimo laikas: 2006-06-08
[9] Lietuvos Respublikos Seimo nutarimas „Dėl Elektroninės valdžios koncepcijos patvirtinimo“. 2002-12-31 Nr. 2115 // http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=198184; prisijungimo laikas: 2006-10-12
[10] Elektroninės viešosios paslaugos Lietuvoje. IVPK prie LR Vyriausybės. 2002-08-01 // http://www.ivpk.lt/main-aktual.php?cat=61&n=11; prisijungimo laikas: 2006-06-12

pagrindu atsako į šį paklausimą. Tačiau viešoji paslauga (pvz.: pažyma) pristatoma neelektronine forma.

- Ketvirtasis lygis – transakcijos. Baigtas e. valdžios projektas. Vartotojas elektroniniais kanalais paduoda užklausą ir gauna galiojančią elektroninę viešąją paslaugą (įgalinamas apmokėjimas).

Atsižvelgiant į atitinkamą elektroninės paslaugos brandos lygį nustatomas ir informacijos saugumo lygmuo, kuris turi būti patenkintas, kad paslauga galėtų būti tinkamai ir patikimai teikiama. (1 Lentelė).

Saugumo lygmenys nustatomi pagal informacijos, kuria operuojama paslaugų teikimo metu, svarbą[11] [34, 105]:

Pirmas saugumo lygmuo – skirtas paslaugą teikiančioms institucijoms skirtai informacijai saugoti, bei informacijai kurios atskleidimas turėtų neigiamos įtakos paslaugos gavėjui ar jos teikėjui; taip pat ir asmens duomenys.

Antras saugumo lygmuo – taikomas visiems asmens duomenims, naudojamiems paslaugas teikiančių institucijų, o taip pat duomenims, kurių neautorizuotas atskleidimas turėtų neigiamos įtakos paslaugos gavėjams.

Trečias saugumo lygmuo taikomas tokiai informacijai, kurios neautorizuotas keitimas ar naikinimas turėtų neigiamos įtakos teikiamų paslaugų kokybei.

1 Lentelė. Informacijos saugumo lygmenų klasifikacija

	1 lygmuo	2 lygmuo	3 lygmuo
Duomenų šifravimas	X	X	
Serverio identifikavimas	X	X	
Vartotojo identifikavimas slaptažodžiu	X	X	
Vartotojo identifikavimas sertifikatu	X		
Duomenų bazės vientisumo užtikrinimas	X	X	X
Atsarginės kopijos	X	X	X
Ugniasienės	X	X	X
Organizacinės saugumo priemonės	X	X	X

Elektroninės paslaugos, kurioms pakanka trečio saugumo lygmens yra tos, kurioms priskiriamas pirmas arba antras brandos lygmuo (informacijos pateikimas Internete arba vienakryptis interaktyvumas). Tokioms paslaugoms apsaugoti pakanka įprastinių organizacinių saugumo priemonių, ugniasienių saugančių nuo įsilaužimų ir duomenų bazės vientisumo užtikrinimo. Taip pat svarbu ir atsarginių kopijų padarymas apsisaugojimui nuo netikėtumų.

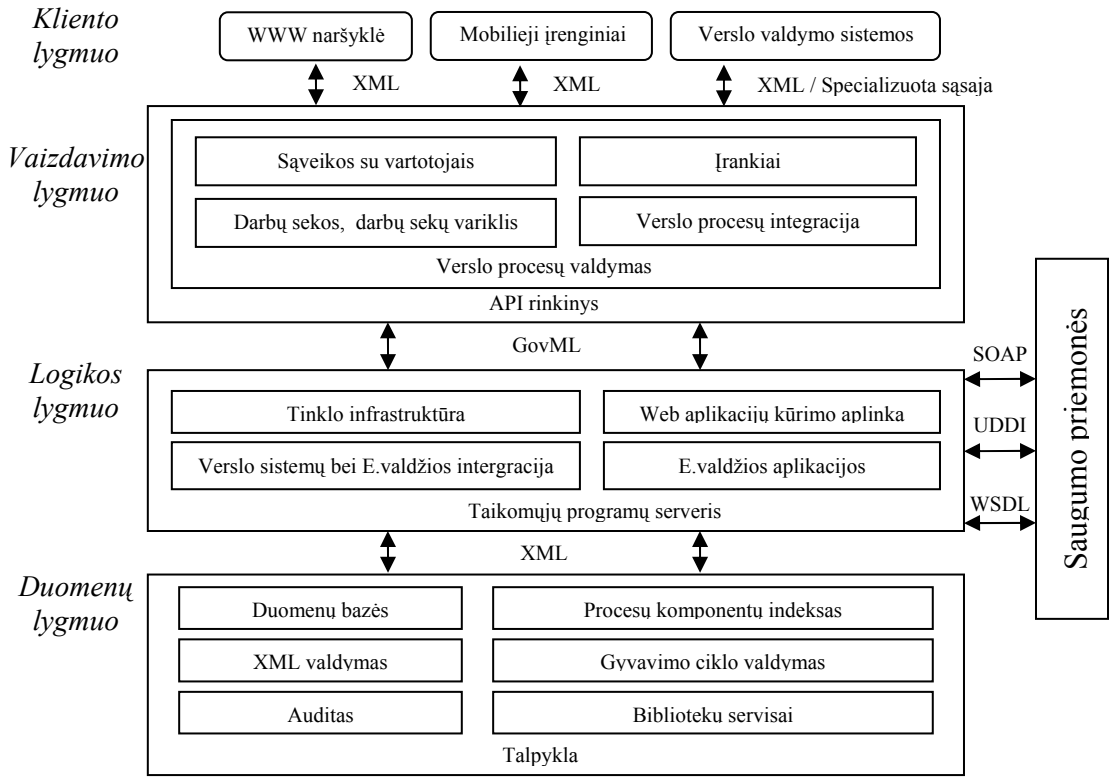
[11] Elektroninių viešųjų paslaugų siekiamo modelio aprašymas. IVPK prie LR Vyriausybės. // http://epp.ivpk.lt/epp/Dokumentai/IVPK_elmodelis_siekiamasV1.pdf; prisijungimo laikas: 2006-06-12

Trečiojo brandos lygio elektroninės paslaugos (dvipusis interaktyvumas) reikalauja antro informacijos saugumo lygmens užtikrinimo. Šioms paslaugoms apsaugoti reikia užtikrinti ne tik anksčiau minėtas priemones, tačiau taip pat pasirūpinti ir duomenų užšifravimu, serverio identifikavimu, bei vartotojo identifikavimu slaptažodžio pagalba.

Ketvirtojo brandos lygio elektroninės paslaugos (transakcijos) negali veikti neužtikrinus pirmojo informacijos saugumo lygmens. Šiuo atveju būtinas vartotojo identifikavimas skaitmeninio sertifikato pagalba.

Jei elektroninės valdžios sistemą vertinti grynai techniniu požiūriu, tai pagal šio darbo tematiką aktualus būtų tik jos loginis lygmuo, kuriame diegiamos visos saugumo priemonės (1 Schema). Jų pagalba gali būti apsaugomi elektroninės valdžios procesai, bei juose naudojama informacija.

1 Schema. Elektroninės valdžios techninis įgyvendinimas[12]



Loginis lygmuo gali būti vertinamas kaip svarbiausias keturių skiriamų lygmenų – jame realizuojamas duomenų gavimas iš duomenų lygmens, informacija transformuojama į suprantamą vaizdavimo ar kliento lygmeniui formatą, perduodama jiems. Tai yra procesų veikimo ir pačios sistemos esmės architektūrinis lygmuo. Jis ne tik leidžia apibrėžti tinklo infrastruktūrą, tačiau taip pat integruoja verslo sistemų, bei teikiamų e.valdžios paslaugų

[12] Elektroninių viešųjų paslaugų siekiamo modelio aprašymas. IVPK prie LR Vyriausybės. // http://epp.ivpk.lt/epp/Dokumentai/IVPK_elmodelis_siekiamasV1.pdf; prisijungimo laikas: 2006-06-12

taikomąsias programas. Tačiau viena iš pačių svarbiausių šio lygmens funkcijų – sistemos saugumo užtikrinimas.

E.valdžios sistemoje naudojami komunikaciniai protokolai:

WSDL (*Web Service Description Language*) – paslaugas apibrėžiantis protokolas XML pagrindu. Tiekiamos paslaugos tampa suprantamomis kitoms programoms.

UDDI (*Universal Description, Discovery and Integration*) – XML paremtas protokolas Internetu teikiamų paslaugų skelbimui, struktūrizavimui, kategorizavimui ir valdymui.

GovML (*Government Markup Language*) – XML protokolas aprašo paslaugas apibūdinančius duomenis.

SOAP (*Simple Object Access Protocol*) – XML paremtas protokolas naudojamas siųsti pranešimams tarp programų.

HTTPS (*Secure Hyper Text Transfer Language*) – naudojamas paslaugoms Internetu teikti, juo koduojamos užklausos paslaugų serveriams, jų atsakymai.

1.2 E.valdžios saugumo reikalavimų reglamentavimas Europos Sąjungoje

1995 metais priimta Europos Parlamento ir Tarybos direktyva 95/46/EB[13] [30] dėl asmenų apsaugos, betvarkant jų asmeninius duomenis, bei tokių duomenų judėjimo. Joje pabrėžiama, jog turi būti užtikrinama techninė ir organizacinė sauga, kuri neleistų netinkamai panaudoti apdorojamų, saugomų ar perduodamos informacijos.

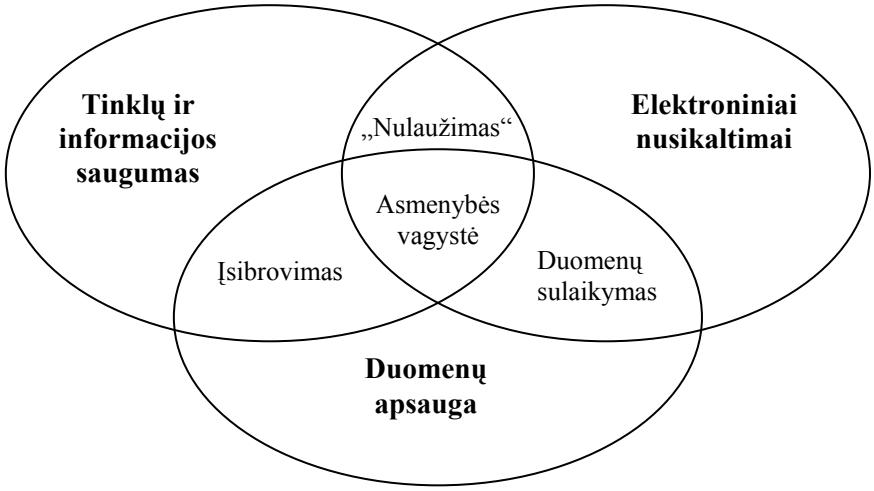
Šios direktyvos 17 straipsnyje pabrėžiama, jog: „Valstybės narės numato, kad duomenų valdytojas privalo įgyvendinti tinkamas technines ir organizacines priemones, skirtas apsaugoti, kad asmens duomenys nebūtų netyčia ar neteisėtai sunaikinti ar netyčia prarasti, pakeisti, neleistinai atskleisti ar palikti prieinami, ypač, kai tvarkomus duomenis tenka perduoti tinklu, taip pat apsaugoti nuo bet kokių kitų neteisėtų tvarkymo būdų. Atsižvelgus į technologijų lygį ir jų įdiegimo išlaidas, minėtos priemonės turi užtikrinti tokį saugumo lygį, kuris atitiktų tvarkymo keliamą riziką ir saugotinų duomenų pobūdį.“.

Taip pat numatoma, kad: „kai duomenys tvarkomi duomenų valdytojo vardu, jis privalo parinkti tokį kitą duomenų tvarkytoją, kuris garantuotų reikiamas techninio saugumo ir organizacines priemones, taikomas tvarkant numatytus duomenis, ir privalo užtikrinti, kad tokių priemonių būtų laikomasi.“.

[13] Direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. 1995-10-25 // http://www3.lrs.lt/pls/inter1/dokpaieska.showdoc_l?p_id=7879&p_query=&p_tr2=2; prisijungimo laikas: 2006-10-14

2001 metais priimtas „Tinklų ir informacijos saugumas: pasiūlymas dėl Europos politikos požiūrio“[14] [27]. Jame pripažįstama, jog saugumas tampa pagrindiniu faktoriumi ekonominiame ir socialiniame vystymesi. Šiuo dokumentu skatinamas visuotinės informacijos saugumo politikos vystymas. Taip pat tvirtinama, jog tinklų ir informacijos saugumo politika turi apimti egzistuojančias telekomunikacijų, duomenų apsaugos ir elektroninių nusikaltimų politikas. Dokumente vaizduojamas šių sričių tarpusavio ryšys (2 Schema).

2 Schema. Trijų politikos laukų persidengimas



Šiame pasiūlyme taip pat grupuojami ir saugumo incidentai: informacijos perėmimas ir modifikavimas, neteisėta prieiga, kenksmingo kodo atakos, klaidinimas, nenumatyti natūralūs įvykiai.

Pateikiamos ir saugumo priemonės: sąmoningumo skatinimas, CERT grupių (Computer Emergency Response Team) sustiprinimas, standartizavimo ir sertifikavimo palaikymas, valdomojo lygmens saugumas, tarptautinė kooperacija.

Toliau siekiant Europos Sąjungos užsibrėžtų tinklų, Europos Komisijos ir Europos Tarybos komunikatu 2001 metais buvo priimtas veiksmų planas „eEurope2005: informacinė visuomenė visiems“[15] [25]. Šis veiksmų planas yra tęstinė Europos saugumo strategijos,

[14]Communication from the Commission to the Council and the European Parliament. Network and information security: proposal for a European policy approach. Executive summary. 2001// http://europa.eu.int/information_society/eeurope/2002/news_library/pdf_files/execsum_en.pdf; prisijungimo laikas: 2006-10-04

[15]Communication from the Commission to the Council and the European Parliament. eEurope 2005: An information society for all. Executive summary 2002-05-28 // http://europa.eu.int/information_society/eeurope/2002/news_library/documents/eeurope2005/eeurope2005_en.pdf; prisijungimo laikas: 2006-05-05

apimančios anksčiau minėtą 2001 metų pasiūlymą[16] [27], Europos Tarybos rezoliuciją dėl tinklų ir informacijos saugumo[17] [28] ir 2001 metų Saugesnės informacinės visuomenės komunikatą[18] [20], dalis.

Pagrindiniai plano pasiūlymai kuriant saugia informacinę infrastruktūrą yra: kibernetinio saugumo reagavimo grupių sukūrimas (Cyber Security Task Force), „saugumo kultūros“, didinančios visuomenės sąmoningumą, diegimas ir saugios komunikacijos tarp viešų serverių kūrimas (keitimuisi valstybine informacija). Taip pat numatomi tolimesni saugumo tyrimai šeštojoje „framework“ programoje. Prioritetai suteikiami: patikimo tinklo ir informacinės infrastruktūros, linkusios į kylančias technologijas, kūrimui, pažeidžiamumų identifikavimui ir infrastruktūrų tarpusavio priklausomybėms. Taip pat ypatingai pabrėžiamas standartizavimo ir „žmogiškojo faktoriaus“ saugumo sistemoje svarba.

2002 metais priimta Europos Parlamento ir Tarybos direktyva 2002/58/EB[19] [31] dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje. Tokiu būdu buvo pakeista 97/66/EB direktyva, kuri taikė 95/46/EB direktyvos principus konkrečiose telekomunikacijų sektoriaus taisyklėse, tačiau jos specifika nebeapėmė visų, nepriklausomai nuo technologijos, paslaugų.

Šioje direktyvoje išskirtinai daug dėmesio skiriama informacijos saugai: „Paslaugų teikėjai, siūlantys viešai prieinamų elektroninių ryšių paslaugas Internetu, turėtų informuoti naudotojus ir abonentus apie tai, kokias priemones jie galėtų taikyti savo pranešimams apsaugoti, pavyzdžiui, specialią programinę įrangą ar šifravimo technologijas. Reikalavimas pranešti abonentams apie konkrečią riziką saugumui neatleidžia paslaugų teikėjo nuo įsipareigojimo savo lėšomis imtis tinkamų ir skubių priemonių pašalinti bet kokią naują, nenumatytą saugumo riziką ir atkurti normalų paslaugos saugumo lygį.“.

Direktyva taip pat reglamentuoja „šnipukų“ ir slaptų numerio nustatymo įtaisų, leidžiančių „be naudotojų žinios įsiskverbti į jų galinius įrenginius siekiant susipažinti su informaciją, saugoti slepiamą informaciją ar sekti naudotojo veiksmus“ naudojimą tik naudotojui apie tai pranešus, ir tik teisėtais tikslais.

---

[16]Communication from the Commission to the Council and the European Parliament. Network and information security: proposal for a European policy approach. Executive summary. 2001// http://europa.eu.int/information_society/eeurope/2002/news_library/pdf_files/execsum_en.pdf; prisijungimo laikas: 2006-10-04

[17]Council resolution on a common approach and specific actions in the area of network and information security. 2001-12-11 // http://register.consilium.eu.int/pdf/en/01/st15/15152en1.pdf; prisijungimo laikas: 2006-09-25

[18] Communication from the Commission to the Council and the European Parliament. Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime. 2001-01-26 // http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeCommEN.html; prisijungimo laikas: 2006-09-25

[19] Direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje. 2002-07-12 // http://www3.lrs.lt/pls/inter1/dokpaieska.showdoc_l?p_id=36605; prisijungimo laikas: 2006-09-25

Direktyvoje 4 straipsnyje išskiriama: „Viešai prieinamų elektroninių ryšių paslaugų teikėjas turi imtis tinkamų techninių ir organizacinių priemonių,, kad užtikrintų savo paslaugų saugumą, o tam tikrais atvejais tokių priemonių imasi kartu su viešųjų ryšių tinklo teikėju, kad užtikrintų ir paties tinklo saugumą. Atsižvelgiant į naujausius technikos laimėjimus bei jų įdiegimo kainą, šios priemonės užtikrina saugumo lygį, atitinkantį atsiradusiai rizikai“. Dokumentas taip pat įpareigoja „Iškilus tam tikrai tinklo saugumo pažeidimo rizikai, viešai prieinamų elektroninių ryšių paslaugų teikėjas turi informuoti abonentus apie šią riziką, o tais atvejais, kai paslaugos teikėjo taikomos priemonės neapima šios rizikos – informuoti abonentus apie visas įmanomas teisės gynimo priemones, nurodant ir galimas jų kainas“.

2003 metais Erkki Liikanen, informacinės visuomenės ir verslo Europos komisaras, pranešė apie ENISA (European Network and Information Security Agency) sukūrimą[20] [36]. Šios Europos tinklų ir informacijos saugumo agentūros užduotis – kibernetinio saugumo Europos Sąjungoje skatinimas. Ji veikia kaip patariamasis organas šalims-narėms ir ES institucijoms tinklų ir informacijos saugumo klausimais. Agentūra taip pat padės užtikrinti informacijos saugumo funkcijų tarpusavio sąveiką valstybiniuose ir pramoniniuose tinkluose, o taip pat ir informacinėse sistemose.

2004 metais agentūra pradėjo savo darbą. Jai buvo suformuluoti aiškūs uždaviniai[21] [35]:

- Patarti šalims-narėms ir Europos Komisijai saugumo klausimais, bei padėti koordinuoti veiklą, užtikrinančią aukštą tinklų ir informacijos saugumo lygį bendruomenėje.
- Padėti informuoti piliečius, verslo ir administracines struktūras apie pavojus susijusius su Interneto ir informacinių sistemų naudojimu, o taip pat pateikti informaciją apie tai, kaip galima apsisaugoti nuo šių grėsmių.
- Atlikti užduotis susijusias su rizikos įvertinimu ir jos valdymu, sekti tyrimų vystymą ir standartizavimo pastangas, glaudžiai bendradarbiaujant su pramone.

Erkki Liikanen, Europos komisaras verslo ir informacinės visuomenės reikalams, pareiškė, kad[22] [35]: „Pasitikėjimas ir saugumas yra kritiniai informacinės visuomenės komponentai, o įkūrus ENISA, mes tęsiame pradėtą darbą sukurti „saugumo kultūrą“, kurią mes numatėme eEurope2005 veiksmų plane.“.

2005 metų Europos Komisijos komunikate „i2010 – Europos informacinė visuomenė augimui ir užimtumui skatinti“ pabrėžiama, jog siekiant skaitmeninio suartėjimo, kuriant bendrą

[20] EU: Plans for a new EU cyber-security agency announced. 2003-02-11 // http://ec.europa.eu/idabc/en/document/863/355; prisijungimo laikas: 2006-09-25
[21] EU: Green light for the European e-security agency. 2003-11-21 // http://ec.europa.eu/idabc/en/document/1828/355; prisijungimo laikas: 2006-09-25
[22] EU: Green light for the European e-security agency. 2003-11-21 // http://ec.europa.eu/idabc/en/document/1828/355; prisijungimo laikas: 2006-09-25

Europos informacinę erdvę, vienas iš svarbiausių tikslų yra saugumas[23] [21, 6]: „saugesnio nuo apgavikų, žalingo turinio ir technologijų gedimo Interneto kūrimas, skatinant tarp investuotojų ir vartotojų pasitikėjimo augimą“. Informacinių sistemų ir tinklų saugumas tiesiogiai įtakoja skaitmeninių paslaugų prieinamumą ir vartotojų kiekį.

Komunikate Europos Komisija įsipareigoja per 2006 metus pasiūlyti strategiją, kuri skatins saugią informacinę visuomenę. Ji apims esamu saugumo priemonių atnaujinimą ir suderinimą, o taip pat savisaugos, nuolatinio budrumo ir staigaus atsako į pažeidimus ugdymą. Numatoma parama tiksliniams tyrimams, kuriais siekiama sukurti apsaugines priemones svarbiausių problemų sprendimui.

2006 vasario 13 dieną Europos Komisija paskelbė komunikatą „Pan-Europinių elektroninės valdžios paslaugų tarpusavio sąveika“[24] [22]. Šiame dokumente pabrėžiama, pabrėžiama, kad moderni viešojo administravimo sistema gali būti sukurta tik remiantis patikima informacinių ir komunikacinių technologijų infrastruktūra. Juo skatinama informacijos sklaida tarp administracijų, paremtos informacine infrastruktūra ir saugumo politika.

2006 gegužės 31 dieną Europos Komisija priėmė saugios informacinės visuomenės strategijos komunikatą „Dialogas, partnerystė ir teisių suteikimas“[25] [20]. Pagrindinis šio komunikato tikslas – atgaivinti anksčiau minėtą 2001 metų Europos Komisijos strategiją, pateiktą komunikate „Tinklų ir informacijos saugumas. Pasiūlymas dėl Europos politikos požiūrio“[26] [26]. Dokumente pateikiamos informacinei visuomenei kylančios grėsmės ir nustatomi veiksmai, kurių būtina imtis siekiant pagerinti tinklų ir informacijos saugumą, siekiama ir toliau plėtoti „saugumo kultūra“, o taip pat dialogo, partnerystės ir teisių suteikimo principais grįstą visuotinę Europos strategiją. Siekdama įveikti su saugumu susijusias problemas, Europos bendrija parengė trijų dalių modelį, kuris apima: konkrečias tinklų ir informacijos apsaugos priemones, elektroninių ryšių reguliavimo sistemą ir kovą su elektroniniais nusikaltimais.

Išanalizavus pagrindinius Europos Sąjungos dokumentus reglamentuojančius informacijos saugą, galima prielaida, jog vis didesnis dėmesys skiriamas visuotinės informacijos

[23]Communication from the Commission to the Council and the European Parliament. i2010 – Europos informacinė visuomenė augimui ir užimtumui skatinti. 2005-06-01 // http://europa.eu.int/information_society/eeurope/i2010/docs/communications/com_229_i2010_310505_fv_lt.doc; prisijungimo laikas: 2006-09-25

[24]Communication from the Commission to the Council and the European Parliament. Interoperability for Pan-European eGovernment Services. 2006-02-13 // http://ec.europa.eu/idabc/servlets/Doc?id=24117; prisijungimo laikas: 2006-02-15

[25]Communication from the Commission to the Council and the European Parliament. Dialogue, partnership and empowerment: A Strategy for a Secure Information Society. 2006-05-31 // http://europa.eu. int/information_society/newsroom/cf/itemlongdetail.cfm?item_id=2766; prisijungimo laikas: 2006-02-15

[26]Communication from the Commission to the Council and the European Parliament. Network and Information Security: Proposal for A European Policy Approach. 2001 // http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52001DC0298:EN:HTML; prisijungimo laikas: 2006-02-15

apsaugos politikai ir priemonėms. Informacijos saugumas – kertinis elektroninės valdžios ir teikiamų elektroninių paslaugų akmuo.

1.3 E.valdžios saugumo projektų kūrimas ir taikymas

1.3.1 IDA programa ir projektai Europai

IDA (Interchange of Data between Administrations) programa sukurta ir pradėta įgyvendinti 1995m. Pagrindinė IDA programos idėja – pakloti pamatus elektroninės valdžios paslaugų įgyvendinimui, kurių poreikis sparčiai auga tiek verslo atstovams, tiek ir Europos šalių gyventojams.

Antroji IDA programos fazė truko 1999 – 2004m. Šiuo metu buvo kuriami juridiniai pagrindai trečiosios fazės (skatinti ir palengvinti elektroninės valdžios paslaugų teikimą visoje Europoje) įgyvendinimui. 2006-2009m. prasidėjo trečioji IDA programos fazė, pavadinta IDABC (Interoperable Delivery of Pan-European eGovernment Services to Public Administrations, Bussinesses and Citizens). Šios fazės uždavinys – apimti e.valdžios paslaugomis visą Europą, tuo prisidedant prie prekių, paslaugų, piliečių ir kapitalo laisvo judėjimo[27] [38]. Šios fazės tinklo dalis vadinama s-TESTA (secure TESTA) įgalina perduoti informaciją pažymėtą žyma „konfidencialiai“.

Programos kūrėjų ir vykdytojų tikslas – tarpusavio suderinamumas tarp IT sistemų ir administracinių procesų Europos Sąjungos šalių ribose. Savaime suprantama, jog tai būtina sąlyga norint teikti tokias atsakomybės reikalaujančias paslaugas.

IDA programa vysto ir remia nemažą skaičių perspektyvių projektų, kurių įgyvendinimas stipriai įtakotų Europos šalių atstovų gyvenimą[28] [39]: mokymosi portalas PLOTEUS, įdarbinimo paslaugos EURES, techninių nuostatų informacijos sistema TRIS, branduolinių medžiagų apskaitos sistema eSAFEGUARDS ir t.t. Be abejo, visi šie projektai verti dėmesio, bet nėra tiesiogiai susiję su šio darbo tematika (nors jiems taip pat aktualu informacijos apsauga, tačiau tai nėra tiesioginės projektų veiklos sritys). Analizuojami susiję IDA programos projektai:

- BRIDGE CA (Gateway Certification Authority)
- PKI (Public Key Infrastructure)
- SECURITY STUDIES

[27] IDA programa. Duomenų mainai tarp Europos Sąjungos administracijų // http://www.svdpt.gov.lt/idabc.php; prisijungimo laikas: 2006-06-05

[28] IDA. From Interchange of data between administrations to Pan-European eGovernment Services: the way forward. 2003 // http://www.is.lt/is/ida/The_way_forward.pdf; prisijungimo laikas: 2006-06-05

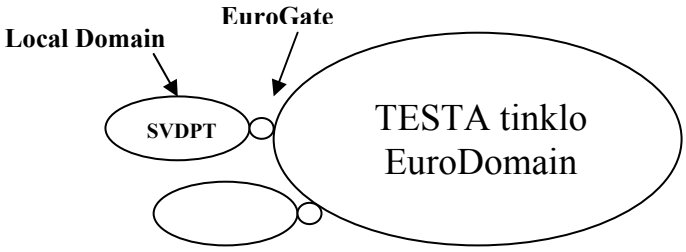
- TESTA (Trans European Services for Telematics between Administrations)

1.3.1.1 TESTA projektas

TESTA (Trans European Services for Telematics between Administrations) – Europos telematikos paslaugos administracijoms. Projektas sukurtas susidūrus dviems interesams – griežtiems informacijos saugumo reikalavimams ir efektyvios komunikacijos poreikiui. Nusprendžiama įgyvendinti projektą, kurio dėka būtų sukurtas uždaras ir atskirtas nuo išorinio Interneto priėjimo Europos bendrijos tinklas. Tai tokia tarpusavio bendravimo terpė, kuri patenkina informacijos pasikeitimo tarp administracijų saugumo reikalavimus.

Tinklas veikia IP protokolo pagrindu. Jį sudaro pagrindinis „stuburinis“ tinklas (EuroDomain) ir vietiniai (regioniniai) tinklai (LocalDomain). Pagrindinį ir vietinius tinklus sujungia „*EuroGate*“ darinys: tai vietinis ES narės komunikacijos centras, per kurį *LocalDomain* tinklai gali prisijungti prie *EuroDomain*. Jis veikia kaip pagrindinis komunikacijos tarp vietinių tinklų kūrėjas. (3 Schema) TESTA tinklo dalis, už kurią atsako Europos Komisija vadinama kamienine dalimi (EuroDomain); tai visą Europą apimanti informacijos apdorojimo ir perdavimo integruotų paslaugų (telematikos) visuma. ES šalys narės pačios atsako už savo lokalių domenų (nacionalinių tinklų) saugumą – šiuo atveju tai būtų SVDPT. Jis gali būti vadinamas nacionaliniu domenu, o valstybinės institucijos tinklas – institucijos domenu. Kiekvienoje valstybinėje institucijoje turi būti SVDPT vartai (analogiškai EuroGate TESTA tinkle). Pagrindinis visų vartų elementas – aparatūrinis informacijos šifravimo įrenginys (Hardware Encription Device), kuris koduoja visą perduodamą informaciją.

3 Schema. TESTA tinklo modelis.[29]



Dėl tokios komplikuotos sandaros (tinklų tinklas), TESTA tinklo saugumas – keleto lygmenų: pagrindinio tinklo, lokalaus tinklo ir vartotojo. Naudojamasi IDA projekto PKI (Public

[29] TESTA – A catalogue of services. Version 1.24. 2001.04.11 // http://www.is.lt/is/ida/TESTA_catalogue_of_services.doc; prisijungimo laikas: 2006-06-05

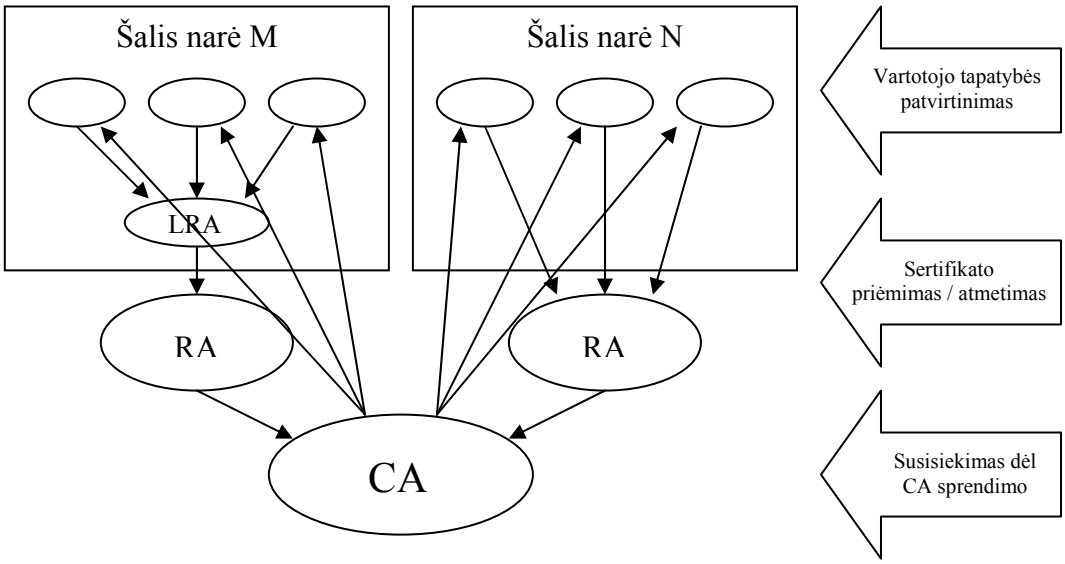
Key Infrastructure) suteikiamomis galimybėmis. Norint pasinaudoti PKI, reglamentuojamos (Certificate Practice Statement – CPS – leidimo suteikimo tvarkos aprašymas) registracijos institucijos (RA – registration authority), iki kurių identifikuoti galutinį vartotoją gali ir vietinės registracijos institucijos (LRA – local registration authority). Per šias institucijas vartotojas kreipiasi į sertifikato išdavimo instituciją (CA – certification authority). Procesas užtikrina maksimalų vartotojo identifikavimą ir tapatybės patvirtinimą (4 Schema).

Duomenų autentiškumas ir komunikacijos procesų saugojimui naudojami koduoti raktai. Vienas raktų poros vienetas priskiriamas galutiniam vartotojui, o kitas - tarnybinei stočiai. Kreipdamasis į sistemą vartotojas turi turėti raktų porą, taip pat ir sertifikatą. Leidimų suteikimo tvarkos aprašyme (CPS) numatomos tokios procedūros:

- Vartotojas programine įranga sukuria raktų porą ir sertifikatą. Kreipiasi su prašymu į RA (registration Authority) - registracijos instituciją.
- RA tikrina besikreipiančiojo tapatybę ir kuria teisinį pagrindą sertifikatui gauti.
- Vietinė registracijos institucija (LRA – local registration authority) patvirtina besikreipiančiojo teisę gauti pažymėjimą.
- Registracijos institucija (RA – registration authority) priima / atmeta prašymą. Jei patvirtina – registruoja atestuojančios institucijos (CA – certificate authority) duomenų bazėje.
- Patvirtinus kreipimąsi, atestuojanti institucija (CA) sukuria viešą naudotojo sertifikatą ir praneša vartotojui, kaip gauti sertifikatą. Pvz.: parsisiunčiama iš tarnybinės stoties ir išsaugoma asmeninio rakto pagalba. Tokiu būdu įgalinama siųsti koduotus pranešimus.

Dėl išorinės izoliacijos, ribojama prieiga prie resursų, o tai papildomai įtakoja informacijos saugumą. Saugumas taip pat sutvirtinamas IPSEC technologija saugančia nuo slaptų prisijungimų. Daug įtakos saugumui turi ir perdavimo kanalo saugumas – dėl to naudojamas optinio pluošto kabelis. Šio projekto dalyviai naudodamiesi TESTA tinklo privalumais tuo pačiu nepraranda savo autonomiškumo. Nuolatinis TESTA tinklo saugumo stiprinimas kuria tokią komunikacinę infrastruktūra, kuri turėtų patenkinti Europos Sąjungos nustatytą „Riboto naudojimo“ informacijos apsaugos lygį. Šis žingsnis dar labiau pastūmėjo projektą tikslo, kurti efektyvesnę ir patikimesnę komunikaciją, link. Numatoma TESTA tinklo modifikacija, kuri visiškai užtikrins E2E (galutinių vartotojų) saugą.

4 Schema. Sertifikatų – leidimų gavimo procesas.[30]



1.3.1.2 PKI projektas

PKI (Public Key Infrastructure) – viešųjų raktų infrastruktūra. Šis IDA projektas kartu su CA (Certification authority – atestuojančia institucija) per TESTA tinklo projektą padeda įgyvendinti dar 45 IDA programos remiamus projektus. PKI per CA užtikrina saugų duomenų judėjimą tarp galutinių vartotojų ES šalyse. Tai atliekama išduodant elektroninius pažymėjimus, kurie garantuoja abipusį pripažinimą. Šis projektas inicijuotas siekiant padidinti saugumą keičiantis informacija ir elektroninėmis laikmenomis.

1.3.1.3 BRIDGE CA projektas

BRIDGE CA (Gateway Certification Authority) – tinklų sąsajų sertifikavimo institucija. Tai IDA programos projektas, kuriuo siekiama padidinti informacijos saugumo laipsnį. Jos pagrindinis tikslas – užtikrinti tinkamą sertifikatų išdavimą ir jungiamosios grandies (tilto) tarp administracinių padalinių kūrimas. Taip pat siekiama sukurti tokią sistemą, kuri veiktų pasikliaujant CTL (certificate trust list – patikimų sertifikatų sąrašu). Jame būtų numatoma kompetentingos vietinės sertifikatų išdavimo institucijos, o taip pat kuriama bendros savisaugos struktūra.

[30] TESTA – A catalogue of services. Version 1.24. 2001.04.11 // http://www.is.lt/is/ida/TESTA_catalogue_of_services.doc; prisijungimo laikas: 2006-06-05

1.3.1.4 SECURITY STUDIES projektas

Saugumo Tyrimai – IDA programos projektas, skirtas informacijos apsaugos priemonių ir rekomendacijų tarp tinklų suderinimui, o taip pat gautų rezultatų panaudojimui kuriamoje sistemos infrastruktūroje.

1.3.2 Lietuvos prisijungimas prie TESTA

1.3.2.1 Valstybės institucijų kompiuterių tinklo sukūrimas

Ryšių ir informatikos ministerijos iniciatyva 1994 m. pradėtas kurti VIKT (Valstybės institucijų kompiuterių tinklas).

Pagrindinis VIKT projekto tikslas buvo sukurti tinkamą informacijos perdavimo sistemą, kuri atitiktų valstybės institucijų keliamus efektyvios komunikacijos ir saugumo reikalavimus. Paskelbtas konkursas VIKT projekto įgyvendinimui. Konkurse nugalėjo VĮ „Infostruktūra“.

Naujasis kompiuterių tinklas privalėjo aprėpti visą Lietuvą siekiant įgyvendinti užsibrėžtus tikslus: pirmiausiai buvo apjungta LR Seimas, LR Prezidentūra, ministerijos, Vyriausybės kanceliarija, Muitinės ir Statistikos departamentai. 1996 m. į tinklą įtraukti didieji Lietuvos miestai (Kaunas, Klaipėda, Šiauliai, Panevėžys ir Utena). Šis žingsnis papildė Valstybės institucijų kompiuterių tinklą net keturiomis dešimtimis institucijų. 1997-1998 m. įtraukiami likusieji rajonų tinklai ir miestai.

1996 m. įsakyme „Dėl Valstybės institucijų kompiuterių tinklo (VIKT) paslaugų teikimo taisyklių patvirtinimo“ pastebima, kad pagrindinė tinklo paskirtis – informacijos perdavimas, numatomas DNS, SMTP, NNTP ir WWW serverių aptarnavimas. Taip pat apibrėžiama abonentų ratas - „...juridinis arba fizinis asmuo, pasirašęs su Tinklo operatoriumi paslaugų teikimo sutartį.“[31] [15]. Įstatymas numato ir fizinių asmenų dalyvavimą Valstybės institucijų kompiuterių tinkle. Sutartyje numatomas jungimosi prie VIKT būdas, atsižvelgiant į kurį suteikiami adresai. Jungiantis komutuojama ryšio linija, nesuteikiamas pastovus adresas, bet priskiriamas vienas iš galimų „maršrutizuojamų“. Jei jungimosi linija pastovi, abonentui suteikiama adresų aibė, kurią išnaudojęs abonentas gali pretenduoti į papildomus adresus. Visi šie duomenys privalo būti

[31] Lietuvos Respublikos ryšių ir informatikos ministerijos įsakymas „Dėl Valstybės institucijų kompiuterių tinklo (VIKT) paslaugų teikimo taisyklių patvirtinimo“. 1996-11-12 Nr. 123 // http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=32665&p_query=&p_tr2=; prisijungimo laikas: 2006-06-05

numatyti sutartyje. Prie VIKT nuolatinėmis linijomis prisijungė apie 400 abonentų, o komutuojamomis apie 1500 vartotojų.

VIKT tinklu naudojasi šios kompiuterizuotos informacinės sistemos (KIS)[32] [50]:

- Seimo informacinė sistema,
- Vyriausybės informacinė sistema,
- Valstybės biudžeto apskaitos ir mokėjimų informacinė sistema,
- KIS "SAVIVALDYBĖ",
- KIS "APSKRITIS",
- Valstybės kontrolės KIS,
- Valstybinės mokesčių inspekcijos KIS,
- Statistikos departamento KIS,
- Sodros informacinė sistema,
- Ligonių kasų informacinė sistema,
- Valstybinės darbo inspekcijos KIS,
- Lietuvos darbo biržos KIS,
- Valstybinės augalų karantino inspekcijos KIS,
- Kultūros vertybių apsaugos departamento KIS.

Žinoma, tokį pasirinkimą lėmė ne tik patogesnio ar greitesnio apsikeitimo informacija galimybė, bet ir kiti žadami tinklo privalumai. Vienas iš svarbiausių – informacijos saugumas, todėl sujungiant abonento vietinį ir Valstybės institucijų kompiuterių tinklus paruošiamas įsakymu[33] [15] reglamentuojamas protokolas, kuriame fiksuojamos visos naudojamos saugos priemonės. Sudarant sutartį numatomas ir duomenų srauto filtravimas, kuris aptariamas ir aprašomas nustatant filtravimo aspektus. Tinklu gali keliauti tik leidžiamo turinio paketai.

1.3.2.2 Saugaus valstybinio duomenų perdavimo tinklo sukūrimas

2001 m. gruodžio 22 d. Lietuvos Respublikos Vyriausybė priėmė "Informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano" nutarimą, kuriame numatė saugaus valstybinio duomenų perdavimo tinklo sukūrimą, Valstybės institucijų kompiuterinio tinklo (VIKT) pagrindu. Vykdant šį nutarimą ir siekiant užtikrinti perduodamų duomenų saugumą, buvo pradėta diegti perduodamų duomenų apsaugos technologija. Taip buvo kuriamas

[32] VIKT tinklas // http://www.is.lt/vikt_tinklas/apievikt.shtml; prisijungimo laikas: 2006-06-05
[33] Lietuvos Respublikos ryšių ir informatikos ministerijos įsakymas „Dėl Valstybės institucijų kompiuterių tinklo (VIKT) paslaugų teikimo taisyklių patvirtinimo". 1996-11-12 Nr. 123 // http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=32665&p_query=&p_tr2=; prisijungimo laikas: 2006-06-05

visuotinis duomenų perdavimo tinklas. Šiuo metu Valstybės institucijų kompiuterių tinklas apima net penkiasdešimt penkis tinklo komunikacijos mazgus išdėstytus Lietuvos Respublikos teritorijoje. Kiekvieną komunikacijos mazge informacijos srautas stebimas ir kontroliuojamas specializuotas monitoringo sistemas (Cisco works, Tivoli Netview, NavisCore, Alcatel NMS).

2003 m. lapkričio 20 d. Briuselyje pasirašyta Europos Bendrijos ir Lietuvos Respublikos susitarimo memorandumas dėl Lietuvos dalyvavimo Bendrijos elektroninio keitimosi duomenimis tarp administracijų programoje IDA (Interchange of Data between Administrations).

2003 m. gruodžio 31 d. Lietuvos Respublikos Vyriausybė priėmė nutarimą Nr.1705 "Dėl Lietuvos Respublikos dalyvavimo Europos Bendrijos elektroninio keitimosi duomenimis tarp administracijų programoje IDA", kuriuo Vidaus reikalų ministerija įgaliota koordinuoti Lietuvos dalyvavimą šioje Europos Bendrijos programoje. Nutarimu nustatyta, kad susijungimui su Europos Bendrijos administracijų tinklais naudojamas saugus valstybinis duomenų perdavimo tinklas (buvęs VIKT).

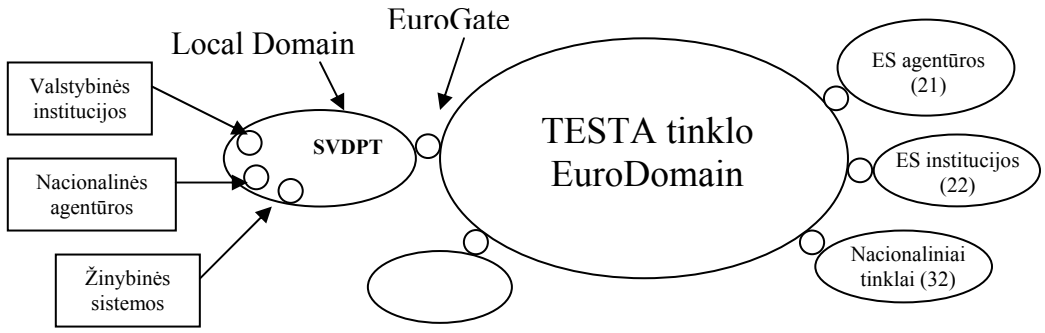
Vykdant nutarimą 2004 metų kovo mėnesį Saugus valstybinis duomenų perdavimo tinklas sujungtas su Europos administracijų duomenų perdavimo tinklu TESTA (Trans-European Telematics Networks for Administrations). VIKT tinklas bus atskirtas nuo Interneto ir pertvarkytas į Saugų valstybinį duomenų perdavimo tinklą, kuris aptarnaus tik valstybės ir savivaldybių institucijas.[34] [49] (5 schema).

Saugaus valstybinio duomenų perdavimo tinklo paskirtis[35] [47]:

- Sudaryti sąlygas valstybės institucijoms saugiai ir efektyviai keistis informacija su Europos Sąjungos administracijomis.
- Apsaugoti tarpusavio komunikaciją tarp valstybinių institucijų ir jų struktūrinių padalinių.
- Sumažinti Lietuvos Respublikos institucijų išlaidas duomenų apsaugos priemonėms, programinei įrangai, duomenų perdavimo paslaugoms.
- Įgalinti Lietuvos Respublikos fizinius ir juridinius asmenims naudotis elektroninės valdžios paslaugomis užtikrinant saugią komunikaciją su Europos Sąjungos ir valstybių narių administracijomis.

[34] TESTA architektūra // http://www.svdpt.gov.lt/architektura.php; prisijungimo laikas: 2006-06-05
[35] Saugus valstybinis duomenų perdavimo tinklas (SVDPT) // http://www.svdpt.gov.lt/kas_yra_SVDPT.php; prisijungimo laikas: 2006-06-05

5 schema. SVDPT integravimo modelis



SVDPT darbą reglamentuoja:

- Duomenų sauga užtikrinama vadovaujantis Bendraisiais duomenų saugos reikalavimais, patvirtintais Lietuvos Respublikos Vyriausybės 1997m. rugsėjo 4 d. nutarimu Nr. 952.
- Saugiame valstybiniame duomenų perdavimo tinkle elektroninio keitimosi duomenimis saugumo užtikrinimo priemonės ir tvarka nustatoma vadovaujantis Lietuvos standartu LST ISO/IEC 17799:2002 „Informacijos technologija. Praktiniai informacijos saugumo valdymo aspektai“.
- Lietuvos Respublikos Vyriausybės nutarimas Nr. 1625 „Dėl informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo". 2001m. gruodžio 22d.
- Vidaus reikalų ministerijos įsakymas „Dėl Tipinių duomenų saugos nuostatų patvirtinimo“, 2003 07 16, Nr. 1V-272.
- Lietuvos Respublikos Vyriausybės 2003 m. lapkričio 25 d. nutarimas Nr. 1468 „Dėl Elektroninės valdžios koncepcijos įgyvendinimo priemonių plano patvirtinimo".
- Europos Bendrijos ir Lietuvos Respublikos susitarimo memorandumas dėl Lietuvos dalyvavimo bendrijos elektroninio keitimosi duomenimis tarp administracijų programoje (IDA) 2003 lapkričio 20 d.
- Lietuvos Respublikos Vyriausybės nutarimas „Dėl Lietuvos Respublikos dalyvavimo Europos Bendrijos elektroninio keitimosi duomenimis tarp administracijų programoje (IDA) 2003 m. gruodžio 31 d. Nr. 1705.
- Lietuvos Respublikos Vidaus reikalų ministro įsakymas Nr. 1v-50, 2004 02 24 „Elektroninio keitimosi duomenimis su Europos Sąjungos ir valstybių narių administracijomis taisyklės".
- Lietuvos Respublikos Vidaus reikalų ministro įsakymas Nr. 1v-167, 2004 05 14 „Dėl Saugaus valstybinio duomenų perdavimo tinklo nuostatų ir Saugaus valstybinio duomenų perdavimo tinklo paslaugų teikimo taisyklių patvirtinimo".

- 2006 m. birželio mėn. 19 d. Vyriausybės nutarimu Nr. 601 patvirtino "Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinę strategiją iki 2008 metų" ir "Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinės strategijos iki 2008 metų įgyvendinimo priemonių planą".
- Saugaus valstybinio duomenų perdavimo tinklo duomenų saugos nuostatai tvirtinami VĮ „Infostruktūra“ direktoriaus įsakymu, suderinus su Lietuvos Respublikos vidaus reikalų ministerija.
- Europos Sąjungos ir valstybių narių administracijų elektroninio keitimosi duomenimis saugos užtikrinimo priemonės yra įdiegtos IDA programos tinkluose, o Lietuvos Respublikoje – Saugiame valstybiniame duomenų perdavimo tinkle.
- Elektroninio keitimosi duomenimis ir duomenų saugos užtikrinimo priemonės turi atitikti sutarties tarp Europos Bendrijos IDA programos komisijos ir Lietuvos Respublikos Vyriausybės įgaliotos institucijos sąlygas.
- Siekiant padidinti Saugaus valstybinio duomenų perdavimo tinklo kamieninės dalies patikimumą, Saugaus valstybinio duomenų perdavimo tinklo operatorius konkursu atrenka ne mažiau kaip du telekomunikacijų paslaugų teikėjus.

2. INFORMACIJOS SAUGOS SISTEMOS KŪRIMAS

Informacija – vertingas organizacijos turtas, kurio apsaugai skiriama vis daugiau dėmesio. Taip siekiama sumažinti galimus komercinės veiklos nuostolius, padidinti investicijų pelną, užtikrinti komercinės veiklos nepertraukiamumą.

Informacijos saugumas apibrėžiamas kaip technologijų, techninių ir administracinių priemonių panaudojimas informacinio turto apsaugai nuo tyčinio ar atsitiktinio nesankcionuoto įgijimo, sunaikinimo, atskleidimo, manipuliacijos, modifikacijos, praradimo ar panaudojimo.[36]

Skiriamos trys informacijos saugos sudėtinės dalys (kurios gali būti laikomos saugos tikslais, principais ar savybėmis):[37] [41, 5]

Konfidencialumas – užtikrinama, jog informacija bus prieinama tik tiems, kurių kreiptis į ją yra sankcionuota.

Vientisumas – informacijos ir jos apdorojimo metodų tikslumo ir užbaigtumo garantija.

Prieinamumas – užtikrinama, kad įgalioti vartotojai turi galimybę pasiekti informaciją.

Tačiau organizacijos vis dažniau susiduria su įvairiausiomis grėsmėmis iškylančiomis šioms trims informacijos saugumo savybėms.

2.1 Potencialios saugumo grėsmės

Organizacijos informacinės sistemos – gyvybiškai svarbus bet kurios modernios veiklos įrankis. O jei organizacijos specializacija yra elektroninės valdžios paslaugų teikimas, informacinė sistema tampa ne tik įrankiu, bet ir savotišku organizacijos prekiniu ženklu, kuris, dėl tiesioginio ryšio su vartotojais, sukuria pastarosios įvaizdį ir su jį sieja su informacinės sistemos savybėmis.

Saugumas – bene svarbiausia tokios informacinės sistemos (o tuo pačiu ir organizacijos) demonstracinių ir faktinių savybių, kuri organizacijos įvaizdį sieja su patikima ir efektyvia veikla. Tai, puikiai privačiame sektoriuje išbandyta, savybė, kuri yra vertinama visų, kliento ilgalaikį pasitikėjimą norinčių išlaikyti, verslo struktūrų.

Tai ir pagrindinė, su kompiuteriais susijusių nusikaltimų (*computer related crime*), latentiškumo prielaida: paviešinto, su saugumu susijusio incidento, pasekmė gali būti didžiuliai

[36] Termino apibūdinimas // http://www.sei.cmu.edu/str/indexes/glossary/information-security.html; prisijungimo laikas: 2006-04-21

[37] Lietuvos Standartizacijos departamentas. Informacijos technologija. Praktiniai informacijos saugumo valdymo principai ISO/IEC 17799:2000.

finansiniai ir moraliniai nuostoliai, kurie stipriai įtakotų arba visiškai sugriautų organizacijos įvaizdį, priverstų ją bankrutuoti.

Informacijos saugumo incidentu gali tapti piktybinis informacinės sistemos puolimas ar atsitiktinė jos veiklos klaida. Siekiant sukurti patikimą ir efektyviai veikiančią sistema, būtina išanalizuoti galimas grėsmes sistemai ir jų prevencijos priemones.

Grėsmių atsiradimą įgalina ir jį padidinantys faktoriai:

- Globalaus tinklo koncepcija ir nuotolinės prieigos galimybė.
- Informacinių sistemų automatizmas ir jų tarpusavio komunikacija.
- Pastovus technologijų progresas ir naujų galimybių atsiradimas.
- Spartėjantys duomenų apdorojimo, saugojimo ir perdavimo procesai.
- Laikmenų raida ir taikymas.
- Didžiulis vartotojų ratas.
- Centralizuotas informacijos saugojimas ir prieigų valdymo sudėtingumas.

Šie faktoriai tiesiogiai kuria grėsmę duomenų ir informacijos saugumui organizacijoje. Pačios grėsmės gali būti skiriamos į vidines ir išorines. O pagal atsiradimo priežastį į: piktybines ir atsitiktines. Atsitiktinės vidinės ar išorinės grėsmės (techniniai gedimai ir sutrikimai, nelaimingi atsitikimai, stichinės nelaimės ir pan.) nors ir nemalonios, tačiau nėra tokios pavojingos, kaip piktybinės. Piktybinės grėsmės duomenų ir informacijos saugumui pavojingos tuo, jog jų destruktyvus ar kenkėjiškas poveikis yra sistemingas ir logiškas – jos ne tik atkakliai siekia užsibrėžto tikslo, tačiau daro tai slapčia, dangstant veiklos metodus ir padarinius, naikinant pėdsakus. Tokiu būdu, elektroninės informacijos ar duomenų vagystė, sistemos veiklos spraga ar neigiamas poveikis jai, gali išaiškėti labai negreitai. Tai dar viena elektroninių nusikaltimų latentiškumo priežastis.

Statistiškai, net 55% kompiuterinės informacijos saugumui kylančių pavojų atsiranda dėl žmonių darbo klaidų[38] [46, 16]. Tam tikra prasme šios klaidos gali būti traktuojamos kaip atsitiktinė grėsmė, tačiau jos atsiranda dėl organizacijoje taikomos informacijos apsaugos politikos nustatytų taisyklių nesilaikymo, o tai gali būti įvardinta kaip „nusikalstamas neveiksnumas" (kai darbuotojas veikė ne pagal saugumo instrukcijas, nors žinojo arba privalėjo žinoti apie galimas grėsmes). Šių grėsmių aktualumą galėtų įtakoti organizacinių ir moralinių priemonių pasirinkimas. Tai, kaip bus vykdoma organizacijos informacijos apsaugos politika, tiesiogiai atsispindės personalo darbe pasitaikančiose kritinėse klaidose, dėl kurių atsiradimo gali nukentėti visos sistemos saugumas.

[38] Petrauskas R., Štitilis D. Kompiuteriniai nusikaltimai ir jų prevencija. Vilnius: Lietuvos teisės akademija, 2000.

Prie piktybinių vidinių grėsmių galima priskirti nepatenkintų ar nesąžiningų darbuotojų veiklą. Tokie darbuotojai gali padaryti labai daug žalos organizacijai, dėl jiems legaliai suteiktų privilegijų, kurias jie gali savarankiškai praplėsti. Taip pat įmanomas privilegijų panaudojimas ne pagal paskirtį, viršijant savo įgaliojimus ar net jų perleidimas pašaliniams asmenims. Nuo šios grėsmės padeda apsisaugoti atsakingas kompiuterinės sistemos administratorių darbas ir tikslus privilegijų skirstymas, o taip pat ir atsakingų už informacijos saugumą asmenų atliekamas situacijos stebėjimas. Tyrimai rodo, jog didžioji dalis nusikaltimų (73%) buvo priskirta vidiniams veiksniams[39] [29, 29].

Prie piktybinių išorinių grėsmių duomenų ir informacinės sistemos saugumui priskiriami neteisėti prisijungimai prie sistemos, kurie apeina arba įveikia taikomas apsaugos priemones ir pažeidžia informacijos vientisumą, juos nukopijuoja, sugadina arba sunaikina.

Pagrindiniai pažeidėjų veiklos metodai yra informacijos srauto analizė ir neteisėtas įsibrovimas į sistemą. Šie metodai yra kompleksiniai ir apima daug pagalbinių priemonių.

Srauto analizės metu pažeidėjas gali veikti aktyviai arba pasyviai. Pasyvusis pažeidėjo veikimas pasireiškia perimamų pranešimų skaitymu, jų ilgio ir perdavimų dažnio fiksavimu, vartotojų identifikavimu ir informacijos kopijavimu. Ši veikla ypač pavojinga dėl pranešimuose esančio turinio atskleidimo, o taip pat jų pardavimo suinteresuotoms grupėms. Be to, ji ilgą laiką gali vykti nepastebimai arba likti visai nepastebėta. Tuo tarpu, aktyvi įsilaužėlio veikla ne tik pavojinga, tačiau ir žalinga dėl jos metu vykdomų darbą trukdančių veiksmų, bet ir poveikio duomenims darymo. Atliekami ne tik pasyvios veikos veiksmai, bet taip pat keičiamas pats perduodamos informacijos srautas — modifikuojami arba stabdomi pranešimai, klaidinami vartotojai. Tokia veikla organizacijai gali atsieiti ne tik paslapčių atskleidimu ar pranašumo praradimu, bet ir įvaizdžio sugriovimu ar visišku bankrotu.

Neteisėto prisijungimo prie sistemos metu įmanomas ne tik apdorojamos, bet ir saugomos informacijos kopijavimas, modifikavimas ar sunaikinimas. Užfiksavus net ir labai trumpą nesankcionuotą prisijungimą prie sistemos, organizacija sugaišta nemažai laiko, o taip pat išleidžia ir milžiniškas sumas pinigų vien tam, kad būtų patikrinta duomenų bazėse saugoma informacija, jos vientisumas ir teisingumas.

Dažniausiai nusikaltėliai pasinaudoja programinėmis apsaugos ir operacinių sistemų klaidomis, neteisingu ar nepilnu apsaugos priemonių panaudojimu, tačiau neretai griebiamasi ir papildomų priemonių, kurių pagalba lengviau pralaužiama informacijos apsaugos sistema[40] [43, 28]:

[39] Česna R., Štitilis D. Kompiuterinės informacijos ir elektroninių dokumentų apsauga viešajame administravime. Vilnius: Lietuvos teisės akademija, 2000.
[40] Maiwald E. Network security. A begginers guide. New York. 2003.

1. *Privilegijų pasisavinimas.* Sužinomi arba pritaikomi teisėtų vartotojų slaptažodžiai, prisijungimo duomenys. Tai gali būti atliekama ir fiziniu (pamatymas, užrašai, pasiklausymas, šiukšlės, prasmukimas paskui vartotoją), ir virtualiu būdu (programinių priemonių naudojimas, „Trojos arkliai“, prisidengimas teisėtu vartotoju, slaptažodžių parinkimas ar pritaikymas, programinių klaidų ar trūkumų išnaudojimas).
2. *Informacijos perėmimas ir įsibrovimas į sistemą.* Įvairaus pobūdžio programinės įrangos, kurios pagalba galima trikdyti sistemos darbą (virusai, kirminai, serverio atakos, užklausų lavina), pagrobti (tiesioginis prisijungimas prie sistemos ir pranešimų perėmimas, elektromagnetinis perėmimas) ar sunaikinti norimą informaciją, palengvinti patekimą į sistemą įveikiant apsaugos priemones.
3. *Specializuotos priemonės.* Specifinės priemonės reikalaujančios nemažai žinių ir išradingumo, analitinių sugebėjimų ir bandančiojo įsibrauti asmens intelektualumo. Gali būti kombinuojamos anksčiau minėtos fizinės, techninės ir programinės priemonės, suburiamos nusikalstamos grupuotės, susipažįstama ir pajungiami organizacijos darbuotojai.

Visi aptarti metodai ir priemonės skirti vieninteliam tikslui – įveikti organizacijos apsaugos sistemą ir gauti prieigą prie saugomų duomenų. Būtent dėl to reikia atkreipti ypatingą dėmesį į informacijos apsaugos politikos vystymą, o taip pat pačios apsaugos sistemos kūrimą. Laipsnis, kuriuo bus įvykdomi saugumo reikalavimai, tiesiogiai įtakos disponuojamos informacijos saugumą.

2.2 Informacijos saugumo politika – veiklos strategijos dalis

Informacijos apsaugos politika apibrėžiama kaip tikslių rekomendacijų ir bendrų saugumo taisyklių, kurių laikymasis maksimaliai saugo organizacijoje cirkuliuojančią informaciją, visuma. Ji turi būti puikiai žinoma visiems organizacijos darbuotojams (atsižvelgiant į jų atsakomybės ribas). Tinkamai vystoma ir taikoma organizacijos informacijos apsaugos politika papildo bendrą kuriamą informacijos apsaugos sistemą organizaciniame, moraliniame ir etiniame lygmenyje.

Pagrindinis vystomos apsaugos politikos uždavinys – disponuojamos informacijos valdymo ir perdavimo apsauga, o taip pat galimų grėsmių rizikos sumažinimas. Tai individuali kiekvienos organizacijos sukurta informacijos apsaugos politikos koncepcija, kuri privalo optimaliai atitikti

organizacijos struktūrą ir tikslus, jos veiklos pobūdį ir specifiką. Tuo pat metu informacijos apsaugos politika betarpiškai taikoma atsižvelgiant į naudojamas darbo apsaugos priemones.

Informacijos apsaugos politika vaidina labai svarbu vaidmenį visuotinės darbo vietų kompiuterizacijos periode. Teigiama, kad „...elektroninis duomenų apdorojimas, palyginti su rankiniu, yra apsaugotas tik l procentu"[41] [29, 29], todėl kuriant ir vystant informacijos apsaugos politiką būtina atsižvelgti į riziką susijusią su turima informacija, numatyti pasekmes ją praradus ar pagrobus, atsižvelgti į daugybę personalo žmogiškųjų faktorių (darbuotojų sveiką nuovoką, pareigingumą, etiškumą, lojalumą ir motyvaciją). Be abejo, tvirtų taisyklių, kaip kurti organizacijos informacijos apsaugos politiką, negali būti dėl jos individualumo, tačiau sukurta daug rekomendacijų, nurodančių pagrindinius aspektus, į kuriuos būtina atkreipti dėmesį.

Ekonominio bendradarbiavimo ir plėtros organizacija (OECD) paskatino organizacijas atkreipti dėmesį į saugumo kultūros vystymą ir apibrėžė devynis principus, kuriais vadovaujantis galima sumažinti riziką susijusią su informacijos saugumu[42] [45]. Šių principų paskirtis yra kurti bendrą vartotojų supratimą apie pavojus kylančius informacijai, o taip pat formuoti saugos įgūdžius, kuriuos galima būtų naudoti praktikoje.

1. *Sąmoningo atsargumo principas (awareness) – Privaloma suprasti informacinių sistemų saugumo poreikį ir kaip galima jį sustiprinti.* Tai suvokimo, kad informacijos apsauga būtina visuose informacinės veiklos procesuose, diegimas visų lygių darbuotojams ir vadovams. Pirmas ir svarbiausias dalykas saugant informaciją – pačio saugojimo reikalingumo įsisąmoninimas, o ne aklas instrukcijų kartojimas. Taip pat ir potencialios žalos suvokimas, bei pasekminio ryšio tarp saugumą užtikrinančių veiksmų ir padarinių matymas; išorinio ir vidinio pavojaus skyrimas; tarpusavio sąryšių ir priklausomybių, bei dėl jų didėjančios rizikos įvertinimas; saugumo kultūros, kaip natūralios organizacijos tvarkos dalies vertinimas, priėmimas ir taikymas.
2. *Atsakomybės principas (responsibility) – Visi yra atsakingi už informacinių sistemų ir tinklų saugumą.* Sekantis saugumo politikos elementas – darbuotojai suvokia savo, kaip savarankiško vieneto svarbą bendros sistemos saugumo užtikrinime, motyvuotai vertina savo indėlį. Tai atsakomybės tarp darbuotojų paskirstymas, kuris neleidžia aplaidžiai žiūrėti į patikėtą darbą, verčia nuolat vertinti atliekamus veiksmus ir stebėti kitų darbo procesus: sistemos projektavimas, jos atnaujinimas, kasdieninių veiksmų atlikimas, atsakomybės

[41] Čėsna R., Štitilis D. Kompiuterinės informacijos ir elektroninių dokumentų apsauga viešajame administravime. Vilnius: Lietuvos teisės akademija, 2000.
[42] Organization for economic co-operation and development. Guidelines for the security of information systems and networks. Towards the culture of security. 2002-07-25, Paris.// http://www.oecd.org/dataoecd/16/22/15582260.pdf; prisijungimo laikas: 2006-03-23

kontrolės būdai.

3. *Reakcijos principas (response) – Veikti privaloma laiku ir bendradarbiaujant, kad būtų galima lengviau išvengti, aptikti ar sureaguoti į saugumo incidentus.* Tai neatidėliotinas ir tvirtas atsakas į iškilusias grėsmes. Vertinant informacinių sistemų tarpusavio sujungimą ir procesų vykimo greiti – žalos augimą, būtina veikti žaibiškai. Bendradarbiaujant su kitais darbuotojais rezultatai gali gerokai pagerėti, todėl skatinamas informacijos apie pavojus dalinimasis ir bendrų gynybos būdų kūrimas.
4. *Etiškumo principas (ethics) – Privaloma gerbti teisėtus kitų interesus.* Tai ne tik savo, bet ir kitų interesų gerbimas. Atkreipiamas dėmesys į tai, kad informacinės sistemos ir tinklai yra apjungti, kas padaro juos vieną nuo kito priklausomus, o veikla ar ne veikla gali paliesti kitus. Šis principas glaudžiai siejasi su sąmoningumo, atsakomybės ir reakcijos principais. Etiški veiksmai yra kritiniai, todėl darbuotojai turėtų atkakliai vystyti ir taikyti geriausią praktiką, kuri patenkintų saugumo poreikius, tačiau gerbtų ir kitų teisėtus interesus.
5. *Demokratijos principas (democracy) – informacinių sistemų ir tinklų saugumas turi būti suderinamas su svarbiausiomis demokratiškos visuomenės vertybėmis.* Saugumo siekimas negali pažeisti tokių demokratinės visuomenės vertybių kaip asmens privatumas, laisvė, nuomonės ar idėjų apsikeitimas, nevaržomo informacijos srauto, informacijos ir komunikacijos konfidencialumas, atvirumas ir skaidrumas.
6. *Rizikos įvertinimo principas (risk assessment) – Privalu taikyti rizikos vertinimą.* Tai geras būdas nustatyti galimoms grėsmėms ir silpniausioms sistemos vietoms. Vertinami išoriniai ir vidiniai faktoriai (tokie kaip technologijos, fiziniai ir žmogiškieji faktoriai, politikos ir trečiųjų šalių įtaka), kurie padeda parinkti atitinkamą rizikos lygį. Be to, numatomos priemonės ir sprendimai informacijos apsaugai, kai jai iškyla pavojus, nustatomas pačios informacijos pobūdis, priskiriama adekvataus lygio apsauga. Svarbu atsižvelgti į tarpusavio sujungimo faktorių (interconnectivity), kad būtų galima įvertinti riziką susijusią su galima žala, kurią galima gauti ar padaryti kitiems.
7. *Saugumo kūrimo ir diegimo principas (security design and implementation) – Saugumas turi būti integruojamas kaip gyvybiškai svarbus informacinių sistemų ar tinklų elementas.* Tai sistemos kūrimo atsižvelgiant į saugumą principas, kuris akcentuoja darbuotojų dėmesį kuriant ir diegiant sistemą. Pabrėžiama saugumo politikos kūrimas, taikymas ir koordinavimas siekiant optimizuoti sistemą. Pagal turimos informacijos vertę numatomi informacijos apsaugos sprendimai, kurie taikomi kuriamoje sistemoje. Taikomi techniniai ir netechniniai sistemos saugumo sprendimai. Tai pagrindinis principas, kuriuo vadovaujantis įmanoma gauti norimą efektą atitinkantį reikalavimus. Saugumas pateikiamas

kaip fundamentalus, visų produktų, paslaugų, sistemų ar tinklų dizaino ir architektūros, elementas: galutiniams vartotojams saugumo taikymas paprastai reiškia produkto pasirinkimą ir pritaikymą.

8. *Saugumo valdymo principas (security management) – Turi būti taikomas visa apimantis saugumo galimybių valdymas.* Saugumo procesų ir priemonių valdymas organizacijos informacinėje sistemoje turi remtis rizikos numatymu ir apimti visus veiklos lygius ir juose vykdomas operacijas. Labai svarbu, kad saugumo valdymas nebūtų primetamas, o vystytųsi dinamiškai - laikantis jau išvardintų saugumo principų. Tokiu būdu iškylantys nesklandumai ir situacijos, į kurias pakliūva organizacijos darbuotojai, būtų lengviau koordinuojamos, sprendimai efektyvesni ir greičiau priimami. Saugumo valdymas apima prevencinį požiūrį į vis naujai iškylančias grėsmes, reakciją į saugumo incidentus, sistemos atkūrimą ir pastovų jos palaikymą, o taip pat ir kontrolę, auditą. Jei visa sistema paremta saugumo įgyvendinimo principais - informacijos saugumo lygis optimalus, atsižvelgiant į rizikos vertinimą ir informacijos kategoriją. Informacinės sistemos saugumo politika, priemonės ir procedūros turi būti koordinuojamos ir integruojamos sukurti tvirtą ir išbaigtą sistemą.
9. *Pakartotinio vertinimo principas (reassessment) – Privalu peržvelgti ir įvertinti iš naujo informacinės sistemos saugumą, atitinkamai modifikuoti saugumo politiką, priemones ir procedūras*. Šis principas reikalingas sistemos gyvybingumui palaikyti. Kadangi grėsmė visą laiką kinta, priklausomai nuo aplinkos situacijos ir naudojamų priemonių, tai pakartotinis periodiškas sistemos saugumo vertinimas padeda laiku pastebėti naujas galimas grėsmes ir atnaujinti apsisaugojimo būdus.

Šių, tarptautinės organizacijos sukurtų, informacinių sistemų ir tinklų saugumo gairių tikslas yra sužadinti organizacijų atsargumą atkreipiant dėmesį į riziką susijusią su informacijos apsauga ir paskatinti apsaugos sistemų vystymą, bendrų standartų diegimą.

Vystant informacijos apsaugos politiką organizacijoje labai svarbu nustatyti turimos informacijos reikšmę ir atitinkamą apsaugos lygį, kad būtų išvengta per didelio arba nepakankamo finansavimo, apsaugos užtikrinimo (6 Schema).

JAV Nacionalinis standartų ir technologijos institutas federaliniame informacijos ir informacinių sistemų saugumo kategorizavimo standarte FIPS 199[43] [17] Kategorijos

[43] Barker W.C. Guide for mapping types of information and inforamtion systems to security categories. Information security. Volume I. 2004 June, United States of America // http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V1-final.pdf; prisijungimo laikas: 2006-03-23

nustatomos remiantis poveikio lygiu (silpnas, vidutinis ir stiprus) ir kiekvieno iš jų apsaugos tikslais (slaptumu, vientisumu ir naudingumu).

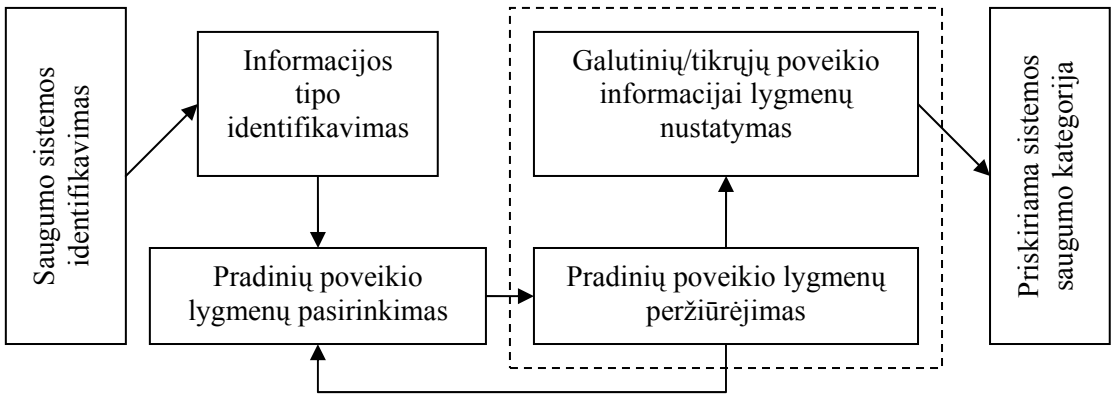
Apsaugos tikslai apibrėžiami kaip:

- *Slaptumas* (confidentiality) - leidimo prieiti prie informacijos saugojimas, o taip pat draudimas viešinti asmeninę ar privačią informaciją.
- *Vientisumas* (integrity) - autentiškumo saugojimas neleidžiant neteisėtai keisti ar sugadinti informaciją.
- *Pasiekiamumas* (availability) - patikimo ir nepertraukiamo informacijos pasiekimo užtikrinimas.

Poveikio lygiai vertinami:

- *Silpnas* (low) – jei potencialus poveikis, informacijai netekus slaptumo, vientisumo ir pasiekiamumo, turės ribotą neigiamą poveikį organizacijai, individui ar jų tikslams.
- *Vidutinis* (moderate) – jei potencialus poveikis, informacijai netekus slaptumo, vientisumo ir pasiekiamumo, turės didelį neigiamą poveikį organizacijai, individui ar jų tikslams.
- *Stiprus* (high) – jei potencialus poveikis, informacijai netekus slaptumo, vientisumo ir pasiekiamumo, turės katastrofišką neigiamą poveikį organizacijai, individui ar jų tikslams.

6 Schema. Informacijos saugumo kategorizavimo procesas[44]



[44] Barker W.C. Guide for mapping types of information and inforamtion systems to security categories. Information security. Volume I. 2004 June, United States of America // http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V1-final.pdf; prisijungimo laikas: 2006-03-23

Saugumo kategorijos parinkimui naudojama formulė:

SAUGUMO KATEGORIJA informacijos tipas = {(slaptumas, poveikis), (vientisumas, poveikis), (prieinamumas, poveikis)}

Pavyzdžiai:

SAUGUMO KATEGORIJA tyrimų informacija = {(slaptumas, stiprus), (vientisumas, vidutinis), (prieinamumas, stiprus)}

SAUGUMO KATEGORIJA vieša informacija = {(slaptumas, netaikomas), (vientisumas, vidutinis), (prieinamumas, silpnas)}

SAUGUMO KATEGORIJA administracine informacija = {(slaptumas, silpnas), (vientisumas, silpnas), (prieinamumas, silpnas)}

Teisingai kurti norimą individualią informacijos apsaugos politiką labai svarbu, tačiau nemažiau svarbu ir sugebėti ją įgyvendinti. Patartina vadovautis pagrindiniais apsaugos politikos praktinio diegimo principais[45] [40, 38]:

- Darbuotojų išskirstymas į grupes. Tokiu būdu atskirų projektų darbuotojai negalės viršyti turimų įgaliojimų, jiems bus griežtai apribotos privilegijos. Grupes lengviau gerai kontroliuoti.
- Sukurtos informacijos savininkų teisė į ją, bei šios teisės perleidimo numatymas. Tačiau būtinas apsaugos mechanizmas prižiūrintis, kad ši disponuojama informacija nebūtų sukurta iš jau esančios aukštesnio saugumo laipsnio informacijos.
- Privilegijų minimumo numatymas. Svarbus apsaugos politikos įgyvendinimo aspektas, nes remiantis šia taisykle paskirstomos ir pačios privilegijos. Suteikiant tam tikras teises, atsižvelgiama į jų būtinumą atliekamam darbui ar pareigoms. Tokiu būdu suteikiamos tik tos teisės, kurių vartotojui tikrai reikia.
- Centralizuotas rūšinės informacijos saugojimas ir automatizuotų informacijos vientisumo stebėjimo programų diegimas.
- Suteikiamų teisių ir privilegijų pavaldumo hierarchija. Efektyviai derinama kartu su teisių minimumo nustatymu.

[45] Jastramskas V. Informacijos apsaugos pagrindai. Kaunas: Technologija, 1999.

2.3 Informacijos saugumo sistemos kūrimas

Informacijos apsaugos sistema – programinių, techninių, organizacinių, etinių ir moralinių priemonių visuma, kuri kuriama atsižvelgiant į teisines normas reglamentuojančias informacijos apsaugą. Pagrindinis apsaugos sistemos kūrimo tikslas – saugoti informaciją, kuria disponuoja organizacija, kiek įmanoma sumažinti riziką ją prarasti ir įveikti potencialiai dėl to atsirasiančius nuostolius.

Pirmas žingsnis kuriant patikimą apsaugos sistemą – atlikti rizikos analizę[46] [41, 15]. Rizika tai bet kurio proceso ar veiklos neišvengiamas bruožas. Tik geras išankstinis pasiruošimas padeda ją maksimaliai sumažinti ir išvengti nepageidaujamų pasekmių. Pačią rizikos analizę galima įvardinti kaip nuostolių, atsiradusių grėsmei pasitvirtinus, paskaičiavimą. Kiekvienos analizės metu įvertinamos kylančios grėsmės, sistemos dalių pažeidžiamumas ir galimos kontrpriemonės nelaimės atveju. Paprastai rizikos analizė prasideda nuo galimų grėsmių numatymo ir labiausiai pažeidžiamų sistemos vietų aprašymo. Pagal numatytas grėsmes ir įvertintą riziką parenkamos atitinkamos apsaugos priemonės. Vertinant pasirinktų priemonių tinkamumą, lyginamos išlaidos apsaugos sistemai kurti ir galimų nuostolių dydis. Pagal padarytas išvadas priimamas galutinės rizikos analizės išvados. Galima pastebėti, jog kuo mažiau skiriama investicijų apsaugos priemonėms, tuo labiau išauga galima rizika. Pagrindinis rizikos įvertinimo principas: priežiūros išlaidos turi būti palyginamos su komercinės veiklos nuostoliais, kaip saugumo nesėkmės rezultatu.

Informacijos apsaugą taip pat galima pavadinti ir būsena arba tęstine paslaugą kurią sukuria pati organizacija arba išoriniai ekspertai (trečia šalis). Be abejo, kaip ir bet kuri kita paslauga ar prekė, ji turi savo gyvavimo ciklą. Nacionalinis standartų ir technologijų institutas taip apibrėžia informacijos paslaugos gyvavimo ciklą (7 Schema)[47] [37, 27]:

1) **Inicijavimo fazė.** Informacijos apsaugos poreikio atpažinimas ir suformulavimas. Dažnai ši fazė prasideda dėl įvykusio incidento, tačiau organizacijai, be abejo, naudingiau, jei galima grėsmė numatoma iš anksto. Poreikis gali atsirasti dėl *strateginių* (pertvarkos organizacijoje), *biudžeto* (padidintas ar sumažintas IT saugumo biudžetas), *techninių* (naujų technologijų taikymas ar senų atnaujinimas), *organizacinių* (nepasitenkinimas vykdomais apsaugos procesais), *personalo* (sumažėja profesionalų saugos srityje) *ar politinių* (politika neatitinka organizacijos tikslų) priežasčių. Kadangi nuo šios fazės

[46] Lietuvos Standartizacijos departamentas. Informacijos technologija. Praktiniai informacijos saugumo valdymo principai ISO/IEC 17799:2000.
[47] Grance T., Hash J., Stevens M. etc. Guide to information technology security services. 2003 October, United States of America // http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf; prisijungimo laikas: 2006-03-23

prasideda naujos IT saugumo paslaugos ciklas, jis greičiausiai pabaigia ar modifikuoja kitą, prieš tai buvusį, todėl organizacijos atsakingi asmenys turėtų būti ypatingai dėmesingi tokių pasikeitimų metu. Ši fazė taip pat apsprendžia ar organizacijai patogiau kurti saugumo paslaugą viduje, ar pirkti ją iš išorės.

2) **Įvertinimo fazė.** Šioje ciklo dalyje atsižvelgiama į aplinką ir numatomas būsimas inicijuojamos apsaugos priemonės efektas – vertinama jos efektyvumas ir investavimo praktiškumas. Taip pat analizuojama būsimo sprendimo suteikiamos galimybės ir numatomi barjerai. Analizės metu įvardijamos funkcijos ir sritys organizacijos veikloje, kurias įtakos naujos apsaugos diegimas ir šios įtakos priežastys. Tinkamai atliktoje įvertinimo analizėje atsižvelgiama į *strateginius* (apsaugos paslaugos būtinumas organizacijos veiklai), *biudžeto* (programos finansavimas), *techninius* (organizacijos techninės kompetencijos svarbos nustatymas ir suvokimas), *organizacinius* (nustatomas apsaugos paslaugos tinkamumas organizacijos aplinkai ir vertybėms), *personalo* (specifiniai paslaugos reikalavimai) ir *politinius* (norimos paslaugos kūrimas) aspektus. Apibendrinamos tyrimo išvados. Po šios fazės tampa aišku kokio lygio apsaugos paslauga reikalinga ir kiek ji bus efektyvi.

3) **Sprendimo priėmimo fazė.** Tai nėra vien tik tinkamiausio sprendimo, peržvelgus įvertinimo fazės rezultatus, pasirinkimas. Pasirinktam sprendimui antrą kartą taikomos įvairios situacijos ir svarstomas jo tinkamumas. Lyginama sprendimo kaina ir efektyvumas esant tam tikroms sąlygoms. Jei įvertinimo metu buvo tiriama sprendimo aplinka, tai šioje fazėje sprendimui pavaizduoti kuriamas konkretus atvejis, kuris padeda išskirti geriausią sprendimą. Taip pat svarstomos ir alternatyvos. Numatomos informacijos paslaugos savybės naudingos ir reikalingos organizacijai. Sukuriamas apsaugos paslaugos įdiegimo planas: diegimo vykdymas, reikalingas biudžetas, numatomas rizikos sušvelninimo ir pereinamojo laikotarpio planas, sukuriamos pasitraukimo strategijos (netikėtai atsitikus nenumatytam atvejui).

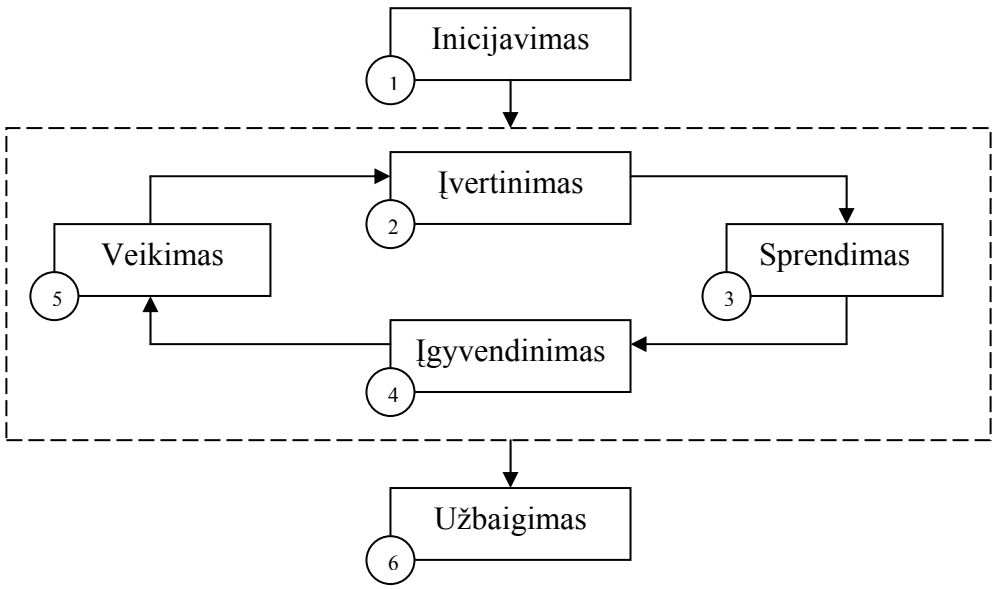
4) **Įgyvendinimo fazė.** Tai projekto realizavimo žingsnis. Numatomas paslaugos teikėjas – diegėjas. Jei organizacija numato naudotis išorinių teikėjų paslaugomis, gali būti svarstomi keli kandidatai. Esant valstybinei organizacijai – skelbiamas konkursas paslaugos teikėjo vietai užimti. Išrinkus paslaugos teikėją, projekto vadovai supažindiną jį su keliamais sistemai specifiniais reikalavimais: kuriamos paslaugos specifikacijos, sutvarkomi formalumai. Labai svarbus šios fazės tikslas – aiškus tarpusavio supratimas tarp paslaugos kūrėjo ir jos užsakovo: reikalavimai turi atitikti paslaugos savybes, kad investicija nevirstų nuostoliais. Galiausiai sukuriamas diegimo

planas ir juo remiantis projektuojama, bei diegiama reikalinga informacijos apsaugos paslauga.

5) **Veikimo fazė.** Prasideda kai paslaugos diegimas į organizacijos sistemą baigiamas. Jos metu organizacijos darbas ir sistemos veikla pastoviai stebimas, jog būtų užtikrinamas paslaugos išbaigtumas ir ji atitiktų organizacijos saugumo poreikius. Fazė tęsiama, kol atsiranda poreikis prasidėti sekančiai. Šios fazės metu aktyviai bendraujama su paslaugos kūrėju. Stebima ne tik įdiegta paslauga besinaudojančios organizacijos veikla, bet ir informacijos apsaugos paslaugos kūrėjo darbas. Pagal tarpusavio susitarimus ruošiamos ataskaitos aptariančios stebėjimo rezultatus. Atsiradus poreikiui, paslauga gali būti keičiama, perdaroma ar jos atsisakoma.

6) **Užbaigimo fazė.** Taip pat svarbus projekto žingsnis, kurio metu numatoma informacijos apsaugos paslaugos atsisakymas ar jos pakeitimas kita. Pasinaudojama trečioje projekto fazėje sukurtomis pasitraukimo strategijų alternatyvomis. Jei situacija pasikeitusi, šios strategijos gali būti modifikuojamos ir atnaujinamos. Pasirinkus tinkamą pasitraukimo strategiją, atsakingi už informacijos apsaugą vadybininkai turėtų būti pasirengę ją greitai ir efektyviai pritaikyti. Be abejo, būtina atkreipti dėmesį į taikyto informacijos apsaugos sprendimo savybes, kad ateityje galima būtų lengviau nustatyti organizacijos apsaugos poreikius ir nekartoti buvusių klaidų.

7 Schema. Informacinių technologijų saugumo paslaugos gyvavimo ciklas[48]



[48] Grance T., Hash J., Stevens M. etc. Guide to information technology security services. 2003 October, United States of America // http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf; prisijungimo laikas: 2006-03-23

Informacinių technologijų apsaugos paslaugos kūrimo cikle galimi įvertinimo, sprendimo priėmimo, įgyvendinimo ir veikimo fazių pasikartojimai nebaigiant pradėtojo projekto. Taip gali atsitikti dėl reikalavimų saugumui arba aplinkos situacijos pasikeitimo. Žinoma, kiekviena iš minėtų, o taip pat inicijavimo, fazės gali iš karto nuvesti prie paskutinės - užbaigimo fazės. Priežastimi tam gali tapti biudžeto pokyčiai arba paslaugos pakartotinis įvertinimas situacijos atžvilgiu. Apgalvotas išankstinis projekto baigimas leidžia organizacijai sumažinti nuostolius.

Informacijos apsaugos sistemos kūrimas – saugios informacijos vadybos procesų taikymas. JAV Nacionalinis standartų ir technologijos institutas skirsto informacijos apsaugos sistemos kūrimą į tris kategorijas:

- Valdymo (Tokie veiklos būdai ir atsakomybės išraiškos, kurios yra valdančiųjų kompetencijoje, kuriant organizacijos kompiuterių apsaugos programą. Jie atsakingi už šios programos ir rizikos organizacijoje valdymą.).
- Operacinė (Nukreipta į žmonių diegiamas ir valdomas programos dalis. Jiems dažnai prireikia techninės ar specialios patirties. Remiasi valdančiųjų asmenų veikla ir technine kontrole.).
- Techninė (Tokie techniniai procesai, kurie yra nukreipti į kompiuterių sistemų vykdomus informacijos saugojimo procesus. Stipriai priklausomi nuo organizacijos sistemos efektyvumo ir stabilaus jos darbo.).

Šios kategorijos apima visą informacijos apsaugos organizavimą. Labai svarbu, kuriant ar įdiegiant informacijos apsaugos sistemą, atkreipti dėmesį į šių kategorijų tarpusavio derinimą ir tai, kaip jos viena kitą įtakoja. Per didelis dėmesys vienai kategorijai, o tuo pačiu per mažas kitai, gali padaryti, organizacijai kurtą, daug investicijų ir laiko pareikalavusią, informacijos apsaugos programą – beverte. Todėl labai svarbu šių kategorijų detalizavimas, o taip pat teisingas dėmesio ir resursų paskirstymas.

Valdymo kategorija, kuriant informacijos apsaugos sistema, sudaro:

- *Informacinių technologijų saugumo programos vystymas.* Tai bendras visos saugumo programos kūrimo vaizdas ir jo koregavimas atsižvelgiant į jau minėtas valdymo, operacijų ir technines kategorijas. Procesų planavimas, koordinavimas ir kontroliavimas. Ne tik pačios sistemos diegimas, bet taip pat ir darbuotojų apmokymas. Išorinių ekspertų sistemos įvertinimas ar audito atlikimas. Atliekamų operacijų rizikos ir organizacijos valdomo turto įvertinimas ir atitinkamo saugumo lygio nustatymas. Sistemos saugumo ir incidentų valdymo plano sukūrimas.

- *Informacinių technologijų saugumo politikos kūrimas.* Politika skirstoma į programos, specifinių problemų ir specialios sistemos politikas. Programos politika - tai organizacijos kuriamos apsaugos programos politika, kuri numato programos apimtį ir kompetenciją, nustato jos įgyvendinimo atsakomybių ribas, kuria strategiją ir nurodo pagrindinę veiklos kryptį, o taip pat paskirsto organizacijos išteklius reikalingus programos įgyvendinimui. Specifiniu problemų politika - elgsena susidūrus su tokiomis nenumatytomis problemomis kaip: įstatymų arba naujų taisyklių rizikos valdymui ar diegimui taikymas. Specialios sistemos politika - atskirų posistemių toje pačioje organizacijoje valdymas. Elgsenos, naudojantis jomis, apibrėžimas, procedūrų taikymas.
- *Rizikos valdymas.* Subalansuoti saugumo priemonių operacines ir rentabilumo išlaidas, o taip pat pasiekti gerų rezultatų saugant informaciją ir organizacijos informacinę sistemą.
- *Informacinių technologijų saugumo architektūrinis planavimas.* Ši sritis susijusi su strateginiu planavimu ir informacinių technologijų infrastruktūros vystymu, siekiant apsaugos programos tikslų. Saugumo architektūros žingsnis inicijuojamas po to, kai buvo atlikta saugumo poreikių analizė ir nustatyti reikalavimai sistemai. Remiasi ir tokiomis ankstesnėmis fazėmis kaip rizikos nustatymas ir informacijos apsaugos politikos suformuota strategija, jos uždaviniai.
- *Sertifikavimas ir akreditacija.* Akreditacija - oficialus pripažintos institucijos pareiškimas, jog sukurtoji sistema atitinka jai keliamus reikalavimus, bei yra pasirengusi efektyviai veikti numatytos rizikos aplinkoje, naudojantis esamomis valdymo, operacinėms ir techninėms priemonėms. Sertifikavimas - techninis akreditaciją palaikančios IT sistemos saugumo priemonių įvertinimas, kuris padeda nustatyti diegimo ir apsaugos priemonių taikymo lygį. Sertifikavimo kompleksiškumas ir griežtumas priklauso nuo organizacijos sistemos kritiškumo ir galimų nuostolių, informacijos jautrumo, sistemos sudėtingumo ir informacijos įvertinimo laipsnio. Išbandomas ir įvertinamas saugumas, paruošiamos saugumo įvertinimo rezultatų ataskaitos.
- *Informaciniu technologijų saugumo produkto vertinimas.* Sukurtos informacinės sistemos saugumą bandančių ir įvertinančių programų taikymas. Sekamas nuoseklus ir teisingas saugumo standartų taikymas. Padaromos saugumą įvertinančios išvados.

Operacine kategorija, kuriant informacijos apsaugos sistema, sudaro:

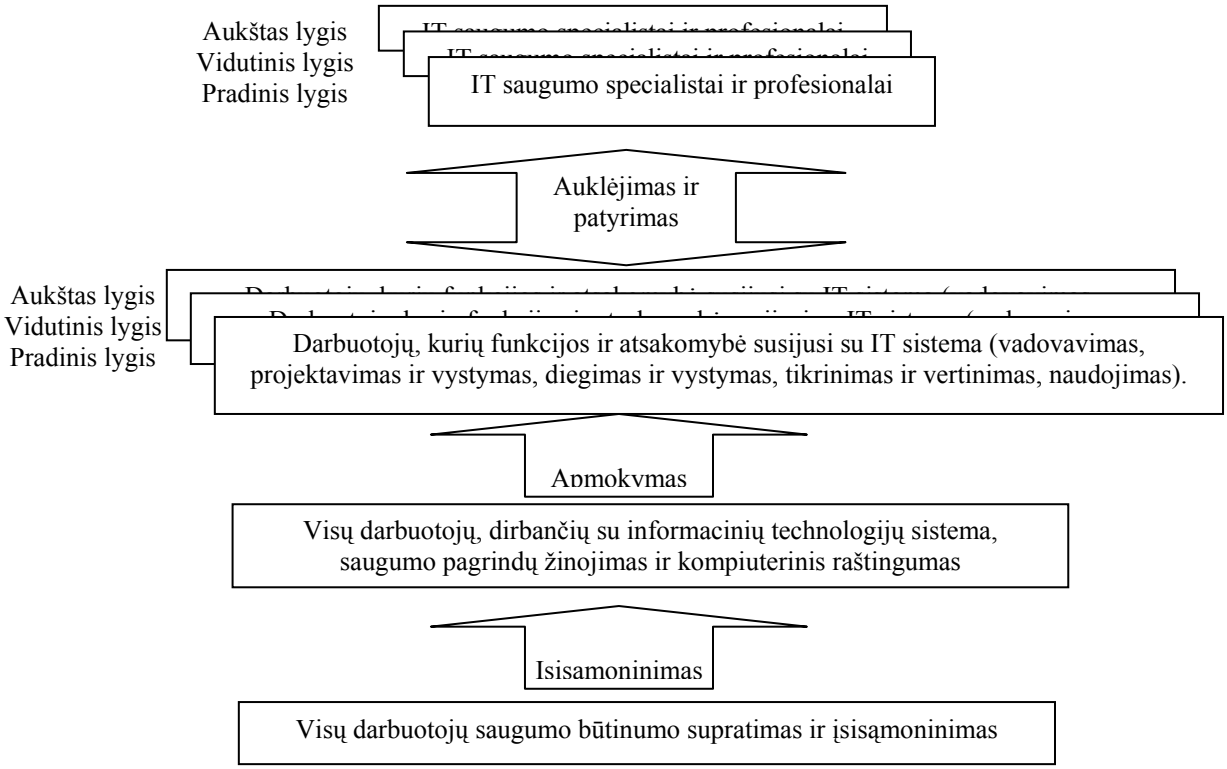
- *Nenumatytų atvejų planavimas.* Šis planavimas yra skirtas pasekmių, atsiradusių dėl informacijos ar sistemos dalies praradimo, sumažinimui. Organizacijos darbuotojai įgalinami efektyviai ir greitai atstatyti informacinių technologijų sistemos funkcijas, o taip pat ir duomenų srautą. Tokie atsarginiai planai apibrėžia procedūras, išteklius, užduotis

ir informaciją būtiną sprendžiant iškilusias problemas, siekiant grąžinti sistemą į pradinę būklę ir sumažinti nepageidaujamus padarinius. Gerai parengtas ir išbandytas sprendimo planas padeda užtikrinti darbo nepertraukiamumą ir pagalbą krizės metu. Todėl nenumatytų atvejų planas turėtų būti periodiškai peržiūrimas, papildomas ir iš naujo įvertinamas, kad objektyviai reprezentuotų esamą sistemos padėtį. Paprastai planą turi sudaryti penkių rūšių informacija: *palaikymo* (plano numatomų operacijų ir koncepcijų aprašymas), *pranešimo* (plano taikymo, žalos įvertinimo ir informavimo procedūrų numatymas), *atgavimo* (pirminės būsenos atstatymo procedūrų ir veiklų seka), *atkūrimo* (informacijos atkūrimo veiklų seka, sistemos išbandymas), *plano priedai* (kontaktai, įrangos sąrašas, sutartys ir kiti susiję planai).

- *Incidentų valdymas.* Ši sistemos dalis sudaro galimybę greitai ir efektyviai reaguoti į iškilusias saugumo problemas ar normalaus darbo sutrikimus, užkertant kelią tolimesniems įvykiams, kurie padarytų didesnę žalą. Norint sukurti naudingą informacijos apsaugos sistemą, būtina atsižvelgti į šešis pagrindinius tokios programos aspektus: pasiruošimą, incidentų atpažinimą, nepageidaujamų reiškinių sustabdymą, padarinių panaikinimą, sistemos darbo atkūrimą, o taip pat veiklos pratęsimą ir jos aktyvų stebėjimą. Svarbiausias šios dalies aspektas - pastovus budėjimas ir pasiruošimas neatidėliotinam reagavimui į situaciją.
- *Išbandymas.* Tai viena iš pačių svarbiausių sričių saugios sistemos kūrime. Be abejo, tai vienintelis būdas įsitikinti, kad kuriama sistema veikia taip, kaip tai numatyta, o taip pat ir būdas atrasti naujoms, dar nenumatytoms ir neapibrėžtoms problemoms. Bandymo rezultatai gali būti naudojami sistemos taisymui, lyginimui su analogiškais produktais ar diegiamos sistemos naudingumui įvertinti. Bandymo metu gali būti samdoma trečioji šalis, kuri gavusi nurodymus iš sistemos savininkų, bandytų sistemos pažeidžiamumą, patekimo į ją galimybę, slaptažodžių patikimumą ir virusinį atsparumą.
- *Apmokymai.* Tai kitą gyvybiškai svarbi sritis kuriant saugią sistemą. Net turint geriausią naujausią apsaugos sistemą neįmanoma išsiversti be patikimo ir kvalifikuoto personalo. Jei organizacijos darbuotojai nesugebės pasinaudoti sistemos suteikiamais privalumais, tai investicijos į šią sistemą ne tik virs nuostoliais, bet ir taps trukdžiu darbe. Svarbus vadovų supratimas ir teisingas požiūris į šią fazę. Jie turi ją inicijuoti ir investuoti į darbuotojų kvalifikacijos kėlimą. Mokymasis turėtų vykti nuosekliai (8 Schema). Tokia organizacijos darbuotojų apmokymo sistema sukuria ir palaiko IT sistemos saugumą, padeda išvengti nesusipratimų, ženkliai sumažina galimybę prarasti informaciją dėl žmogiškojo faktoriaus įtakos sistemos veikloje. Mokymo sistemos kūrimas ir diegimas organizacijoje neabejotinai gyvybiškai svarbus žingsnis, kuris ne tik padidina

informacijos saugumą organizacijoje, tačiau ir padaro ją nepriklausoma nuo išorinio poveikio ar trečiųjų asmenų.

8 Schema. Informacinių technologijų saugumo testinio mokymo modelis[49]



Technine kategoriją, kuriant informacijos apsaugos sistemą, sudaro:

- *Ugniasienės.* Tai klasikinis sprendimas padedantis atskirti du tinklus. Paprastai tai būna vidinis organizacijos tinklas ir išorinis - Internetas. Šis techninis ir programinis apsaugos būdas nuo įsibrovimo į sistemą tuo pačiu padeda kontroliuoti „įeinančius" ir „išeinančius" duomenų srautus. Taip pat galimi įvairūs sprendimo variantai - keleto ugniasienių apjungimas, tinklų išskirstymas ir apsaugos priemonių derinimas.
- *Įsibrovimų aptikimas.* Tai pasyvus apsaugos elementas, kuris reaguoja į bandymus pažeisti sistemos vientisumą ir slaptumą, o taip pat į neleistinus ir nenumatytus duomenų ar kitų resursų priėjimo būdus. Informacija apie tokio tipo įvykius patenka darbuotojams atsakingiems už sistemos saugumo, o jie padaro išvadas ir nusprendžia tolimesnę veiksmų seką (Dažnai tai numatoma instrukcijomis). Šis sistemos elementas taip pat užsiima sistemos ir vartotojų darbo leistinumo, sistemos vientisumo ir pažeidžiamumo stebėjimu,

[49] Grance T., Hash J., Stevens M. etc. Guide to information technology security services. 2003 October, United States of America // http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf; prisijungimo laikas: 2006-03-23

priešinasi žinomų užpuolimų formoms, o taip pat fiksuoja ir analizuoja nesuprantamą sistemos darbą, paruošia ir perduoda veiklos ataskaitas sistemos saugumo prižiūrėtojams. Norint užtikrinti efektyvų darbą, būtina dažnai ir periodiškai atnaujinti įsibrovimo aptikimo programų duomenų bazes.

- *Viešųjų raktų infrastruktūra.* Tai technologijos, paslaugos, procedūrų, politikos ir darbuotojų sudaroma galimybė saugiai bendrauti esant skirtingose vietose. Šios techninės saugumo sistemos taikymas užtikrina siuntėjo ir gavėjo autentiškumą bei tikrumą, o taip pat ir perduodamos informacijos vientisumą. Taip pat palengvina kontrolės procesus organizacijoje -informacijos perdavimo procesų patikrinimą/atkūrimą ir vartotojo identifikavimą.

2.4 Informacijos apsaugos priemonės ir jų taikymas.

Kompiuterinei informacijai apsaugoti organizacijos imamasi įvairių priemonių, kurios padeda visapusiškai vertinti situaciją, kurioje yra organizacija, o taip pat kurti individualią apsaugos programą atsižvelgiant į kilsiančias grėsmes. Dažnai šios priemonės klasifikuojamos pagal jų taikymo pobūdį[50] [29, 47]:

- *Administracinis ir organizacinis saugumas.* Tai priemonė, kurios pagrindinis elementas ir yra saugumo politikos vystymas, bei būdų jai efektyviai įgyvendinti sukūrimas. Šiomis priemonėmis įvertinama galima rizika, paskirstomos atsakomybės ribos ir privilegijos, o taip pat numatomos vartotojų tapatybės nustatymo procedūros. Nenumatytiems atvejams paruošiami veiklos planai.
- *Personalo saugumas.* Tai personalo saugumo programos sudarymas, kuri apima ir išorines, ir vidines grėsmes. Asmenų identifikavimas ir hierarchijos, priėjimui prie saugomos informacijos, nustatymas. Nuosavo personalo elgesys vertinamas pagal priėjimo prie kompiuterinių sistemų tipą, išsilavinimo lygį ir galimus pažeidėjo motyvus.
- *Fizinė informacijos prieigų apsauga.* Tai ne tik pačių kompiuterių ar archyvų, bet ir darbo patalpų, priėjimo prie terminalų ir darbuotojų darbo vietų apsauga. Gali būti diegiamos įvairios apsaugos priemonės: nuo spynų ar grotų iki kortelių sistemų ir atspaudų skenerių. Taip pat įvairios paskirties signalizacijos sistemos.
- *Programinės įrangos saugumas.* Įvairūs programinės įrangos ir duomenų apsaugos

[50] Čėsna R., Štitilis D. Kompiuterinės informacijos ir elektroninių dokumentų apsauga viešajame administravime. Vilnius: Lietuvos teisės akademija, 2000.

mechanizmai, kuriais apsunkinamas informacijos grobimas ir programinės įrangos gadinimas. Šios priemonės apima duomenų šifravimą, programinį duomenų paketų skenavimą, prisijungimo prie operacinių sistemų ir patekimo į serverį procedūrų slaptažodžių taikymą, o taip pat kitos žalingo kodo programų ieškančias ir naikinančias priemones.

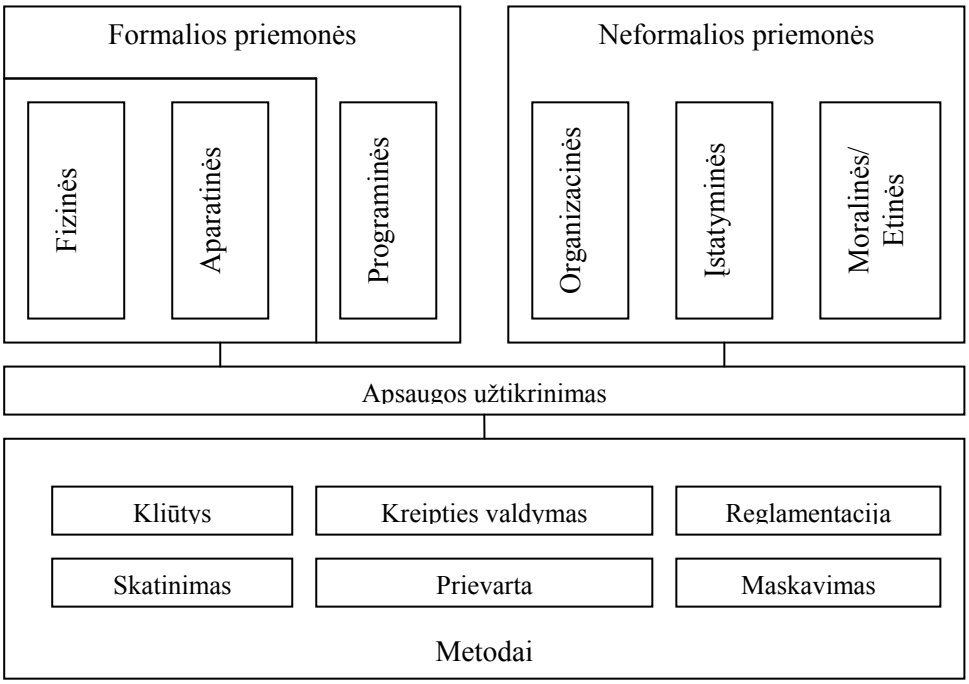
- *Operacijų saugumas*. Paprastai galima skirti du operacijų saugumo užtikrinimo būdus – vartotojų informavimo apie galimas grėsmes ir trukdymo nusikaltėliams daryti žalą. Pirmasis skatina darbuotojų apmokymus, kad informacijos apsauga natūraliai jiems rūpėtų, o esant reikalui, darbuotojai galėtų atpažinti nusikalstamą veiklą. Antrasis apima kontroliavimą ir įspėjančių sistemų diegimą.

Be abejo, būtina suprasti, jog vienos iš apsaugos priemonių taikymas, negali užtikrinti informacijos apsaugos organizacijoje. Geriausias sprendimas – jų tarpusavio derinimas. Taip sukuriama papildoma apsaugos sistemos vertė - savotiškas sinergijos efektas.

Galima atskirai klasifikuoti apsaugos metodus ir priemones. Toks išskaidymas leidžia numatyti atskirus apsaugos sistemoje taikomus metodus, kurių pagalba stiprinama informacijos apsauga. Šiame modelyje šiek tiek pakeičiamas ir apsaugos priemonių taikymas. Jos skiriamos į formalias ir neformalias. Formalias sudaro techninės (fizinės ir aparatinės) ir programinės priemonės. Prie neformaliųjų skiriamos organizacinės, įstatyminės, o taip pat moralinės-etinės informacijos apsaugos priemonės.

Fizinės, programinės ir organizacinės priemonės tiksliai atitinka anksčiau minėtąsias (9 Schema). Joms priskiriami informacijos apsaugos metodai: kliūtys (fizinių kliūčių sudarymas), kreipties valdymas (tiek fizinis, tiek programinis priėjimo prie resursų ribojimas, o taip pat ir organizacinių elementų vykdymas – privilegijų nustatymas), maskavimas (kriptografijos taikymas) ir reglamentacija (specialių priemonių kūrimas ir diegimas, pvz.: aparatūros išdėstymas arba pastato konstrukcija). Moralinės ir etinės priemonės dalinai atitinka anksčiau minėtą personalo ir procesų saugumą. Šių priemonių metodas – skatinimas (darbuotojų motyvavimas, bendros organizacijos kultūros sukūrimas). Ankstesniame klasifikavime visiškai neminėtos priemonės – įstatyminės. Jų taikomas metodas – prievarta (grasinimas nuobaudomis).

9 Schema. Informacijos apsaugos metodų ir priemonių klasifikacija[51]



Informacijos apsaugos priemonių taikymas tiesiogiai priklauso nuo organizacijos vystomos informacijos apsaugos politikos. Tai, kaip organizacija vertina savo informaciją ir jos slaptumą, parodoma investicijomis į informacijos apsaugos sistemos kūrimą ir taikymą. Labai svarbu tinkamai pasirinkti apsaugos priemones, kad investicijos nebūtų beprasmės arba nuostolingos.

[51] Jastramskas V. Informacijos apsaugos pagrindai. Kaunas: Technologija, 1999.

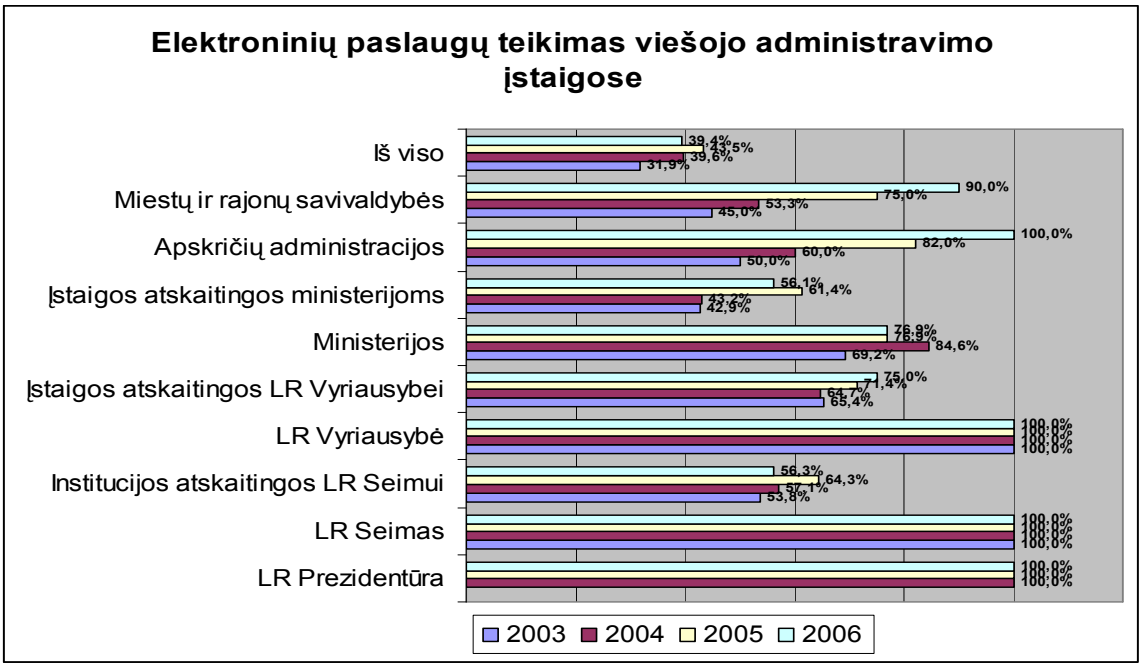
3. INFORMACIJOS SAUGUMO LIETUVOS E.VALDŽIOS SISTEMOJE TYRIMAS

3.1 Elektronines paslaugas teikiančios institucijos ir informacijos sauga

Lietuvos Statistikos departamento prie Lietuvos Respublikos Vyriausybės leidinyje „Informacinės technologijos Lietuvoje 2006“ pateikia statistinius duomenis apie informacines technologijas valstybės ir savivaldybių viešojo administravimo įstaigose, elektroninių paslaugų prieinamumą ir populiarumą, informacijos saugą.

Statistikos departamento duomenimis, 2006 metų pradžioje 39,4% valstybės ir savivaldybių viešojo administravimo įstaigų (tai būtų apie 70,1% visų turinčių Interneto svetaines įstaigų) teikė viešojo administravimo paslaugas Internetu[52] [42, 36]. Tačiau šis skaičius yra šiek tiek mažesnis nei 2005 metų pradžioje, kai elektronines viešąsias paslaugas teikė 43,5% (1 Diagrama).

1Diagrama. Elektroninių paslaugų teikimas viešojo administravimo įstaigose



Ypatingai didelis viešųjų elektroninių paslaugų pasiūlos augimas pastebimas apskričių administracijų, o taip pat ir miestų, bei rajonų savivaldybių sektoriuje: nuo 2003 iki 2006 metų

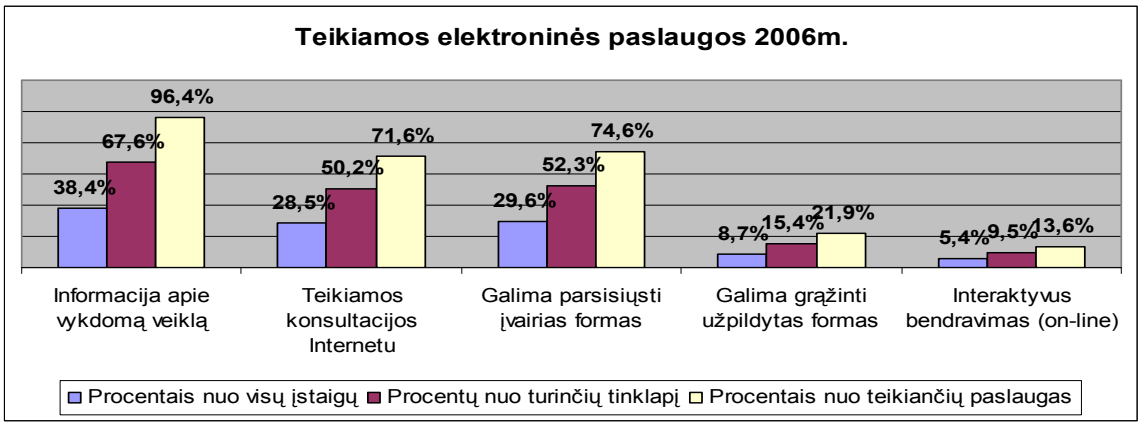
[52] Lietuvos Statistikos departamentas prie LR Vyriausybės. Informacinės technologijos 2006. Vilnius, 2006.

šiuose sektoriuose teikiamų viešųjų elektroninių paslaugų padaugėjo 45-50%. Šiek tiek mažesnis pasiūlos augimas institucijų bei įstaigų atskaitingų Seimui, Vyriausybei ir ministerijoms, sektoriuje (10-15%).

Informacinės plėtros komiteto prie Lietuvos Respublikos Vyriausybės pateiktais duomenimis, bendras viešųjų elektroninių paslaugų pasiekiamumo lygis 2005 metais buvo 64,6% (2004 metais jis siekė 49,2%). Piliečiams teikiamų elektroninių viešųjų paslaugų vidurkis 2005 metais buvo 56,6% (2004m. – 43,6%). Verslo subjektams teikiamų elektroninių viešųjų paslaugų vidurkis 2005 metais buvo 76,1% (2004m. – 59,7%). Lietuvos Statistikos departamento duomenimis, 2005 metais 10% Lietuvos gyventojų naudojosi elektroninės valdžios paslaugomis (ES vidurkis 2005 metais – 23%). Tarp verslo atstovų elektroninės valdžios paslaugos daug populiaresnės – 2005 metais 72% įmonių jomis pasinaudojo (ES vidurkis 2005 metais – 57%)[53] [42, 43].

Retai galima pasinaudoti aukštesnio lygmens elektroninėmis paslaugomis, pavyzdžiui: parsisiųstas ir užpildytas elektronines formas grąžinti jas pateikiančiai institucijai. Parsisiųsti įvairias elektronines formas leidžia 29,6% visų viešojo administravimo įstaigų (74,6% visų teikiančių elektronines paslaugas įstaigų), tačiau tik 8,7% įstaigų galima grąžinti užpildytas elektronines formas (21,9%) (2 Diagrama).

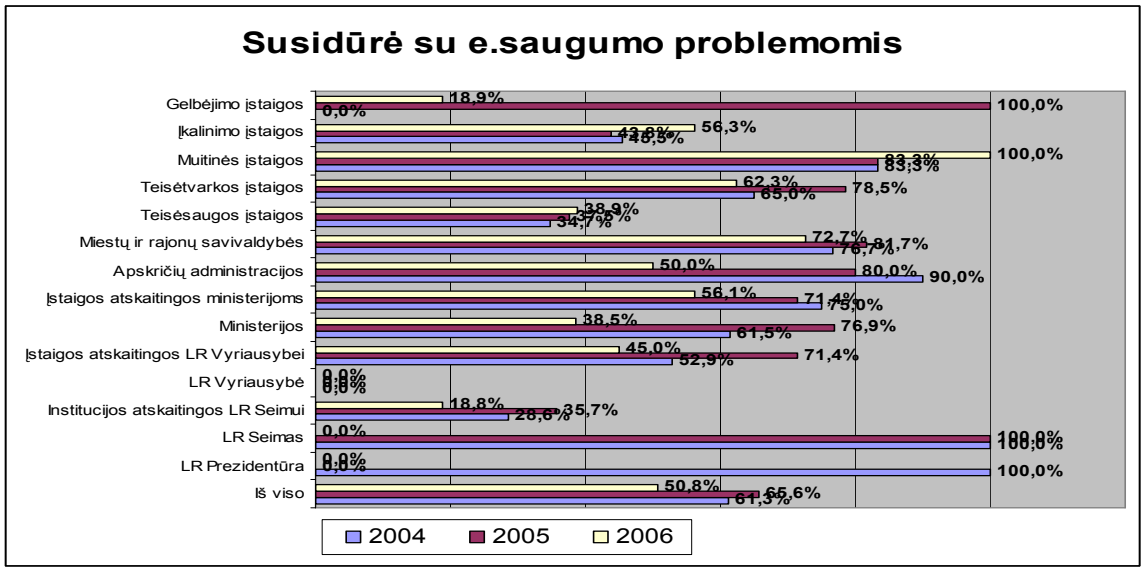
2 Diagrama. Teikiamos elektroninės paslaugos 2006 metais



Be abejo, nedidelis aukšto lygmens viešųjų elektroninių paslaugų ir vartotojų skaičius yra glaudžiai susijęs su informacijos saugumo užtikrinimo klausimu. Net 14,4% apklaustųjų, kurie naudoja Internetą, bet nesinaudoja elektroninės valdžios paslaugomis, pabrėžė, jog nerimauja dėl jų pateikiamų duomenų saugumo[54] [42, 45]. 50,8% įstaigų susidūrė su elektroninio saugumo problemomis per 2006 metus (3 Diagrama).

[53] Lietuvos Statistikos departamentas prie LR Vyriausybės. Informacinės technologijos 2006. Vilnius, 2006.
[54] Lietuvos Statistikos departamentas prie LR Vyriausybės. Informacinės technologijos 2006. Vilnius, 2006.

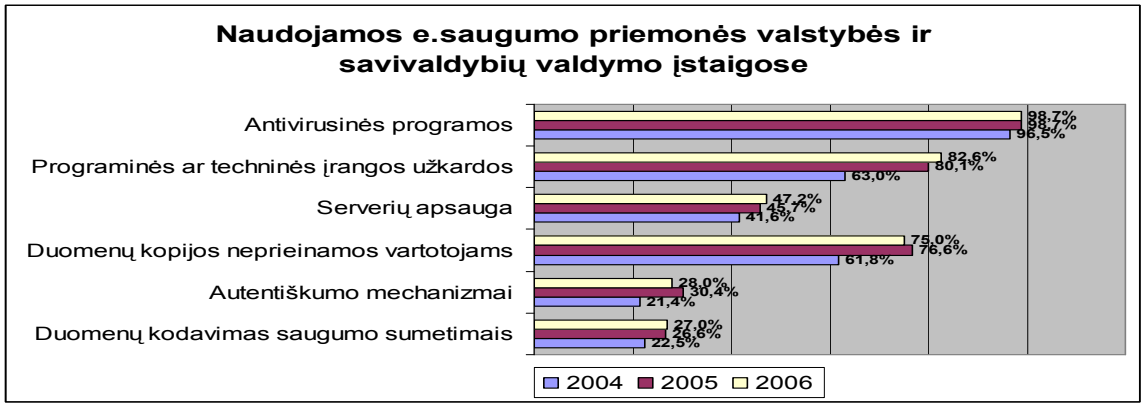
3 Diagrama. Susidūrė su e.saugumo problemomis



Tolygiai augant naudojamų elektroninio saugumo priemonių naudojimui (4 Diagrama), laipsniškai kasmet sumažėja ir incidentų valstybinėse įstaigose skaičius. Tačiau atsižvelgiant į 2005 metais Lietuvos Statistikos departamento pateikiamus duomenis apie elektroninio saugumo priemonių atnaujinimą bent kartą per tris mėnesius (beveik visos valstybinės įstaigos atnaujino apsaugos priemones – bendras vidurkis 90-95%), stebina gana didelis saugumo incidentų 2005 metais skaičius (3 Diagrama). Tai dar kartą patvirtina ir leidžia daryti prielaidą, jog informacijos sauga negali apsiriboti techninių ar programinių priemonių diegimu ir atnaujinimu.

Tarp valstybės ir savivaldybių valdymo įstaigose naudojamų elektroninio saugumo priemonių populiariausios yra įprastos antivirusinės programos, programinės ar techninės prieigos užkardos ir atsarginių duomenų kopijų, nepasiekiamų vartotojui, darymas (4 Diagrama). Šios saugumo priemonės patrauklios savo santykiniu pigumu ir paprastumu, tačiau jos neužtikrina aukštesnio lygmens saugumo. Tai akivaizdžiai iliustruoja informacijos saugumo incidentų skaičius.

4 Diagrama. Naudojamos elektroninio saugumo priemonės valstybės ir savivaldybių įstaigose



Pateikti statistiniai duomenys dar kartą akivaizdžiai parodo, jog elektroninio saugumo priemonių diegimas ir atnaujinimas yra gyvybiškai svarbus informacinės sistemos elementas, tuo labiau, kai kalbame apie svarbią valstybinio pobūdžio informaciją ar asmens duomenis.

3.2 Informacijos saugos aspektus reglamentuojantys Lietuvos Respublikos teisės aktai

1997 metais Lietuvos Respublikos Vyriausybės priimtas nutarimas „Dėl duomenų saugos valstybės ir vietos savivaldos informacinėse sistemose“[55] [8]. Čia pirmą kartą mėginama reglamentuoti informacinės sistemos sąvoka, duomenų perdavimo saugumas, pateikiami rekomenduojamieji standartai saugumo priemonių reikalavimams sudaryti (juose minimi tyčiniai arba netyčiniai duomenų pažeidimo rizikos veiksniai). Taip pat čia pateikiama duomenų apsaugos įgyvendinimo tvarka ir priemonės (techninė, programinė, duomenų bazių, patalpų apsauga ir kt.).

2000 metais priimtas, o 2002 pataisytas elektroninio parašo įstatymas – vienas iš pirmųjų žingsnių tobulesnės informacijos saugos link[56] [1]. Teisiškai reglamentavus šio svarbaus elemento naudojimą buvo sukurta galimybė saugiau perduoti informaciją, ji įgijo teisinio svorio.

2001 priimta Lietuvos Vyriausybės nutarimu priimta, o 2003 metais papildyta informacijos technologijų saugos valstybinė strategija ir jos įgyvendinimo planas[57] [11]. Čia pirmą kartą pamėginama apibrėžti terminą „Informacijos technologijų sauga“ kaip siekimą išvengti arba sušvelninti pavojus prarasti, paviešinti ar pakeisti informaciją. Apibrėžimas labai bendro pobūdžio, tiksliai nereglamentuojantis nei paties termino, nei grėsmių. Tarp svarbiausių strategijos tikslų minima įvairių sričių saugos reikalavimų nustatymai ir kontrolės užtikrinimas. Priemonių plane numatomas SVDPT tinklo kūrimas, valstybinių institucijų IT saugos vertinimas, IT saugos standartų rengimas, saugos planų ir specialistų rengimas, vertinimas.

2002 metais Lietuvos Respublikos Vyriausybės nutarimu patvirtinta elektroninė valdžios koncepcija. Joje atsižvelgiama į Europos politinę iniciatyvą dėl e.valdžios: „užtikrinti informacinių technologijų saugumą, kai viešosioms paslaugoms teikti naudojamos skaitmeninės

[55] Lietuvos Respublikos Vyriausybės nutarimas „Dėl duomenų apsaugos valstybės ir vietos savivaldos informacinėse sistemose“. 1997-09-04 Nr. 952 // http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=42817&p_query=&p_tr2=; prisijungimo laikas: 2006-10-12

[56] Lietuvos Respublikos elektroninio parašo įstatymas. 2000-07-11 Nr.VIII-1822// http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=169880; prisijungimo laikas: 2006-10-12

[57] Lietuvos Respublikos Vyriausybės nutarimas „Dėl informacinių technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo“. 2001-12-22 Nr. 1625 // http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=215825&p_query=&p_tr2=; prisijungimo laikas: 2006-10-12

technologijos“[58] [16]. Šioje koncepcijoje pabrėžiama, jog gyventojų pasitikėjimą elektroninės valdžios paslaugomis galima gauti tik užtikrinus informacinių sistemų saugumą: „E. valdžios projektai galės funkcionuoti, kai bus užtikrinta informacinių technologijų ir telekomunikacijų sauga, gyventojų interesų teisinė apsauga valstybės informacinėse sistemose“.

2003 metais Lietuvos Respublikos Vidaus reikalų ministerijos vadovo įsakymu patvirtinti tipiniai duomenų saugos nuostatai[59] [7]. Šie nuostatai reglamentuoja automatizuotą duomenų apdorojimą informacinėje sistemoje, o taip pat ir duomenų saugos organizavimą, bei nenumatytų situacijų valdymą (sistemos tvarkytojo ir saugos įgaliotinio veiklą). Numatomas darbo su duomenimis taisyklių, kurias teikia saugos įgaliotinis, apimamas turinys: techninės, programinės ir fizinės duomenų apsaugos priemonės (tinklų sauga, duomenų šifravimas, fizinės ir programinės saugos priemonės), prieinamumo principai ir kontrolė (vartotojų atžvilgiu), vientisumo stebėjimas ir duomenų atkūrimas, saugaus duomenų teikimo ar perkėlimo tvarka.

2003 metais priimtas valstybės ir tarnybos paslapčių įstatymas reglamentuoja automatinių duomenų apdorojimo sistemų ir tinklų, o taip pat ir įslaptintos informacijos perdavimo tais tinklais saugumo reikalavimus[60] [3].

2003 metais Lietuvos Respublikos Vidaus reikalų ministerijos vadovo įsakymu buvo patvirtintos informacijos klasifikavimo pagal duomenų grupes rekomendacijos[61] [4]. Dokumente reglamentuojamos duomenų savybės naudojamos informacijos saugai apibrėžti (vientisumas, prieinamumas, konfidencialumas), o taip pat aprašomos informacinių sistemų kategorijos.

2004 metais buvo priimtas Lietuvos Respublikos elektroninių ryšių įstatymas, kurio pagrindinis tikslas buvo reglamentuoti „visuomeninius santykius, susijusius su elektroninių ryšių paslaugomis, tinklais ir su jais susijusiomis priemonėmis bei paslaugomis, elektroninių ryšių išteklių naudojimu, taip pat visuomeninius santykius, susijusius su radijo įrenginiais, galiniais įrenginiais ir elektromagnetiniu suderinamumu.“[62] [2]

---

[58] Lietuvos Respublikos Vyriausybės nutarimas „Dėl elektroninės valdžios koncepcijos patvirtinimo“. 2002-12-31 Nr. 2115 // http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=198184&p_query=&p_tr2=; prisijungimo laikas: 2006-10-12

[59] Lietuvos Respublikos Vidaus reikalų ministro įsakymas „Dėl tipinių duomenų saugos nuostatų patvirtinimo“. 2003-07-16 Nr. 1V-272 // http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=216052&p_query=&p_tr2=; prisijungimo laikas: 2006-10-12

[60] Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo pakeitimo įstatymas. 2003-12-16 Nr. IX-1908 // http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=224465&p_query=&p_tr2=; prisijungimo laikas: 2006-10-12

[61] Lietuvos Respublikos Vidaus reikalų ministro įsakymas „Dėl informacijos klasifikavimo pagal duomenų grupes rekomendacijų patvirtinimo“. 2003-01-27 Nr. 1V-33 // http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=216170&p_query=&p_tr2=; prisijungimo laikas: 2006-10-12

[62] Lietuvos Respublikos elektroninių ryšių įstatymas. 2004-04-15 Nr. IX-2135 // http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=232036&p_query=&p_tr2=; prisijungimo laikas: 2006-10-12

Tačiau šis įstatymas nėra tiesiogiai orientuotas į tinklų ir informacijos saugą – jo reguliuojamos radijo, telefono, televizijos ir kitos elektroninės infrastruktūros. Artimiausias informacijos saugai šio įstatymo straipsnis teigia, jog „Viešųjų elektroninių ryšių paslaugų teikėjai privalo įgyvendinti tinkamas technines ir organizacines priemones savo teikiamų paslaugų saugumui užtikrinti, o prireikus - kartu su viešųjų ryšių tinklų teikėjais imtis tokių pat priemonių viešųjų ryšių tinklų saugumui užtikrinti. Šios priemonės turi užtikrinti iškilusią grėsmę atitinkantį saugumo lygį. Iškilus ypatingai elektroninių ryšių tinklo ar jo dalies saugumo pažeidimo grėsmei, viešųjų elektroninių ryšių paslaugų teikėjas privalo informuoti abonentus apie tokią grėsmę ir tais atvejais, kai paslaugų teikėjo taikomos priemonės nepanaikina grėsmės kilmės priežasčių, taip pat informuoti abonentus apie visas įmanomas gelbėjimo priemones ir nurodyti tikėtinas jų kainas.“[63] [2]. Tačiau šiuo straipsniu tik bendrai liepiama imtis apsaugos priemonių, o jos turėtų būti konkrečios ir privalomos atsižvelgiant į būtiną saugumo lygį. Be to, nekalba apie elektroninių paslaugų teikėjus ar kitus, su pačios elektroninių ryšių infrastruktūros kūrimu nesusijusius subjektus.

Įstatymas taip pat reglamentuoja ir ryšio slaptumą: „Asmenims, kurie nėra faktiniai elektroninių ryšių paslaugų naudotojai, be suinteresuotų faktinių elektroninių ryšių paslaugų naudotojų sutikimo draudžiama atskleisti elektroninių ryšių tinklais perduodamos informacijos turinį ir (ar) susijusius srauto duomenis arba sudaryti sąlygas sužinoti tokią informaciją ir (ar) susijusius srauto duomenis. Ne faktiniams elektroninių ryšių paslaugų naudotojams draudžiama be atitinkamų faktinių elektroninių ryšių paslaugų naudotojų sutikimo klausytis, įrašyti, kaupti ar kitu būdu perimti informaciją ar susijusius srauto duomenis ar su tokia informacija bei susijusiais srauto duomenimis slapta susipažinti“[64] [2].

2004 metais Lietuvos Respublikos Vidaus reikalų ministerijos vadovo įsakymu buvo patvirtinta informacinių technologijų saugos atitikties vertinimo metodika[65]. Joje reglamentuojama informacinių sistemų vertinimo metodika ir kriterijai. Taip pat buvo patvirtintos Interneto tarnybinių stočių apsaugos rekomendacijos[66] [6]. Jose reglamentuojamas techninės ir programinės įrangos planavimas, vartotojų tapatybės nustatymas ir saugos priemonių naudojimas (kopijos, programinė apsauga, nuotolinės ir fizinės prieigos valdymas).

---

[63] Tas pats įstatymas, 62 straipsnis.

[64] Lietuvos Respublikos elektroninių ryšių įstatymas. 2004-04-15 Nr. IX-2135 // http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=232036&p_query=&p_tr2=; prisijungimo laikas: 2006-10-12

[65] Lietuvos Respublikos Vidaus reikalų ministro įsakymas „Dėl informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“. 2004-05-06 Nr. 1V-156 // http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=233268&p_query=&p_tr2=; prisijungimo laikas: 2006-10-12

[66] Lietuvos Respublikos Vidaus reikalų ministro įsakymas „Dėl Interneto tarnybinių stočių apsaugos rekomendacijų patvirtinimo“. 2004-05-21 Nr. 1V-176 // http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=234012&p_query=&p_tr2=; prisijungimo laikas: 2006-10-12

2004 metais Lietuvos Respublikos Vyriausybės nutarimu priimtos valstybės informacinių sistemų steigimo ir įteisinimo taisyklės[67] [12]. Jos įpareigoja valstybinių informacinių sistemų steigėjus paruošti informacinės sistemos duomenų saugos nuostatus.

2004 metais LR Vyriausybės patvirtinta, o 2006 metais atnaujinta viešojo administravimo plėtros iki 2010 metų strategija[68] [13]. Joje teigiama, jog tam, „kad viešąsias paslaugas būtų galima teikti Internetu trečiuoju ir ketvirtuoju lygiu, reikia išspręsti fizinių ir juridinių asmenų identifikavimo valstybės informacinėse sistemose problemą, užtikrinti asmens duomenų teisinę apsaugą ir tai, kad administruojama viešoji paslauga būtų suteikiama tik tam asmeniui, kuriam ji skirta. Visi šie klausimai bus sprendžiami pagal fizinių ir juridinių asmenų tapatybės nustatymo valstybės informacinėse sistemose koncepciją, kurią pateikti tvirtinti Lietuvos Respublikos Vyriausybei numatyta Elektroninės valdžios koncepcijos įgyvendinimo priemonių plane“. Tame pačiame dokumente pateikiamoje SSGG (stiprybių, silpnybių, galimybių, grėsmių) analizėje teigiama, jog silpnybės neleidžiančios toliau vystyti sistemos yra infrastruktūros trūkumai: „Nėra elektroninio parašo sertifikavimo paslaugų teikėjų, nes tam reikėtų daug investicijų; Neveikiantis elektroninis parašas labai riboja viešųjų paslaugų teikimą elektroniniu būdu; Nepatvirtinta fizinių ir juridinių asmenų tapatybės nustatymo valstybės informacinėse sistemose koncepcija“. Viena iš analizėje minimų grėsmių – „Nepakankamai moderni Valstybės tarnautojų registro apsauga gali sudaryti galimybes duomenims nutekėti“. Šiuo dokumentu skatinamas tolimesnis teisinis saugos reglamentavimas, infrastruktūros vystymas. Mėnesiu vėliau priimtas šios strategijos įgyvendinimo priemonių planas. Vienas iš šio plano tikslų – „Teikti viešąsias paslaugas naudojant saugias informacines technologijas“[69] [13].

2006 metais LR Vyriausybės nutarimu patvirtintas elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinės strategijos iki 2008 metų įgyvendinimo priemonių planas[70] [9]. Dokumente pateikiami pagrindiniai elektroninės informacijos saugos užtikrinimo principai, kurie savo turiniu yra labai panašūs į Ekonominio bendradarbiavimo ir

[67] Lietuvos Respublikos Vyriausybės nutarimas „Dėl valstybės informacinių sistemų ir įteisinimo taisyklių patvirtinimo“. 2004-04-19 Nr. 451 // http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=231255&p_query=&p_tr2=; prisijungimo laikas: 2006-10-12

[68] Lietuvos Respublikos Vyriausybės nutarimas „Dėl viešojo administravimo plėtros iki 2010 metų strategijos patvirtinimo“. 2004-04-28 Nr. 488 // http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=285917&p_query=&p_tr2=; prisijungimo laikas: 2006-10-12

[69] Lietuvos Respublikos Vyriausybės nutarimas „Dėl viešojo administravimo plėtros iki 2010 metų strategijos įgyvendinimo 2007-2010 metų priemonių plano patvirtinimo“. 2006-11-06 Nr. 1097 // http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=286022&p_query=&p_tr2=; prisijungimo laikas: 2006-10-12

[70] Lietuvos Respublikos Vyriausybės nutarimas „ Dėl elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinės strategijos iki 2008 metų ir jos įgyvendinimo priemonių plano patvirtinimo“. 2006-06-19 Nr. 601 // http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=278475&p_query=&p_tr2=; prisijungimo laikas: 2006-12-18

plėtros organizacija (OECD) pateikiamus saugumo kultūros kūrimo principus[71] [45] (aptarti 2.2 skyriuje).

Dabartinę situaciją vertinančios SSGG analizės skyriuje „silpnybės“ pabrėžiama, jog ne visos institucijos parengė saugos dokumentus, nėra sukurta efektyvi išankstinio perspėjimo ar kovos su nusikalstamomis veikomis sistema, neatliekamas nuolatinis saugos stebėjimas ir atnaujinimas, mažas SVDPT naudojamumas, trūksta kvalifikuoto personalo.

Dokumente pateikiami svarbūs strategijos tikslai: tobulinti informacijos saugos koordinavimą ir priežiūrą, elektroninės informacijos saugą reglamentuoti teisės aktais, kelti informacijos saugos kultūrą, skatinti informacijos saugos užtikrinimo projektų įgyvendinimą.

2005 metais Mykolo Romerio Universiteto pateikta projekto SAFARI tyrimo ataskaita yra puikus pagrindas kurti teisinius dokumentus reglamentuojančius informacijos saugą valstybinėse informacinėse sistemose[72] [44]. Joje detaliai išvardinami saugos užtikrinimo aspektai: institucijos saugos nuostatų (saugos tikslai, prioritetinės kryptys, duomenų svarbos skirstymas ir saugos priemonių parinkimas, rizikos vertinimo kriterijai, atsakomybė už pažeidimus) ir teisinės bazės parengimas (informacijos tvarkymo taisyklės, informacinės sistemos veiklos tęstinumo valdymo planas, naudotojų administravimo taisyklės).

Ataskaitoje taip pat smulkiai tiriamas elektroninės informacijos saugos organizavimas, saugos įgaliotinio skyrimas ir jo funkcijos, informacinių sistemų administratoriaus kompetenciją, naudotojų apmokymus.

Svarbiausios iš dokumente akcentuojamų sričių – rizikos vertinimas ir incidentų valdymas. Vertinamieji rizikos veiksniai, į kuriuos atsižvelgiama ruošiant rizikos vertinimo ataskaitą – subjektyvius netyčinius (tvarkymo klaidos, ištrynimas, programinės klaidos ar technologiniai sutrikimai), subjektyvius tyčinius (nesankcionuota prieiga, duomenų pakeitimas ar sunaikinimas, kiti elektroniniai nusikaltimai) ir „nenugalimą jėgą“ (angl. force majeure).

3.3 Elektroninės valdžios paslaugas teikiančių institucijų informacijos saugos tyrimas

Statistinių duomenų ir teorijos analize įrodžius informacijos saugos reikalingumą viešojo administravimo įstaigose, buvo stengiamasi praktiškai išsiaiškinti esamą informacijos saugos lygmenį elektronines viešąsias paslaugas teikiančiose institucijose.

[71] Organization for economic co-operation and development. Guidelines for the security of information systems and networks. Towards the culture of security. 2002-07-25, Paris.// http://www.oecd.org/dataoecd/16/22/15582260.pdf; prisijungimo laikas: 2006-03-23

[72] Mykolo Romerio Universitetas. Projekto SAFARI tyrimo ataskaita. 2005.

Tyrimo tikslas: Informacijos saugos reglamentavimo ir taikymo užtikrinimas viešąsias elektronines paslaugas teikiančiose įstaigose.

Uždaviniai:

- Ištirti teikiamų viešųjų elektroninių paslaugų brandos lygmenis.
- Išanalizuoti institucijų taikomas informacijos saugos priemones ir jų pagrįstumą.
- Nustatyti ar taikomų informacijos saugos priemonių pakanka atsižvelgiant į teikiamų elektroninių paslaugų brandos lygmenį.

Tyrimo objektas: Viešojo administravimo įstaigų, teikiančių viešąsias elektronines paslaugas, informacijos saugos reglamentavimas ir užtikrinimas.

Tyrimo imtis: Remiantis 2002 metų Lietuvos Respublikos Vyriausybės nutarimu patvirtinta elektroninės valdžios koncepcija[73] [16] ir joje pateikiamomis viešosiomis elektroninėmis paslaugomis (12 paslaugų piliečiams ir 8 verslo atstovams) buvo atrinkta 17 viešojo administravimo institucijų, kurios teikia arba ateityje numato teikti anksčiau paminėtas viešąsias elektronines paslaugas.

Tyrimo metodas: Atlikta lyginamoji analizė. Atrinkus elektroninės valdžios koncepcijoje pateikiamų viešųjų elektroninių paslaugų vykdytojus, buvo atliekama esamos situacijos analizė nustatant šiuo metu teikiamų elektroninių paslaugų bandos lygmenis. Atsižvelgiant į tai, kurį paslaugos brandos lygmenį yra pasiekusi tam tikra teikiama paslauga, buvo tikrinamas informacijos saugos priemonių taikymas institucijoje, remiantis Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės pateikiamu elektroninių viešųjų paslaugų siekiamojo modelio aprašymu[74] [34, 105], kuris numato privalomas informacijos saugos priemones tam tikro brandos lygmens elektroninėms viešosioms paslaugoms (2 Lentelė). Tyrimo metu institucijos buvo suskirstytos į tris grupes pagal elektroninių paslaugų teikimą. Taip pat buvo tiriami šių institucijų pateikiami dokumentai reglamentuojantys informacijos saugą arba susiję su saugos priemonių taikymu. Tyrimo metu surinkta informacija analizuojama ir apibendrintai pateikiama lentelėse ir diagramose.

[73] Lietuvos Respublikos Seimo nutarimas „Dėl Elektroninės valdžios koncepcijos patvirtinimo“. 2002-12-31 Nr. 2115 // http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=198184; prisijungimo laikas: 2006-10-12

[74] Elektroninių viešųjų paslaugų siekiamo modelio aprašymas. IVPK prie LR Vyriausybės. // http://epp.ivpk.lt/epp/Dokumentai/IVPK_elmodelis_siekiamasV1.pdf; prisijungimo laikas: 2006-06-18

2 Lentelė. Informacijos saugumo lygmenų klasifikacija

	1 lygmuo	2 lygmuo	3 lygmuo
Duomenų šifravimas	X	X	
Serverio identifikavimas	X	X	
Vartotojo identifikavimas slaptažodžiu	X	X	
Vartotojo identifikavimas sertifikatu	X		
Duomenų bazės vientisumo užtikrinimas	X	X	X
Atsarginės kopijos	X	X	X
Ugniasienės	X	X	X
Organizacinės saugumo priemonės	X	X	X

Tyrimo eigoje buvo pasinaudota viešųjų elektroninių paslaugų brandos lygių klasifikacija, kurią siūlo Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės[75] [33] (3 Lentelė).

3 Lentelė. Brandos lygmenų aprašymas

Elektroninės viešosios paslaugos brandos lygmuo	**Brandos lygmens skyrimo reikalavimai**
Pirmas lygmuo – informacijos publikavimas.	Tam, kad institucija būtų laikoma teikiančia šią paslaugą, ji privalo savo Interneto puslapyje publikuoti informaciją, kuri yra būtina pradėti paslaugų, teikiamų šios viešojo administravimo institucijos, gavimo procesą.
Antrasis lygmuo – vienpusis interaktyvumas.	Šio brandumo lygmens paslaugas teikianti institucija ne tik pasirūpina informacijos publikavimu, tačiau taip pat pateikia vartotojams ir pildyti ir atspausdinti paruoštas elektronines formas, kurios reikalingos norint pradėti teikiamos paslaugos gavimo procesą.
Trečiasis lygmuo – dvipusis interaktyvumas.	Tai visiškai kito brandos lygmens paslauga, kuri jau kokybiškai skiriasi nuo ankstesniųjų. Galimas elektroninis bendravimas, elektroninių formų Internete užpildymas. Šiuo atveju vartotojo tapatybė turi būti nustatoma institucijos informacinėje sistemoje. Nepaisant elektroninio bendravimo, galutinė paslauga paprastai pateikiama ne elektronine forma.
Ketvirtasis lygmuo – transakcijos.	Tai baigtinė elektroninės valdžios paslauga, kuri apima pilna elektroninį paslaugos įvykdymą, apmokėjimą ar kitas

[75] Elektroninės viešosios paslaugos Lietuvoje. IVPK prie LR Vyriausybės. 2002-08-01 // http://www.ivpk.lt/main-aktual.php?cat=61&n=11; prisijungimo laikas: 2006-06-18

	operacijas. Tuo pačiu šis lygmuo reikalauja ne tik patikimo vartotojo tapatybės nustatymo, bet taip pat ir aukščiausio lygmens informacijos saugos priemonių.

Atliekant šią analizę, buvo tiriami viešųjų elektroninių paslaugų teikėjai. Lentelėse apibendrintai pateikiama informacija apie konkrečias elektronines paslaugas, jas teikiančias institucijas, tokių paslaugų brandos lygmenį, reikalaujamas informacijos saugos priemones.

4 Lentelė. Piliečiams skirtų elektroninių paslaugų analizė

Viešoji elektroninė paslauga	**Paslaugą teikianti institucija (Vykdytojai)**	**Brandumo ir saugumo lygmuo**	**Paslaugos specifika ir taikomos apsaugos priemones**
Pajamų deklaravimas	Valstybinė mokesčių inspekcija prie LR Finansų ministerijos http://deklaravimas.vmi.lt	4 lygmens paslauga 1 lygio saugumas	VMI elektroninio deklaravimo sistema – viena iš populiariausių ir žinomiausių elektroninių viešųjų paslaugų Lietuvoje. (veikia nuo 2004 metų). VMI skiria ypatingą dėmesį informacijos saugai teikiant e.paslaugas. Vartotojas privalo tapti elektroninės deklaravimo sistemos (EDS) vartotoju, o tai padaroma elektroninio banko, kuriuo naudojasi pilietis, pagalba (Arba raštu). VMI informacijos saugos strategijoje numatomos visos pirmam saugumo lygmens reikalaujamos saugumo priemonės (šifravimas, identifikavimas, kitos kombinuotos saugumo priemonės).
Laisvų darbo vietų paieška	Lietuvos darbo birža prie LR Socialinės apsaugos ir darbo ministerijos http://www.ldb.lt/	4 lygmens paslauga 2 lygio saugumas	Norint pasinaudoti šia viešąja elektronine paslauga būtina registracija puslapyje. Vartotojas identifikuojamas slaptažodžiu. Registruojantis piliečiui prašomas asmens kodas, o darbdaviui –

			juridinio asmens duomenys. Kitos informacijos saugos priemonės – serverio apsauga, duomenų bazės vientisumo užtikrinimas, kitos įprastinės saugos priemonės.
Socialinės kompensacijos	Savivaldybės, Socialinės apsaugos ir darbo ministerija http://www.sodra.lt/	2 lygmens paslauga 3 lygio saugumas	„Sodra“ rimtai ruošiasi socialinių paslaugų piliečiams perkėlimui į elektroninę terpę (Šiuo metu baigiamas projektas su Šiaulių savivaldybe). Valstybinio socialinio draudimo fondo valdybos patvirtintos informacijos saugumo nuostatos, parengtos remiantis ISO 19977 standartu, apima visas su informacijos sauga institucijoje susijusias sritis: numatomas infrastruktūros saugumas, informacinių sistemų kūrimas, saugos priemonių naudojimas. Tačiau šiuo metu su elektroninėmis paslaugomis susijęs informacijos saugumas yra 3 lygmens (pilnai pakankamas).
Asmens dokumentai	LR Vidaus reikalų ministerija http://www.migracija.lt/	2 lygmens paslauga (maks. – 3) 3 lygio saugumas	Paslauga nėra aukšto lygmens (informacija, formos), todėl naudojamos standartinės informacijos saugos priemonės: programinės ir organizacinės priemonės, duomenų kopijos, duomenų bazės sauga.
Automobilių registravimas	LR Vidaus reikalų ministerija http://www.regitra.lt/	3 lygmens paslauga 2 lygio saugumas	Institucija teikia nemažai skirtingos informacijos, bei formų, reikalingų paslaugų gavimui (jas galima pateikti elektroniniu būdu). Informacijos pateikimui naudojamas

			saugus protokolas. Institucija atlieka studiją dėl elektroninių paslaugų pilno įgyvendinimo (automobilių registravimo). Svarsto galimybę prisijungti prie SVDPT, kad galėtų saugiai naudotis G2G elektroninėmis paslaugomis.
Leidimai statyti pastatus	Valstybinė teritorijų planavimo ir statybos inspekcija prie Aplinkos ministerijos http://www.vtpsi.lt/	2 lygmens paslauga 3 lygio saugumas	Institucija teikia informaciją ir elektronines formas reikalingas pradėti paslaugos gavimo procesus, tačiau jų nepriima elektronine forma. Šiuo metu atliekamas projekto, pilnam elektroninių paslaugų teikimui, tvirtinimas. Šiuo metu naudojamos saugos priemonės – įprastinės.
Pranešimai policijai	Policijos departamentas prie Vidaus reikalų ministerijos http://www.policija.lt/	1 lygmens paslauga 3 lygio saugumas	Pateikiama tik informacija. Šiuo metu ruošiami informacijos saugos nuostatai. Numatomas vartotojų identifikavimas, tarnybinės stoties sauga. Planuojama nauja elektroninė paslauga – elektroninis prašymas leidimui turėti ginklą.
Leidinių, publikacijų paieška bibliotekose	LR Kultūros ministerija http://www.libis.lt/	4 lygmens paslauga 2 lygio saugumas	Puikiai on-line veikianti viešoji paslauga naudojanti vartotojo identifikavimą. Turi nacionalinės bibliotekos direktoriaus patvirtintus informacijos sistemos duomenų saugos nuostatus, kurie reglamentuoja nenumatytų situacijų valdymą, infrastruktūros saugos reikalavimus.
Gimimo ir	Savivaldybės civilinės	1 lygmens	Šiuo atveju pasirinktas Vilniaus

mirties liudijimai	metrikacijos skyrius http://www.vilniaus.lt/	paslauga 3 lygio saugumas	miestas. Pateikiama tik informacija šiuo klausimu. Kai kurie miestai kuria projektus šios elektroninės paslaugos teikimui. Šiuo metu informacijos apsauga standartinė.
Gyvenamosios vietos deklaracijos	LR Vidaus reikalų ministerija http://www.migracija.lt/	2 lygmens paslauga (maks. – 3) 3 lygio saugumas	Paslauga nėra aukšto lygmens (informacija, formos), todėl naudojamos standartinės informacijos saugos priemonės: programinės ir organizacinės priemonės, duomenų kopijos, duomenų bazės sauga.
Gydytojų konsultacijos ir registracija poliklinikoje	LR Sveikatos apsaugos ministerija http://www.sam.lt/ http://www.pylimas.lt/lt/	1,3 lygmens paslauga 2 lygio saugumas	Pateikiama informacija, o taip pat suteikiama galimybė registruotis konsultacijoms poliklinikoje (pvz: Centro poliklinika). Registracijai taikomas vartotojo identifikavimas. Atlikta eSveikatos galimybių studija.
Paraiškos mokytis, kelti kvalifikaciją	LR Švietimo ir mokslo ministerija http://www.lamabpo.lt/	3 lygmens paslauga 2 lygio saugumas	Teikiama informacija, pateikiamos ir priimamos užpildytos elektroninės formos. Naudojamas vartotojų identifikavimas, o taip pat ir įprastos saugos priemonės.

5 Lentelė. Verslo atstovams skirtų elektroninių paslaugų analizė

Viešoji elektroninė paslauga	**Paslaugą teikianti institucija**	**Brandumo ir saugumo lygmuo**	**Paslaugos specifika ir taikomos apsaugos priemones**
Įmonių mokesčiai	Valstybinė mokesčių inspekcija prie LR Finansų ministerijos http://deklaravimas.vmi.lt	4 lygmens paslauga 1 lygio saugumas	VMI skiria ypatingą dėmesį informacijos saugai teikiant e.paslaugas. Vartotojas privalo

Pridėtinės vertės mokesčiai	Valstybinė mokesčių inspekcija prie LR Finansų ministerijos http://deklaravimas.vmi.lt	4 lygmens paslauga 1 lygio saugumas	tapti elektroninės deklaravimo sistemos (EDS) vartotoju, o tai padaroma pateikus juridinio asmens duomenis, ir atvykus pasirašyti sutarties į AVMI. VMI informacijos saugos strategijoje numatomos visos pirmam saugumo lygmens reikalaujamos saugumo priemonės (šifravimas, identifikavimas, kitos kombinuotos saugumo priemonės).
Naujų įmonių registravimas	LR Teisingumo ministerija http://www.registrucentras.lt/	2 lygmens paslauga 3 lygio saugumas	Pateikiama informacija ir formos leidžiančios pradėti paslaugos gavimo procedūrą. Planuojamos aukštesnio brandos lygio paslaugos.
Duomenų suteikimas Statistikos departamentui	LR Vyriausybė http://www.stat.gov.lt/lt/	3 lygmens paslauga 2 lygio saugumas	Ši viešoji elektroninė paslauga sudaro galimybę teikti duomenis Statistikos departamentui. Tam vartotojas turi būti registruojamas sistemoje, o naudojimui – identifikuojamas slaptažodžiu. Naudojamas saugus protokolas. Pagirtinas aspektas – ID, o ne įmonės kodo naudojimas jungimuisi.
Viešieji pirkimai	LR Ūkio ministerija http://www.vpt.lt/	3 lygmens paslauga 2 lygio saugumas	Vartotojas gali prisijungti prie viešųjų pirkimų monitoringo sistemos. Tam jis yra identifikuojamas slaptažodžiu. Kuriamas aukštesnio lygio paslaugos projektas.

Socialinės išmokos darbuotojams	LR Socialinės apsaugos ir darbo ministerija http://www.sodra.lt/	2 lygmens paslauga 3 lygio saugumas	Pateikiama informacija ir elektroninės formos. Informacijos saugos priemonės – standartinės.
Muitinės deklaracijos	LR Muitinės departamentas prie finansų ministerijos http://www.cust.lt/	4 lygmens paslauga 2 lygio saugumas	Sudarius sutartį galima pateikti deklaracijas elektroniniu būdu, tačiau laikinai ši paslauga neprieinama.
Leidimai derinami su aplinkos apsaugos tarnybomis	LR Aplinkos ministerija http://aaa.am.lt/	1 lygmens paslauga 3 lygio saugumas	Pateikiama tik informacija. Naudojamos standartinės informacijos saugos priemonės.

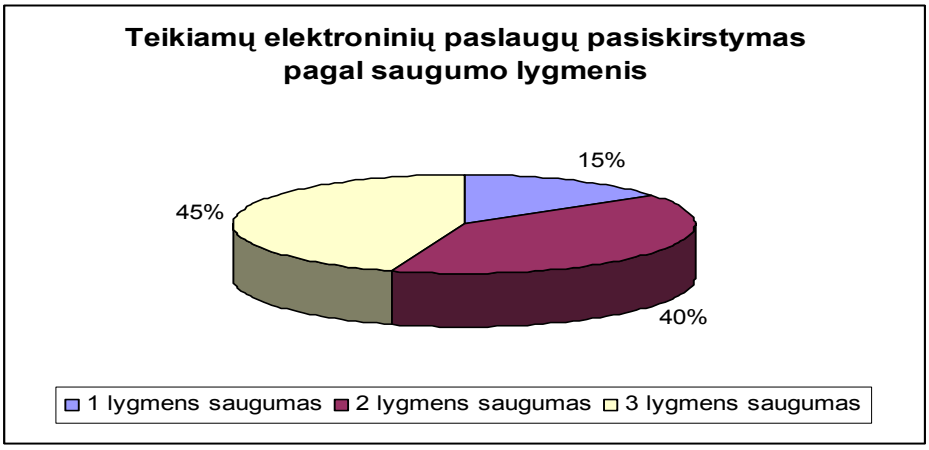
Tyrimo išvados:

Viešąsias elektronines paslaugas teikiančių institucijų informacijos saugos lygmuo yra patenkinamas (atsižvelgiant į teikiamų paslaugų brandos lygmenį), tačiau bendras saugumo laipsnis nėra aukštas – tai gali būti susiję su nedideliu skaičiumi institucijų teikiančių brandžias elektronines paslaugas, o taip pat ir su paties tyrimo atlikimu (Buvo tiriamos saugos priemonės ir jų taikymas, tačiau nebuvo domimasi saugumo incidentais, o atsižvelgiant į tokio pobūdžio incidentų latentiškumą ir institucijų nesuinteresuotumą teikti tokią informaciją, galima numatyti gilesnio pobūdžio tyrimą).

15%, elektroninės valdžios koncepcijoje numatytų viešųjų elektroninių paslaugų, teikiamos užtikrinant aukščiausią – 1 informacijos saugumo lygmenį (5 diagrama). Didelė dalis teikiamų elektroninių paslaugų (40%) teikiamos tik identifikavus vartotoją. Tai dažniausiai atliekama informacijos vientisumo užtikrinimui. Trečio saugumo lygmens paslaugos naudoja paprasčiausias saugumo užtikrinimo priemones siekdamos tik institucijos pateikiamos informacijos vientisumo ir prieinamumo užtikrinimo.

Svarbu pastebėti, jog nei viena elektroninė paslauga neišnaudoja elektroninio parašo kaip tiesioginio saugumą užtikrinančio elemento. Vartotojų identifikavimui paprastai panaudojama institucijos susikurta sistema arba elektroninės bankininkystės paslauga. Viešųjų elektroninių paslaugų sistema dar nesugeba pasinaudoti elektroninio parašo suteikiamomis galimybėmis. Viena iš rekomendacijų būtų infrastruktūros plėtimas ir elektroninio parašo populiarinimas paprastų vartotojų tarpe (Šiuo metu jį įsigyti ir pasinaudoti gana brangu ir sudėtinga).

5 Diagrama. Teikiamų elektroninių paslaugų pasiskirstymas pagal saugumo lygmenis



Visų tirtų institucijų informacijos saugos priemonių taikymą galima lyginti su jų pasirengimu teikti elektronines paslaugas. Jos skirstomos į tris grupes:

- Institucijos, teikiančios galutinai išvystytas viešąsias elektronines paslaugas, kurių taikomos informacijos saugos priemonės atitinka aukščiausią saugumo lygmenį.
- Institucijos, numatančios aukšto lygmens viešųjų elektroninių paslaugų teikimą, kuriančios jų teikimo projektus ir informacijos saugos priemones reglamentuojančius dokumentus.
- Institucijos, teikiančios žemiausio brandos lygmens viešąsias elektronines paslaugas, kurios taiko tik paprasčiausias informacijos saugos priemones, tenkinančias brandos lygmens reikalavimą.

Tyrimo metu paaiškėjo, jog ne visos institucijos (35%), teikiančios viešąsias elektronines paslaugas, turi aiškiai reglamentuotus informacijos saugos nuostatus ir strateginius informacinių sistemų planavimo dokumentus. Taip pat pastebėtina, jog ne visos institucijos (nevaldančios valstybinių informacinių sistemų) turi parengusios reikalavimus informacijos saugai (arba jie nėra apimantys visas sritis) ar informacinių sistemų saugos politiką reglamentuojančius dokumentus. Rekomenduotina įstatymiškai įpareigoti institucijas paruošti šiuos dokumentus.

IŠVADOS

1. Informacijos saugumas, teikiant viešąsias elektronines paslaugas – kritinis aspektas jų patikimumo ir naudojamumo atžvilgiu. Ne vienas Europos Sąjungos ir Lietuvos Respublikos teisinis dokumentas pabrėžia, jog nuo informacijos saugos užtikrinimo elektroninės valdžios infrastruktūroje, priklauso šios sistemos ateitis ir ilgalaikė reputacija. Informacijos sauga, kuriant elektroninės valdžios infrastruktūrą, yra prioritetinė sritis tiek Europos Sąjungoje, tiek ir Lietuvoje.
2. Nepaisant Lietuvos Respublikos teisinių dokumentų gausos, tinklų ir informacijos saugos užtikrinimas nėra reglamentuotas įstatymu, kuris apimtų tokių sąvokų kaip „tinklų ir informacijos sauga“ ar „informacijos saugos politika“ apibrėžimą, įpareigotų valstybės institucijas vykdyti informacinės saugos kontrolę, nurodytų sukurti informacinių sistemų saugos politiką institucijoje reglamentuojantį dokumentą. Institucijos nėra įstatymiškai įpareigojamos laikytis praktinių informacijos saugumo valdymo principų ISO/IEC 17799:2000 saugumo standarto – paprastai jis paminimas tik kaip rekomendacija.
3. Ne visos viešąsias elektronines paslaugas teikiančios institucijos turi aiškiai reglamentuotus informacijos saugos nuostatus ir strateginius informacinių sistemų planavimo dokumentus, o taip pat ir parengusios reikalavimus informacijos saugai (neapimantys visų sričių) ar informacinių sistemų saugos politiką reglamentuojančius dokumentus. Rekomenduotina įstatymiškai įpareigoti valstybės institucijas paruošti šiuos dokumentus.
4. Informacijos saugumas yra kompleksinė sritis, kurioje, stengiantis išvengti informacijos saugos fragmentiškumo ar institucijų funkcijų dubliavimo, reikia koordinuoti tarpusavio veiksmus, aiškiai paskirstyti atsakomybę tarp valstybės institucijų.
5. Informacijos saugos kaina negali viršyti saugomos informacijos vertės, todėl saugos priemonės turėtų būti parenkamos ir diegiamos tik po gerai atliktos rizikos ir ekonominės analizės, kuri įvertintų reikalingą saugumo lygį ir būtų atsižvelgta į saugomos informacijos vertę.
6. Saugiai informacinei sistemai sukurti būtinas kvalifikuotas ir patikimas personalas. Jo pagalba užtikrinamas efektyvus incidentų valdymas ir veiksminga informacijos saugos kontrolė, todėl būtinas periodiškas personalo kvalifikacijos kėlimas informacijos saugos srityje.

7. Siekiant informacijos saugumo Europos lygmenyje, buvo kuriamas IDA programos projektas TESTA. Nacionalinis šio projekto variantas – saugus valstybinis duomenų perdavimo tinklas, kurį galima naudoti komunikacijai Europos lygmeniu, – priemonė saugių elektroninių paslaugų plėtrai, todėl turėtų būti tęsiamas infrastruktūros kūrimas, skatinant organizacijų, kurioms ši priemonė yra aktuali, dalyvavimą.
8. Šiuo metu nėra sukurta ir patvirtinta fizinių ir juridinių asmenų tapatybės nustatymo valstybės informacinėse sistemose koncepcija. Būtina skubiai spręsti fizinių ir juridinių asmenų identifikavimo valstybės informacinėse sistemose problemą siekiant geresnių informacijos saugos sąlygų teikiant viešąsias elektronines paslaugas. Piliečių identifikavimo problema – esminė kliūtis tolimesniam elektroninių paslaugų vystymui.
9. Nemažas skaičius piliečių vengia naudoti viešąsias elektronines paslaugas nepasitikėdami informacijos saugumu, todėl šias paslaugas teikiančios institucijos turėtų užtikrinti būtiną saugą, o taip pat informuoti vartotojus apie institucijos naudojamas saugos priemones ir joje vykdomą saugos politiką, siekdami padidinti paslaugų vartotojų skaičių.

LITERATŪROS SĄRAŠAS

Lietuvos Respublikos teisės aktai

1. Lietuvos Respublikos elektroninio parašo įstatymas. 2000-07-11 Nr.VIII-1822// http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=169880; prisijungimo laikas: 2006-10-12
2. Lietuvos Respublikos elektroninių ryšių įstatymas. 2004-04-15 Nr. IX-2135 // http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=232036&p_query=&p_tr2=; prisijungimo laikas: 2006-10-12
3. Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo pakeitimo įstatymas. 2003-12-16 Nr. IX-1908 // http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=224465&p_query=&p_tr2=; prisijungimo laikas: 2006-10-12
4. Lietuvos Respublikos Vidaus reikalų ministro įsakymas „Dėl informacijos klasifikavimo pagal duomenų grupes rekomendacijų patvirtinimo“. 2003-01-27 Nr. 1V-33 // http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=216170&p_query=&p_tr2=; prisijungimo laikas: 2006-10-12
5. Lietuvos Respublikos Vidaus reikalų ministro įsakymas „Dėl informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“. 2004-05-06 Nr. 1V-156 // http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=233268&p_query=&p_tr2=; prisijungimo laikas: 2006-10-12
6. Lietuvos Respublikos Vidaus reikalų ministro įsakymas „Dėl Interneto tarnybinių stočių apsaugos rekomendacijų patvirtinimo“. 2004-05-21 Nr. 1V-176 // http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=234012&p_query=&p_tr2=; prisijungimo laikas: 2006-10-12
7. Lietuvos Respublikos Vidaus reikalų ministro įsakymas „Dėl tipinių duomenų saugos nuostatų patvirtinimo“. 2003-07-16 Nr. 1V-272 // http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=216052&p_query=&p_tr2=; prisijungimo laikas: 2006-10-12
8. Lietuvos Respublikos Vyriausybės nutarimas „Dėl duomenų apsaugos valstybės ir vietos savivaldos informacinėse sistemose“. 1997-09-04 Nr. 952 //

http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=42817&p_query=&p_tr2=; prisijungimo laikas: 2006-10-12

9. Lietuvos Respublikos Vyriausybės nutarimas „ Dėl elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinės strategijos iki 2008 metų ir jos įgyvendinimo priemonių plano patvirtinimo“. 2006-06-19 Nr. 601 // http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=278475&p_query=&p_tr2=; prisijungimo laikas: 2006-12-18
10. Lietuvos Respublikos Vyriausybės nutarimas „Dėl elektroninės valdžios koncepcijos patvirtinimo“. 2002-12-31 Nr. 2115 // http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=198184&p_query=&p_tr2=; prisijungimo laikas: 2006-10-12
11. Lietuvos Respublikos Vyriausybės nutarimas „Dėl informacinių technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo“. 2001-12-22 Nr. 1625 // http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=215825&p_query=&p_tr2=; prisijungimo laikas: 2006-10-12
12. Lietuvos Respublikos Vyriausybės nutarimas „Dėl valstybės informacinių sistemų ir įteisinimo taisyklių patvirtinimo“. 2004-04-19 Nr. 451 // http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=231255&p_query=&p_tr2=; prisijungimo laikas: 2006-10-12
13. Lietuvos Respublikos Vyriausybės nutarimas „Dėl viešojo administravimo plėtros iki 2010 metų strategijos patvirtinimo“. 2004-04-28 Nr. 488 // http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=285917&p_query=&p_tr2=; prisijungimo laikas: 2006-10-12
14. Lietuvos Respublikos Vyriausybės nutarimas „Dėl viešojo administravimo plėtros iki 2010 metų strategijos įgyvendinimo 2007-2010 metų priemonių plano patvirtinimo“. 2006-11-06 Nr. 1097 // http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=286022&p_query=&p_tr2=; prisijungimo laikas: 2006-10-12
15. Lietuvos Respublikos ryšių ir informatikos ministerijos įsakymas „Dėl Valstybės institucijų kompiuterių tinklo (VIKT) paslaugų teikimo taisyklių patvirtinimo“. 1996-11-12 Nr. 123 // http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=32665&p_query=&p_tr2=; prisijungimo laikas: 2006-06-05
16. Lietuvos Respublikos Seimo nutarimas „Dėl Elektroninės valdžios koncepcijos patvirtinimo“. 2002-12-31 Nr. 2115 //

http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=198184; prisijungimo laikas: 2006-10-12

Kiti šaltiniai

17. Barker W.C. Guide for mapping types of information and inforamtion systems to security categories. Information security. Volume I. 2004 June, United States of America // http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V1-final.pdf; prisijungimo laikas: 2006-03-23
18. Clift S. E-Democracy, E-Governance and Public Net-Work. 2003 September // http://www.publicus.net/articles/edempublicnetwork.html; prisijungimo laikas: 2006-06-08
19. Communication from the Commission to the Council and the European Parliament. Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime. 2001-01-26 // http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeCommEN.html; prisijungimo laikas: 2006-09-25
20. Communication from the Commission to the Council and the European Parliament. Dialogue, partnership and empowerment: A Strategy for a Secure Information Society. 2006-05-31 // http://europa.eu.int/information_society/newsroom/cf/itemlongdetail.cfm?item_id=2766; prisijungimo laikas: 2006-02-15
21. Communication from the Commission to the Council and the European Parliament. i2010 – Europos informacinė visuomenė augimui ir užimtumui skatinti. 2005-06-01 // http://europa.eu.int/information_society/eeurope/i2010/docs/communications/com_229_i2010_310505_fv_lt.doc; prisijungimo laikas: 2006-09-25
22. Communication from the Commission to the Council and the European Parliament. Interoperability for Pan-European eGovernment Services. 2006-02-13 // http://ec.europa.eu/idabc/servlets/Doc?id=24117; prisijungimo laikas: 2006-02-15
23. Communication from the Commission to the Council and the European Parliament. The Role of eGovernment for Europe's Future. 2003-09-26 // http://europa.eu.int/information_society/eeurope/2005/doc/all_about/egov_communication_en.pdf; prisijungimo laikas: 2006-06-08
24. Communication from the Commission to the Council and the European Parliament. eEurope 2005: An information society for all. 2002-05-28 //

http://europa.eu.int/information_society/eeurope/2005/all_about/action_plan/index_en.htm; prisijungimo laikas: 2006-05-05

25. Communication from the Commission to the Council and the European Parliament. eEurope 2005: An information society for all. Executive summary 2002-05-28 // http://europa.eu.int/information_society/eeurope/2002/news_library/documents/eeurope2005/eeurope2005_en.pdf; prisijungimo laikas: 2006-05-05
26. Communication from the Commission to the Council and the European Parliament. Network and Information Security: Proposal for A European Policy Approach. 2001 // http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52001DC0298:EN:HTML; prisijungimo laikas: 2006-02-15
27. Communication from the Commission to the Council and the European Parliament. Network and information security: proposal for a European policy approach. Executive summary. 2001// http://europa.eu.int/information_society/eeurope/2002/news_library/pdf_files/execsum_en.pdf; prisijungimo laikas: 2006-10-04
28. Council resolution on a common approach and specific actions in the area of network and information security. 2001-12-11 // http://register.consilium.eu.int/pdf/en/01/st15/15152en1.pdf; prisijungimo laikas: 2006-09-25
29. Čėsna R., Štitilis D. Kompiuterinės informacijos ir elektroninių dokumentų apsauga viešajame administravime. Vilnius: Lietuvos teisės akademija, 2000.
30. Direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. 1995-10-25 // http://www3.lrs.lt/pls/inter1/dokpaieska.showdoc_l?p_id=7879&p_query=&p_tr2=2; prisijungimo laikas: 2006-10-14
31. Direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje. 2002-07-12 // http://www3.lrs.lt/pls/inter1/dokpaieska.showdoc_l?p_id=36605; prisijungimo laikas: 2006-09-25
32. eGovernemnt, more that as automation of government services. 2003 October // www.isc.ie/downloads/egovernment.pdf; prisijungimo laikas: 2006-06-08
33. Elektroninės viešosios paslaugos Lietuvoje. IVPK prie LR Vyriausybės. 2002-08-01 // http://www.ivpk.lt/main-aktual.php?cat=61&n=11; prisijungimo laikas: 2006-06-18

34. Elektroninių viešųjų paslaugų siekiamo modelio aprašymas. IVPK prie LR Vyriausybės. // http://epp.ivpk.lt/epp/Dokumentai/IVPK_elmodelis_siekiamasV1.pdf; prisijungimo laikas: 2006-06-18
35. EU: Green light for the European e-security agency. 2003-11-21 // http://ec.europa.eu/idabc/en/document/1828/355; prisijungimo laikas: 2006-09-25
36. EU: Plans for a new EU cyber-security agency announced. 2003-02-11 // http://ec.europa.eu/idabc/en/document/863/355; prisijungimo laikas: 2006-09-25
37. Grance T., Hash J., Stevens M. etc. Guide to information technology security services. 2003 October, United States of America // http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf; prisijungimo laikas: 2006-03-23
38. IDA programa. Duomenų mainai tarp Europos Sąjungos administracijų // http://www.svdpt.gov.lt/idabc.php; prisijungimo laikas: 2006-06-05
39. IDA. From Interchange of data between administrations to Pan-European eGovernment Services: the way forward. 2003 // http://www.is.lt/is/ida/The_way_forward.pdf; prisijungimo laikas: 2006-06-05
40. Jastramskas V. Informacijos apsaugos pagrindai. Kaunas: Technologija, 1999.
41. Lietuvos Standartizacijos departamentas. Informacijos technologija. Praktiniai informacijos saugumo valdymo principai ISO/IEC 17799:2000.
42. Lietuvos Statistikos departamentas prie LR Vyriausybės. Informacinės technologijos 2006. Vilnius, 2006.
43. Maiwald E. Network security. A begginers guide. New York. 2003.
44. Mykolo Romerio Universitetas. Projekto SAFARI tyrimo ataskaita. 2005.
45. Organization for economic co-operation and development. Guidelines for the security of information systems and networks. Towards the culture of security. 2002-07-25, Paris.// http://www.oecd.org/dataoecd/16/22/15582260.pdf; prisijungimo laikas: 2006-03-23
46. Petrauskas R., Štitilis D. Kompiuteriniai nusikaltimai ir jų prevencija. Vilnius: Lietuvos teisės akademija, 2000.
47. Saugus valstybinis duomenų perdavimo tinklas (SVDPT) // http://www.svdpt.gov.lt/kas_yra_SVDPT.php; prisijungimo laikas: 2006-06-05
48. TESTA – A catalogue of services. Version 1.24. 2001.04.11 // http://www.is.lt/is/ida/TESTA_catalogue_of_services.doc; jungimo laikas: 2006-06-05
49. TESTA architektūra // http://www.svdpt.gov.lt/architektura.php; prisijungimo laikas: 2006-06-05
50. VIKT tinklas // http://www.is.lt/vikt_tinklas/apievikt.shtml; prisijungimo laikas: 2006-06-05

SANTRAUKA

Darbo tema: „Informacijos saugumas elektroninės valdžios infrastruktūros kūrime“ (2006m., darbo vadovas – Prof. Dr. R. Petrauskas).

Raktiniai žodžiai: tinklų ir informacijos saugumas, informacijos sauga, informacijos saugumo politika, viešosios elektroninės paslaugos, elektroninė valdžia.

Santraukos turinys: Informacijos ir tinklų saugumas, teikiant viešąsias elektronines paslaugas, turi lemiamą reikšmę. Informacijos saugumo užtikrinimas – būtina elektroninės valdžios egzistavimo sąlyga. Atlikus teisinių dokumentų, statistinių duomenų, teorinių šaltinių, o taip pat ir praktinį e.valdžios paslaugas teikiančių institucijų tyrimą, buvo padaryta išvada, jog aukšto brandos lygmens paslaugos negali būti teikiamos nepasirūpinus tinkama informacijos sauga.

2006 gegužės 31 dieną Europos Komisija priėmė saugios informacinės visuomenės strategijos komunikatą „Dialogas, partnerystė ir teisių suteikimas“, kurio pagrindinis tikslas – tinklų ir informacijos saugumas. Tai pabrėžė Europos Sąjungos požiūrį ir prioritetus informacijos saugai.

2006 vasario 13 dieną Europos Komisijos paskelbtame komunikate „Tarpusavio sąveika pan-Europinėms e.valdžios paslaugoms“ pabrėžiama, jog moderni viešojo administravimo sistema gali būti sukurta tik pažangios, bei patikimos informacinių ir komunikacinių technologijų infrastruktūros, o taip pat aiškių elektroninės valdžios procesų pagrindu.

Magistrinio darbo tikslas – ištirti ir užtikrinti informacijos saugumą elektroninės valdžios infrastruktūroje, teorinį ir praktinį saugios sistemos pagrindimą.

Darbo metu buvo išanalizuoti Europos Sąjungos ir Lietuvos Respublikos teisiniai dokumentai, Lietuvos Statistikos departamento statistiniai duomenys, tarptautiniai saugumo standartai, teoriniai informacijos saugumo kūrimo ir užtikrinimo šaltiniai, praktiniai saugos projektų pavyzdžiai ir viešųjų elektroninių paslaugų teikėjų kuriama infrastruktūra.

Darbo apibendrinanti išvada – informacijos saugumas, teikiant viešąsias elektronines paslaugas yra kritinis aspektas jų patikimumo ir naudojamumo atžvilgiu. Ne vienas Europos Sąjungos ir Lietuvos Respublikos teisinis dokumentas pabrėžia, jog nuo informacijos saugos užtikrinimo elektroninės valdžios infrastruktūroje, priklauso šios sistemos ateitis ir ilgalaikė reputacija.

SUMMARY

Thesis: „Information security in the creation of the infrastructure of electronic government“. (Supervisor: Professor, Doctor. R. Petrauskas).

Key words: network and information security, policy of the information security, information security, public electronic services, electronic government.

Content of the summary: The network and information security has a critical importance for the public electronic services. The essential condition for the existence of the electronic government is the assurance of the information security. The conclusion, that the electronic services of the higher level can not be offered without suitable measures of security implemented, was made after the analysis of the juridical documents, statistical data, and theoretical sources in addition with the accomplished practical survey on the institutions offering the services of electronic government.

European Commission issued the new communicate “Dialogue, partnership and empowerment: A Strategy for a Secure Information Society” on 31st of May, 2006. The main goal of this document is the security of network and information. This step stressed the priority given to information security by European Union.

European Commission released a communicate “Interoperability for Pan-European eGovernment Services” on 13th of February, 2006, which stressed that the modern system of public administration can not be created without the reliable infrastructure of information and communication technologies, and clear processes of electronic government.

The main objective of this master thesis is to analyze the issues of information security assurance in the infrastructure of electronic government, theoretical and practical creation of the secure system.

The analysis of juridical documents issued by European Union and Lithuanian Republic, statistical data, presented by the Lithuanian Department of Statistics, international security standards, practical projects and Lithuanian infrastructure of electronic government was carried out.

The main conclusion was made – information security is the critical aspect in the creation of the electronic services. Lots of juridical documents emphasize that the future and reputation of the infrastructure of electronic government depend on the information security assurance.