Integralaus informacijos saugumo valdymo modelio taikymas Lietuvos valstybės institucijoms

Saulius Jastiuginas

Vilniaus universiteto Komunikacijos fakulteto
Informacijos ir komunikacijos katedros doktorantas
Department of Information and Communication,
Faculty of Communication, Vilnius University,
Doctoral student
Saulėtekio al. 9, LT-10222 Vilnius
Tel. (8 5) 236 6119, faks. (8 5) 236 6104
El. paštas: saulius.jastiuginas@kf.vu.lt

Pirmieji informacijos saugumą reglamentuojantys dokumentai Lietuvoje patvirtinti prieš 15 metų. Pirmasis informacijos saugumo strateginis dokumentas taip pat jau pradėjo skaičiuoti antrą dešimtmetį. Nuolat kintantis informacijos saugumo praktinis problematikos laukas lėmė ne vieną šių dokumentų atnaujinimo iteraciją bei nemažai informacijos saugumo stiprinimo veiklų. Dauguma šių veiklų apsiribojo techninių ir administracinių priemonių taikymo nustatymu bei formalizavo atsakomybes, susijusias su informacijos saugumu, užtikrinimą.

Vertinant tiek globalų, tiek Lietuvos informacijos saugumo valdymo mokslinių tyrimų kontekstą galima pastebėti, kad šalia ilgą laiką vyravusios technologinių sprendinių taikymo problematikos ryškėja aktualūs žmogiškieji, ekonominiai ir kiti klausimai, kyla platesnio vadybinio požiūrio poreikis ir tampa akivaizdu, kad esamos praktinės informacijos saugumo valdymo priemonės nebėra pakankamos informacijos saugumui valdyti. Sprendžiant šią problemą, kaip nauja priemonė galėtų būti pagalbus teorinis integralus informacijos saugumo valdymo modelis, sujungiantis informacijos saugumo valdymo ir informacijos vadybos dedamąsias.

Šio straipsnio tikslas – aptarti atliktą teorinio integralaus informacijos saugumo valdymo modelio praktinio pritaikomumo tyrimą. Praktinio pritaikomumo tyrimas atliekamas vertinat informacijos saugumo valdymą Lietuvos valstybės institucijose. Straipsnyje aptariamam tyrimui buvo keliami šie uždaviniai: suformuoti informacijos saugumo valdymo Lietuvos valstybės institucijose vertinimo prieigą; atlikti atvejo analizę – dokumentų turinio analizės metodu išnagrinėti teisės aktų bazėse ir Lietuvos valstybės institucijų svetainėse skelbiamus norminius dokumentus, reglamentuojančius informacijos saugumo valdymą; gautus analizės rezultatus pagrįsti kokybiniu tyrimu – ekspertų apklausa.

Straipsnyje pateikti tyrimų rezultatai leido patvirtinti integralaus informacijos saugumo valdymo modelio pagrįstumą, įvertinti informacijos saugumo valdymą Lietuvos valstybės institucijose, identifikuoti trūkumus, pateikti praktinio problemų sprendimo siūlymus ir sukurti prielaidas tolesniems moksliniams tyrimams.

Straipsnis parengtas remiantis dokumentų turinio analizės, lyginamosios analizės, dokumentiniu atvejo tyrimo, kokybinio tyrimo (ekspertų apklausos) ir apibendrinimo metodais.

Pagrindiniai žodžiai: *informacijos saugumo valdymas, integralus informacijos saugumo valdymo modelis, Lietuvos valstybės institucijos.*

Integralus informacijos saugumo valdymo modelis

Integralus informacijos saugumo valdymo modelis suformuotas remiantis informacijos saugumo ir informacijos vadybos tyrėjų mokslinių įžvalgų lyginamosios analizės, analogijos ir apibendrinimo metodais.

Dauguma *informacijos saugumo* apibrėžčių jau daugiau kaip dvidešimt metų remiasi trimis informacijos saugumo tikslais (CIA triada). Pagal CIA triadą įvardijama, kad *informacijos saugumo* tikslas – užtikrinti informacijos konfidencialumą (*confidentiality*), vientisumą (*integrity*) ir prieinamumą (*availability*) (Parker, 1981; McCumber, 2005; Trcek, 2006; ISO 27000 standartų grupė ir kiti). Analizuojant mokslinėse diskusijose nagrinėjamų informacijos saugumo teorinių įžvalgų visumą, galima konstatuoti platų tyrimų turinio kontekstą – tyrėjai aktyviai nagrinėja įvairius vadybinius, organizacinius ir ekonominius (Chang, Lin 2007; Dlamini, Eloff, Eloff, 2009; Gordon, Loeb, 2006), techninių, teisinių, standartų ir kitų saugumo priemonių taikymo (Anderson, Moore, 2009; Weise, 2009; Kazanavičius ir kt., 2012; Japertas, Činčikas, Šestaviskas, 2012; Štitilis, Paškauskas, 2007), socialinės inžinerijos, psichologinius ir kompetencijų (Ashenden, 2008; Bakhshi, Papadaki ir Furnell, 2009) ir kitus aktualius informacijos saugumo valdymo aspektus. Apibendrinant informacijos saugumo tyrimuose analizuotus informacijos saugumo aspektus, galima konstatuoti, kad informacijos saugumo valdymas apima tris dimensijas – *strateginę,* jungiančią administracinius, organizacinius, valdymo, ekonominius, standartų, teisinius, gerųjų praktikų ir pan. aspektus; *žmogiškąją,* jungiančią saugumo kultūros, etinius, kompetencijų, mokymų, psichologinius ir pan. aspektus; *technologinę,* jungiančią informacinių technologijų, techninių ir programinių priemonių, matematinius, kriptografinius ir pan. aspektus (Jastiuginas, 2011).

Jungiant informacijos saugumo valdymo objektą (informaciją), tikslus (konfidencialumą, prieinamumą, vientisumą) ir dimensijas (strateginę, žmogiškąją, technologinę), informacijos saugumo valdymo turinį galima apibrėžti kaip siekį užtikrinti informacijos konfidencialumą, vientisumą ir prieinamumą derinant strateginę, žmogiškąją ir technologinę dimensijas. Tačiau siekiant valdyti informacijos saugumą nepakanka apibrėžti informacijos saugumo valdymo turinį, būtina numatyti ir priemones, kuriomis jis galėtų būti valdomas. Šiuo metu plačiausiai taikomų informacijos saugumo valdymo priemonių (metodikų, standartų, modelių) turinys labai panašus, tačiau stebint nuolat kylančias informacijos saugumo problemas (pavyzdžiui, informacijos saugumo incidentų skaičiaus augimą) ryškėja, kad esamos priemonės nėra pakankamos informacijos saugumui valdyti. Vertinant tendencijas, kad informacijos saugumo valdymas iš technologinės tampa vadybine disciplina, o pagrindinis saugumo objektas yra informacija, informacijos saugumo valdymui siektina pasitelkti informacijos vadybos įrankius.

Informacijos vadybos įrankius, jų apibrėžtis ir svarbą nagrinėjo D. Chaffey, S. Woodas, C. Schlöglis, Ch. Choo, D. Skyrme'as, M. J. Earl, E. Orna, T. H. Davenportas, T. D. Wilsonas ir kiti. Apibendrinant šių informacijos vadybos mokslininkų įžvalgas pagrindiniais informacijos vadybos įrankiais įvardytina informacijos politika, informacijos strategija, infor-

macijos auditas, informaciniai procesai ir aplinka bei informacijos kokybė. Organizacijos informacijos politika sieja informacijos valdymą su organizacijos veiklos procesais, nustato tikslus ir prioritetus (Orna, 2004), informacijos strategija apibrėžia informacijos politikos įgyvendinimo kryptis (Schlögl, 2005), informacijos auditas padeda įvertinti esamą informacijos vadybos veiklą, nustatyti, ar organizacijos ištekliai naudojami efektyviai, identifikuoti problemas, numatyti galimus jų sprendimo būdus (Botha, Boon, 2003; Orna, 2004). Informacinių procesų nenutrūkstamas ciklas ir aplinkos komponentų analizė leidžia organizacijai prisitaikyti prie besikeičiančios aplinkos ir koordinuotai įgyvendinti užsibrėžtus tikslus (Choo, 2002; Davenport ir Prusak, 1997), informacijos kokybės valdymas užtikrina, kad organizacija valdo vertingą, organizacijos lūkesčius atitinkančią ir pridėtinę vertę kuriančią informaciją (English, 2004).

Vertinant informacijos vadybos sąsajas su informacijos saugumo valdymo problematika, galima nustatyti informacijos vadybos įrankių reikšmę informacijos saugumo valdymui. Informacijos politika tiesiogiai sietina su informacijos saugumo politika, joje nustatomais informacijos saugumo tikslais ir prioritetais, kurie turi aiškiai, glaustai ir vienareikšmiškai identifikuoti pagrindinius informacijos saugumo valdymo pricipus. Informacijos strategijos reikšmė svarbi informacijos saugumo valdymui ir leistų apibrėžti informacijos saugumo valdymo atsakomybę, koordinavimą, orientavimą į pagrindinius organizacijos procesus, audito bei informacinių technologijų taikymą. Informacijos audito tikslai aktualūs vertinant informacijos saugumo kontekstą. Informacijos audito analogijų su informacijos saugumo auditu galima įžvelgti vertinant tiek audito tikslus, tiek informacijos audito komandos sudarymo (pasirinkimo tarp vidinių ir išorinių auditorių), tiek paties audito proceso (planavimas, duomenų rinkimas, duomenų analizė ir įvertinimas, rekomendacijų pateikimas ir jų įgyvendinimas) etapus.

Gretinant informacijos vadybos ir informacijos saugumo valdymo įrankius, galima daryti prielaidą, kad sėkmingas informacijos saugumo valdymas, kaip ir organizacijos informacijos valdymas, priklauso nuo organizacijos informacinės brandos, o ši – nuo visų darbuotojų bei vadovybės požiūrio į informacijos kokybę, sykiu ir į informacijos saugumą. Organizacijos branda taip pat sietina su organizacijos sugebėjimu taikyti pažangias valdymo priemones, užtikrinti visų informacijos procesų saugumo valdymą ir nepavėluotą reagavimą į išorinės, organizacinės bei informacinės aplinkos komponentų pokyčius.

Jeigu organizacija turi aiškią informacinę politiką ir strategiją, nuolat atliekamas auditas, valdomi visi informaciniai procesai, operatyviai prisitaikoma prie aplinkos pokyčių ir informacinės brandos lygis yra aukštas, galima pagrįstai tikėtis, kad bus užtikrintas ir informacijos saugumo valdymas.

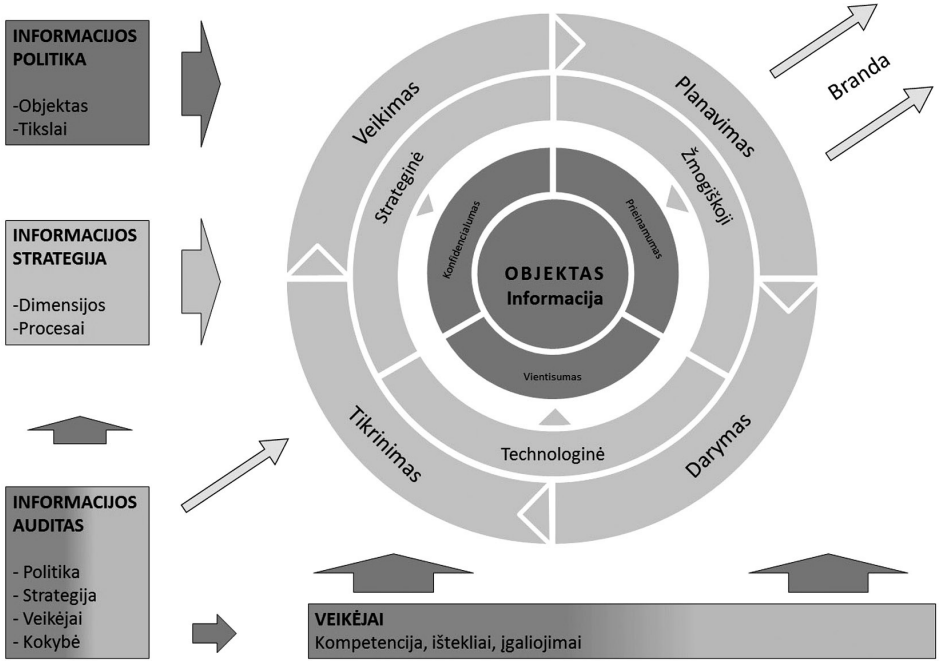
Įvertinus informacijos saugumo valdymo objektą, tikslus ir dimensijas, kaip pagrindiniai informacijos saugumo valdymo įrankiai išskirtini – informacijos saugumo politika, informacijos saugumo strategija ir informacijos saugumo auditas. Informacijos procesai ir aplinkos komponentai bei informacijos brandos vertinimo įrankių taikymas teoriniame ir praktiniame lygmenyse galėtų būti nagrinėjami kaip

informacijos saugumo valdymo brandos ir kokybės gerinimas.

Remiantis atskleista informacijos saugumo valdymo ir informacijos vadybos diskursų sudedamųjų dalių apibrėžtimi, teorinio integralaus informacijos saugumo valdymo modelio formavimo pagrindu išskirtini informacijos saugumo valdymo turinio elementai – objektas, tikslai ir dimensijos, bei pagrindiniai informacijos vadybos įrankiai – informacijos politika, informacijos strategija ir informacijos auditas.

Formuojant integralų informacijos saugumo valdymo modelį, *politikos lygmeniu* nustatomi tikslai ir pagrindiniai principai, t. y. informacijos saugumo objektas (informacija) ir tikslai (konfidencialumas, vientisumas ir prieinamumas). *Strategijos lygmuo* apima priemones, kuriomis bus siekiama politikoje įvardytų tikslų ir kurias apibendrintai išreiškia saugumo dimensijos (strateginė, žmogiškoji ir technologinė) bei leidžia užtikrinti nuolatinį šių priemonių valdymo procesą tam pasitelkiant Demingo (2000) ciklą. *Audito lygmuo* užtikrina efektyvaus valdymo kontrolę, padeda nustatyti valdymo spragas, įvertinti apibrėžtą informacijos politiką bei politikos įgyvendinimo strategiją. Bet kuriems procesams valdyti būtinas įgalinantis veiksnys – įgalioti veikėjai, t. y. pakankamų išteklių (kompetencijos) suteikimas. Kokybės (brandos) kėlimas įvardytinas kaip antrasis procesų tobulinimą įgalinantis veiksnys. Audito lygmuo leidžia įvertinti ir šiuos įgalinančius veiksnius.

Integralus informacijos saugumo valdymo modelis, jungiantis aptartą informacijos valdybos mokslų ir informacijos saugumo valdymo sąsajumą, pateikiamas 1 paveiksle. Modelio centre pavaizduotas



1 pav. ***Integralus informacijos saugumo valdymo modelis (sudaryta autoriaus)***

informacijos saugumo objektas – informacija. Pirmasis modelio žiedas vaizduoja informacijos saugumo tikslus. Šias dvi modelio dedamąsias jungia informacijos politikos įrankis ir apibrėžia, *kas* turėtų būti saugoma (modelyje išskirta tamsiai pilka spalva). Antrasis žiedas iliustruoja informacijos saugumo dimensijas, trečiasis – procesus. Šias modelio dedamąsias jungia informacijos strategijos įrankis ir nusako, *kaip* turėtų būti saugoma (modelyje išskirta šviesiai pilka spalva). Informacijos audito įrankis leidžia patikrinti politikos ir strategijos išsamumą bei įvertinti, *ar yra* prielaidos informacijos saugumui valdyti, t. y. ar paskirti veikėjai (suteikti ištekliai ir kompetencijos), ar užtikrinama veiklos kokybė, ar visi šie veiksniai darniai sąveikaudami leidžia siekti didesnės informacijos saugumo valdymo brandos.

Integralus informacijos saugumo valdymo modelis jungia valdomo informacijos saugumo turinį, nusakantį, kas ir kaip turėtų būti valdoma, ir informacijos vadybos įrankius, kurie sudaro sąlygas įvertinti ir užtikrinti informacijos saugumo valdymo kompleksiškumą.

Integralaus informacijos saugumo valdymo modelio taikymas Lietuvos valstybės institucijoms

Teoriniame lygmenyje suformuotas integralus informacijos saugumo valdymo modelis, tikėtina, gali būti taikomas ne tik mokslinių tyrimų plėtotei, bet ir praktinio lygmens problemų sprendimui. Šiai prielaidai patikrinti būtina atlikti empirinį tyrimą, kuris leistų pagrįsti modelio taikymo galimybes.

Empirinio tyrimo metodologija

Empirinio tyrimo tikslas – nustatyti teorinio integralaus informacijos saugumo valdymo modelio praktinio pritaikomumo galimybes.

Empirinio tyrimo objektas – integralaus informacijos saugumo valdymo modelio praktinis taikymas Lietuvos valstybės institucijų informacijos saugumui valdyti.

Empirinio tyrimo uždaviniai:

1. Suformuoti informacijos saugumo valdymo vertinimo prieigą, įrankius ir vertinimo kriterijus.
2. Nustatyti šaltinius, formuojančius informacijos saugumo valdymo reikalavimus Lietuvos valstybės institucijoms.
3. Ištirti identifikuotų šaltinių turinį suformuotos informacijos saugumo valdymo prieigos įrankių ir vertinimo kriterijų kontekste.
4. Pagrįsti gautų teorinio tyrimo rezultatų praktinį pritaikomumą.

Empirinio tyrimo modelis

Remiantis teoriniu integruotu informacijos saugumo valdymo modeliu buvo suformuota informacijos saugumo vertinimo prieiga, išskirti informacijos saugumo valdymo įrankiai ir apibrėžti vertinimo kriterijai. Ši prieiga taikyta atvejo analizei, atvejo analizės rezultatai patikrinti ekspertų apklauso metodu.

Empirinio tyrimo hipotezės:

1. Informacijos saugumas yra informacijos vadybos sudedamoji dalis, todėl efektyvus informacijos saugumo valdymas gali būti užtikrintas pasitelkiant informacijos vadybos įrankius.

2. Integruotas informacijos saugumo valdymo modelis leidžia identifikuoti informacijos saugumo valdymo Lietuvos valstybės institucijose trūkumus, o šiuos trūkumus pašalinus, užtikrinti kompleksišką ir efektyvų informacijos saugumo valdymą.

Empirinio tyrimo vykdymo laikotarpis

Empirinis tyrimas vykdytas 2012 m. sausio–birželio mėnesiais, rezultatų apdorojimas ir analizė – 2012 m. kovo–rugsėjo mėnesiais.

Empirinio tyrimo metodai

Empiriniam tyrimui atlikti taikyta mišrių metodų prieiga derinant dokumentų turinio analizės ir ekspertų apklausos tyrimo metodus. Pagrindiniai mišrių metodų prieigos taikymo motyvai: siekis surinkti įvairesnę, gausesnę empirinę medžiagą bei pagrįsti tyrimo rezultatus skirtingais duomenų šaltiniais ir formomis (Creswell ir Clark, 2006). Taigi, derinant šiuos metodus galima užtikrinti patikimus tyrimo rezultatus teorinio integralaus informacijos saugumo valdymo modelio praktinei realizacijai.

Atvejo analizės tyrimas

Informacijos saugumo valdymo Lietuvos valstybės institucijose atvejis nagrinėjamas dokumentų analizės metodu. Šis metodas taikytinas pirminiams duomenims rinkti, kai pagrindinis informacijos šaltinis yra dokumentai. Metodo patikimumą užtikrina oficialių dokumentų naudojimas (Tidikis, 2003). Atvejo analizės tyrimo metu dokumentų turinio analizės metodu išanalizuoti Lietuvos valstybės institucijoms galiojantys informacijos saugumo reikalavimai, institucijų nuostatai ir kiti informacijos saugumą reglamentuojantys norminiai dokumentai.

Tyrimui reikalingi norminiai dokumentai atrinkti pasinaudojant viešai prieinama Lietuvos Respublikos Seimo teisės aktų baze[1]. Šioje bazėje buvo ieškoma teisės aktų, reglamentuojančių informacijos saugumą, paieškos kriterijumi pasirenkant reikšminius žodžius „sauga“, „saugumas“, „informacijos sauga“ „informacijos saugumas“, „duomenų apsauga“ ir pan. Išsamesnė paieška buvo vykdoma remiantis teisės aktų bazės nuorodomis į susijusius teisės aktus bei juose rastomis nuorodomis, papildomos paieškos atliktos teisės aktuose nurodytų juos įgyvendinančių institucijų interneto svetainėse.

Ekspertų apklausa

Ekspertų apklausos metodas – tai specialiai parinktos grupės žmonių, kurie išmano tam tikrą sritį, apklausa. Šis metodas leidžia patikrinti metodologijos kokybę, pagrįsti praktinių rekomendacijų argumentavimą, tokiomis apklausomis siekiama mokslinio objektyvumo (Tidikis, 2003). Atliekamame tyrime ekspertų apklausa siekiama pagrįsti ir papildyti atvejo analizės tyrimo rezultatus, taigi šio metodo taikymas leistų susieti teorinį lygmenį su praktinio įgyvendinimo realybe, įvertinti teorinių išvadų pritaikomumą praktikoje. Ekspertams formuluotini nestruktūruoti klausimai, sietini su informacijos saugumo valdymo objektu, tikslais, dimensijomis bei jų sąsajomis su informacijos vadybos įrankių taikymu (politikos, strategijos, audito, veikėjų ir

[1] Lietuvos Respublikos Seimas. Dokumentų paieška: http://www3.lrs.lt/dokpaieska/forma_l.htm [žiūrėta 2012 m. birželio 8 d.].

kokybės). Apibendrintos klausimų grupės suformuotos atlikus dokumentinį turinio analizės tyrimą.

Ekspertų parinkimas

Respondentams atrinkti vykdyta tikslinė atranka, kuriai taikyti kriterijai: ne mažesnė nei penkerių metų darbo patirtis informacijos saugumo srityje, dalyvaujant informacijos saugumo politikos formavime arba įgyvendinime, valdant ypatingos svarbos valstybės informacinius išteklius; atstovavimas skirtingoms organizacijoms. Ekspertai atrinkti iš valstybės institucijų, dalyvavusių rengiant Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programą ir paskirtų atsakingais už šios programos įgyvendinimą; iš Valstybės kontrolės bei institucijų, valdančių ypatingos svarbos valstybės informacinius išteklius.

Remiantis šiais kriterijai kokybiniam tyrimui buvo atrinkti 6 ekspertai.

Informacijos saugumo valdymo vertinimo prieiga

Integralaus informacijos saugumo valdymo modelio taikymui informacijos saugumo valdymui vertinti formuotina informacijos saugumo valdymo vertinimo prieiga. Šiam uždaviniui atlikti dekomponuotas integralus informacijos saugumo valdymo modelis, išskleidžiant informacijos vadybos įrankius, šių įrankių turinį susiejant su informacijos saugumo valdymo turinio dedamosiomis (objektu, tikslais, dimensijomis) ir taip suformuojant vertinimo kriterijus. Informacijos saugumo valdymo vertinimo prieiga pateikiama 1 lentelėje.

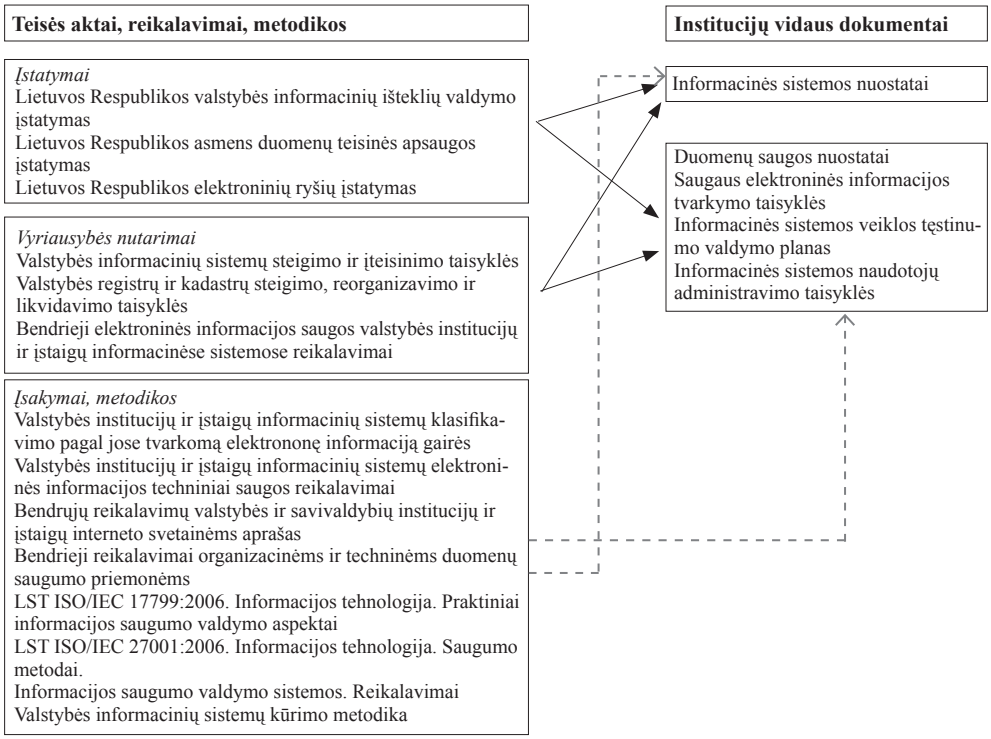
Vertinant tai, kad informacijos saugumo valdymas valstybės lygmeniu galimas tik užtikrinus informacijos saugumo valdymą organizacijų lygmeniu (valstybės institucijose), tikslinga tirti esamą informacijos saugumo valdymo situaciją institucijų ir valstybės lygmeniu.

1 lentelė. ***Informacijos saugumo valdymo vertinimo prieiga (sudaryta autoriaus)***

Įrankis	Vertinimo kriterijus
Informacijos saugumo politika	Ar nustatytas informacijos saugumo valdymo objektas? Ar nustatyti informacijos saugumo tikslai (konfidencialumas, vientisumas ir prieinamumas)?
Informacijos saugumo strategija	Ar nustatytos strateginės informacijos saugumo politikos įgyvendinimo kryptys, prioritetai, uždaviniai? Ar nustatytos strategijos įgyvendinimo priemonės, ar šios priemonės apima strateginę, žmogiškąją ir technologinę dimensijas? Ar apibrėžtas informacijos saugumo procesų ciklas, užtikrinamas reagavimas į aplinkos pokyčius?
Informacijos saugumo auditas	Ar apibrėžtas audito procesas, atsakomybė, periodiškumas ir vykdymo kontrolė? Ar vykdomas informacijos saugumo politikos įgyvendinimo strategijos ir informacijos saugumo veikėjų veiklos vertinimas?
Informacijos saugumo veikėjai	Ar apibrėžtas informacijos saugumo organizavimas ir nustatytos atsakomybės? Ar paskirtos informacijos saugumo valdymo atsakomybės ir įgaliojimai (kompetencijos)?
Informacijos saugumo branda	Ar nustatyti informacijos saugumo brandos lygiai? Ar vertinama informacijos saugumo branda?

Tyrimui reikalingų šaltinių analizė

Atlikta tyrimui reikalingų šaltinių paieška leido sudaryti informacijos saugumą reglamentuojančių teisės aktų sąrašą (chronologinis teisės aktų sąrašas pateiktas straipsnio priede). Analizuojant šių teisės aktų turinį konstatuotina, kad Lietuvoje nėra atskiro įstatymo, nuosekliai reglamentuojančio su informacijos saugumu susijusius santykius. Šiuo metu įstatymai (aukščiausios galios teisės aktai), bent iš dalies reglamentuojantys informacijos saugumą, yra Lietuvos Respublikos elektroninių ryšių įstatymas, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas bei 2012 m. sausio 1 d. įsigaliojęs Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas. Šis įstatymas pakeitė iki tol galiojusi Lietuvos Respublikos valstybės registrų įstatymą. Informacijos saugumas reglamentuotas ir žemesnės teisinės galios norminiuose dokumentuose – Lietuvos Respublikos Vyriausybės nutarimuose, ministrų ir kitų įgaliotų institucijų vadovų įsakymuose bei kituose dokumentuose. Lietuvos valstybės institucijoms galiojančių informacijos saugumo reikalavimų ryšiai pateikiami 2 paveiksle. Kairėje šio paveikslo pusėje išdėstyti aktualūs įstatymai, Vyriausybės nutarimai, atsakingų institucijų įsakymai ir metodiniai dokumentai (valstybės lygmuo), dešinėje – Lietuvos valstybės institucijoms privalomi parengti vidiniai dokumentai (institucijų lygmuo). Šiame paveiksle rodyklės nurodo prievolę nustatančius ryšius, punktyrinės rodyklės – metodinius dokumentus, padedančius parengti privalomus dokumentus.



2 pav. ***Informacijos saugumo valdymo reikalavimų sąryšiai (sudaryta autoriaus)***

Atvejo analizės tyrimo rezultatų aptarimas

Identifikuoti tyrimo šaltiniai analizuojami remiantis suformuota informacijos saugumo valdymo tyrimo prieiga, o tyrimo rezultatai – remiantis išskirtais informacijos saugumo politikos, strategijos, audito, brandos bei veikėjų įrankiais bei suformuotais vertinimo kriterijais.

Informacijos saugumo politika Lietuvos valstybės institucijose

Analizuojant Lietuvoje galiojančią informacijos saugumo valdymo politiką išskirtini šie vertinimo kriterijai – informacijos saugumo valdymo objektas ir tikslai.

Informacijos saugumo valdymo objektas

Remiantis identifikuotų tyrimo šaltinių analize galima išskirti informacijos saugumo valdymo objektus, kuriuos nustato atitinkami Lietuvos Respublikos įstatymai, atsižvelgiant į jų reglamentuojamą sritį. Šie informacijos saugumo objektai pateikiami 2 lentelėje.

Atsižvelgiant į tyrimo objektą, aktualiausias Lietuvos valstybės institucijoms galiojantis informacijos saugumo valdymo objektas yra informaciniai ištekliai. Informacinių išteklių aplinkos analizei iki 2011 m. gruodžio 31 d. aktualiausi galiojantys teisės aktai – Lietuvos Respublikos valstybės registrų įstatymas ir Lietuvos Respublikos Vyriausybės nutarimai, kuriais patvirtinta: Valstybės registrų ir kadastrų steigimo, reorganizavimo ir likvidavimo taisyklės; Valstybės informacinių sistemų steigimo ir įteisinimo taisyklės; Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai. Šių teisės aktų turinio analizė leidžia konstatuoti, kad Lietuvos Respublikos valstybės institucijos valdo keturių rūšių informacinius išteklius – valstybės registrus, žinybinius registrus, valstybės informacines sistemas ir vidaus administravimo informacines sistemas, tačiau tik valstybės registrų gyvavimo ciklas (kartu ir saugumo valdymas) buvo apibrėžtas įstatymų lygiu. Visų kitų informacinių išteklių funkcionavimą nustatė Lietuvos Respublikos Vyriausybė, taigi konstatuotina, kad žinybinių registrų, valstybės informacinių sistemų ir vidaus administravimo sistemų valdytojams, kurie tiesiogiai nepavaldūs Lietuvos Respublikos Vyriausybei (Lietuvos Respublikos Seimas, Lietuvos Respublikos Prezidentūra, savivaldybės, teismai, prokuratūra ir pan.), gyvavimo ciklo ir saugumo reikalavimai buvo tik rekomendacinio pobūdžio.

2 lentelė. ***Informacijos saugumo valdymo objektai (sudaryta autoriaus)***

Lietuvos Respublikos įstatymas	**Saugumo valdymo objektas**
Elektroninių ryšių įstatymas	Viešųjų ryšių tinklų elektroninių ryšių infrastruktūros apsauga Viešųjų ryšių tinklų ir viešųjų elektroninių ryšių paslaugų saugumas ir vientisumas
Asmens duomenų teisinės apsaugos įstatymas	Fizinio asmens duomenų saugumas
Valstybės informacinių išteklių valdymo įstatymas	Valstybės informacinių išteklių sauga

3 lentelė. ***Informacinių išteklių gyvavimo ciklo ir saugumo reikalavimų taikymas nuo 2011 sausio 1 d. (* pažymėtas taikymas Lietuvos Respublikos Vyriausybei nepavaldžioms institucijoms)***

Ištekliai	Valstybės registrai	Žinybiniai registrai	Valstybės informacinės sistemos	Vidaus administravimo informacinės sistemos
Pavyzdžiai	Gyventojų, Juridinių asmenų	Kraujo donorų, Mokinių	Sodros, Vyriausiosios rinkimų komisijos	Dokumentų valdymo, finansų apskaitos
Gyvavimo ciklas	Apibrėžtas	Apibrėžtas	Apibrėžtas	Neapibrėžtas
Saugumas	Privalomas	Privalomas	Privalomas	Privalomas
				Rekomenduojamas*

Nuo 2012 m. sausio 1 d. įsigaliojus Lietuvos Respublikos Valstybės informacinių išteklių valdymo įstatymui, kuris valstybės informacinius išteklius apibrėžė kaip *informacijos, kurią valdo institucijos, atlikdamos teisės aktų nustatytas funkcijas, apdorojamos informacinių technologijų priemonėmis, ir ją apdorojančių informacinių technologijų priemonių visumą,* būtent šis įstatymas apibrėžė valstybės informacinių išteklių *kūrimą, tvarkymą, valdymą, naudojimą, priežiūrą, sąveiką, planavimą, finansavimą ir saugą*.

Apibrėžus valstybės informacinių išteklių gyvavimo ciklą ir jų saugumo užtikrinimą įstatymų lygiu, šie reikalavimai tapo privalomi visam Lietuvos viešajam sektoriui. Pažymėtina, kad Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme išskirti *kiti valstybės informaciniai ištekliai,* kuriuos *sudaro informacija, kurią valdo institucija, atlikdama vidaus administravimo funkcijas, apdorojamas kitomis informacinėmis sistemomis, ir šią informaciją apdorojančios informacinės sistemos. Šiame punkte minimų informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarką nustato Lietuvos Respublikos Vyriausybės įgaliotos institucijos.* Tačiau šiuo metu vidaus administravimo informacinėms sistemoms gyvavimo ciklo reikalavimai nėra apibrėžti, o įstatymo straipsnis, nustatantis valstybės informacinių išteklių saugą, vidaus administravimo informacinėms sistemos netaikomas.

Apibendrinant galima pažymėti, kad šiuo metu informacijos saugumo reikalavimai privalomai taikomi platesnei Lietuvos viešojo sektoriaus subjektų grupei, tačiau vidaus administravimo sistemų valdytojams, kurie nėra tiesiogiai pavaldūs Lietuvos Respublikos Vyriausybei, informacijos saugumo valdymo reikalavimai nėra privalomi (3 lentelė).

Informacijos saugumo valdymo tikslai

Remiantis galiojančiu Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu „tvarkant valstybės informacinius išteklius, privaloma įgyvendinti saugos priemones, skirtas užtikrinti duomenų ir informacijos tikslumą ir apsaugoti...

4 lentelė. ***Informacijos saugumo valdymo tikslų lyginamoji lentelė (sudaryta autoriaus)***

Informacijos saugumo valdymo tikslai	Lietuvos valstybės institucijoms galiojantys informacijos saugumo valdymo tikslai
Konfidencialumas	Privaloma įgyvendinti saugos priemones, skirtas ... apsaugoti nuo ... atskleidimo, neteisėto pasisavinimo, paskelbimo, pateikimo ar kitokio panaudojimo, taip pat nuo bet kokio kito neteisėto tvarkymo...
Prieinamumas	–
Vientisumas	Privaloma įgyvendinti saugos priemones, skirtas užtikrinti duomenų ir informacijos tikslumą ir apsaugoti juos ... nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, sugadinimo...

nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, sugadinimo, atskleidimo, neteisėto pasisavinimo, paskelbimo, pateikimo ar kitokio panaudojimo, taip pat nuo bet kokio kito neteisėto tvarkymo“, taigi galima daryti išvadą, kad šis reikalavimas atitinka tik du iš trijų pagrindinių informacijos saugumo valdymo (konfidencialumas, vientisumas ir prieinamumas) tikslų (4 lentelė), t. y. Lietuvos valstybės institucijoms neprivaloma užtikrinti informacijos prieinamumo tikslo.

Aptarti valstybės lygmens informacijos saugumo reikalavimai nustato ir atitinkamus institucinio lygmens informacijos saugumo politikos reikalavimus. Remiantis Bendrųjų elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimų nuostatomis, Lietuvos valstybės institucijos informacijos saugumo politiką išdėsto rengiamuose duomenų saugos nuostatuose, kuriuose nustato institucijoje taikomus informacijos saugumo užtikrinimo ir valdymo principus bei pagrindines taisykles, į kurias atsižvelgiant derinami institucijos informacinių sistemų veiklos ir naudojimo procesai, procedūros bei rengiami juos reglamentuojantys dokumentai.

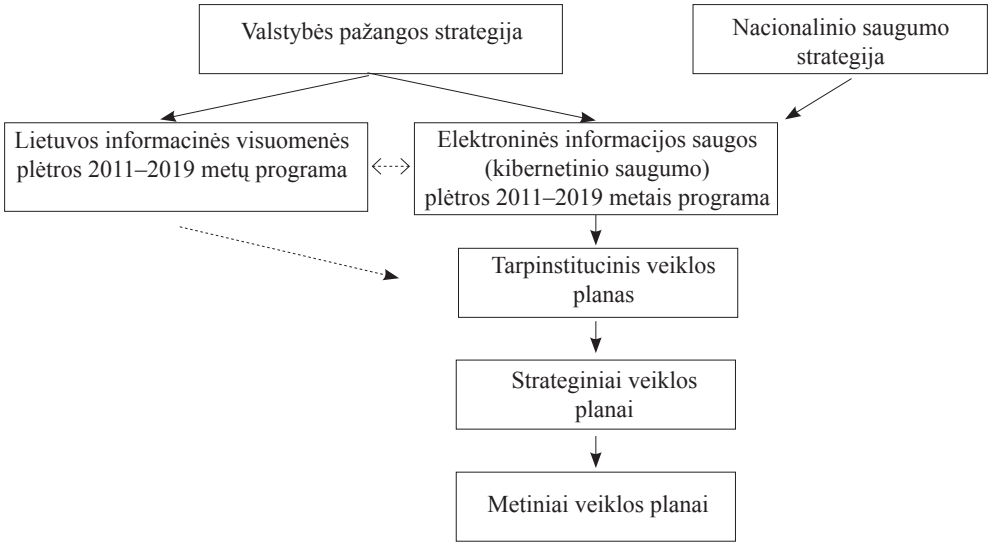
Informacijos saugumo valdymo strategija Lietuvos valstybės institucijose

Analizuojant Lietuvoje galiojančią informacijos saugumo valdymo strategiją išskirtini šie vertinimo kriterijai: informacijos saugumo valdymo politikos įgyvendinimo kryptys, prioritetai, ir uždaviniai; strategijos įgyvendinimo priemonės ir jų turinys (strateginės, žmogiškosios ir technologinės dimensijų kontekste); informacijos saugumo valdymo procesų ciklas, reagavimas į aplinkos pokyčius.

Informacijos saugumo valdymo politikos įgyvendinimo kryptys, prioritetai ir uždaviniai

Lietuvoje apibrėžta valstybės institucijų strateginių dokumentų hierarchija išdėstyta Strateginio planavimo metodikoje[2], kuri nustato planavimo dokumentų schemą. Vertinant šios metodikos nuostatas ir Lietuvoje galiojančius informacijos saugumo strateginius dokumentus galima išdėstyti Lietuvos viešojo sektoriaus strateginių in-

[2] Strateginio planavimo metodika: http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=397970&p_query=&p_tr2=2 [žiūrėta 2012 m. birželio 6 d.].



3 pav. ***Strateginių informacijos saugumo dokumentų schema (sudaryta autoriaus)***

formacijos saugumo dokumentų schemą (3 pav.).

Aukščiausio lygmens Lietuvos Respublikos strateginio dokumento, numatančio šalies vystymosi prioritetus ir perspektyvas iki 2030 m. – Valstybės pažangos strategijos[3] projekte, informacijos saugumas neišskirtas. Paminėtina, kad šis dokumentas tebėra svarstymo stadijos. Analizuojant kitų strateginių šalies dokumentų turinį ir tiriant sąsajas su informacijos saugumu, paminėtina 2012 m. Lietuvos Respublikos Seimo patvirtinta Nacionalinio saugumo strategija, kurioje informacijos ir kibernetinis saugumas minimi tarp pirmaeilių nacionalinio saugumo interesų[4]. Užtikrinti elektroninės erdvės saugumą ir patikimumą, didinti gyventojų ir įmonių pasitikėjimą elektronine erdve – vienas iš Lietuvos informacinės visuomenės plėtros 2011–2019 metų programos[5] prioritetų, tačiau kaip šios programos įgyvendinimo priemonės minimos tik elektroninės tapatybės patikimumo ir elektroninių dokumentų autentiškumo, vientisumo ir išsaugojimo problemos.

Detaliai informacijos saugumo tikslai, uždaviniai ir jų įgyvendinimo vertinimo kriterijai nustatyti 2011 m. birželio 29 d. Lietuvos Respublikos Vyriausybės patvirtintoje Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programoje[6]. Šio dokumento tikslas – apimti visus, ne tik viešąjį, sektorius,

[3] Lietuvos pažangos strategija 2030: http://www.lietuva2030.lt/images/stories/projektas.pdf [žiūrėta 2012 m. vasario 6 d.].

[4] Nacionalinio saugumo strategija: http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=428981&p_query=&p_tr2=2 [žiūrėta 2012 m. rugsėjo 5 d.].

[5] Lietuvos informacinės visuomenės plėtros 2011–2019 metų programa: http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=394457&p_query=&p_tr2= [žiūrėta 2012 m. birželio 5 d.].

[6] Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programa: http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=403385&p_query=&p_tr2=2 [žiūrėta 2012 m. liepos 12 d.].

tačiau uždavinių įgyvendinimo vertinimo kriterijų reikšmės nustatytos tik 2015 ir 2019 metams. Pažymėtina, kad tik kai kurios atsakingos institucijos patvirtindamos savo metinius veiklos planus numatė darbus, kuriuos planuoja atlikti informacijos saugumo valdymo srityje 2012 metais, pavyzdžiui, Vidaus reikalų ministerija[7]. Jokie kiti detalesni tarpinstituciniai veiklos planai dar nepatvirtinti, todėl šiuo metu nėra galimybių atlikti detalesnės dokumento analizės ir vertinimo.

Informacijos saugumo valdymo priemonės (dimensijų kontekste)

Analizuojant Lietuvos Respublikos Valstybės informacinių išteklių valdymo įstatymą, reikšminga šio įstatymo nuostata, kad „registro ar valstybės informacinių sistemų tvarkytojai privalo ... užtikrinti reikiamas *administracines, technines ir organizacines* duomenų saugos priemones ir tokių priemonių laikymąsi“, tačiau ši nuostata neleidžia vienareikšmiškai teigti, ar valstybės institucijoms privaloma taikyti priemones, apimančias pagrindines informacijos saugumo valdymo dimensijas (strateginę, technologinę ir žmogiškąją). Įvertinus kitą nagrinėjamo įstatymo nuostatą, kad „siekiant užtikrinti valstybės informacinių išteklių saugą, vadovaujantis Vyriausybės patvirtintais bendraisiais elektroninės informacijos saugos reikalavimais, rengiami, derinami ir tvirtinami valstybės informacinės sistemos ar registro saugos dokumentai“, galima daryti išvadą, kad tolesnė saugumo reikalavimų turinio analizė turėtų remtis informacijos saugumo valdymo dimensijų turinį gretinant su Bendrųjų elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimų turinio nuostatomis. Atlikus šių reikalavimų ir dimensijų (strateginės, technologinės ir žmogiškosios) turinio lyginamąją analizę galima teigti, kad Bendrųjų elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimų turinys iš esmės apima informacijos saugumo valdymo dimensijų turinį.

Informacijos saugumo valdymo procesų ciklas, reagavimas į aplinkos pokyčius

Valstybės lygmeniu informacijos išteklių valdymo ciklas analizuotas nagrinėjant informacijos saugumo valdymo objektą ir informacijos išteklių funkcionavimo (gyvavimo ciklo) aplinką (3 lentelė), institucijų lygmeniu – remiantis Bendraisiais elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimais, Lietuvos valstybės institucijos įpareigotos atlikti rizikos analizę ir atitikties vertinimą, nuolat peržiūrėti informacijos saugumo valdymą reglamentuojančius dokumentus ir valdyti sistemos pokyčius.

Informacijos saugumo auditas Lietuvos valstybės institucijose

Analizuojant Lietuvoje galiojančio informacijos saugumo auditą išskirtini šie vertinimo kriterijai – audito procesas, atsakomybės, periodiškumas ir vykdymo kontrolė; saugumo politikos įgyvendinimo strategijos ir informacijos saugumo veikėjų veiklos vertinimas.

[7] Lietuvos Respublikos vidaus reikalų ministerijos 2012-ųjų metų veiklos planas: http://www.vrm.lt/index.php?id=1174 [žiūrėta 2012 m. birželio 5 d.].

Valstybės kontrolė, kaip Lietuvos Respublikos aukščiausioji valstybinio audito institucija, yra atlikusi ne vieną auditą, kurio metu buvo vertinamas ir informacijos saugumo valdymas Lietuvos valstybės institucijose. Paskutinis auditas susijęs su informacijos saugumu – „Išankstinio tyrimo ataskaita. Strateginės informacijos sauga“[8]. Šio išankstinio tyrimo metu buvo nustatytos dvi pagrindinės su informacijos saugumo valdymu susijusios problemos, sietinos su informacijos saugumo valdymo politika ir įgyvendinimo strategija:

„1. Strateginio planavimo ir teisinio reglamentavimo trūkumai (neapibrėžti planavimo procesai, nepakankamas teisinis reglamentavimas, neidentifikuoti strateginės elektroninės informacijos saugos objektai).
2. Nesukurta strateginės elektroninės informacijos stebėsenos sistema ir nepakankamai apibrėžta šią sritį koordinuojančių institucijų kompetencija (nebaigta formuoti organizacinė struktūra ir valdymas, nenustatyta grėsmių ir pažeidžiamumų, prevencijos, incidentų pasekmių valdymo ir likvidavimo sistema).“[9]

Valstybės kontrolė šį auditą vykdė 2009 metais iki patvirtinant aptartą Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programą, tačiau šios išvados vertinamo empirinio tyrimo kontekste tebėra aktualios.

Informacijos saugumo vertinimą ir auditą apibrėžia Valstybės informacinių išteklių valdymo įstatymo nuostatos, kad Vidaus reikalų ministerija „organizuoja informacinių technologijų priemonių valdymo ir saugos vertinimą“ ir „atlieka saugos reikalavimų laikymosi priežiūrą“, bei įstatymo 14 straipsnio nuostatos, kad „vertinant valstybės informacinių sistemų, kuriomis apdorojama visai valstybei svarbi institucijos valdoma informacija, ir pagrindinių valstybės registrų, taip pat valstybės informacinių sistemų ir registrų, kuriems kurti ar modernizuoti viršytas Vyriausybės ar jos įgaliotos institucijos nustatytas lėšų dydis, valdymą ir saugą, ne rečiau kaip kartą per trejus metus atliekamas informacinių technologijų auditas“ ir „informacinių technologijų auditą atlieka visuotinai pripažintų tarptautinių organizacijų sertifikuoti informacinių sistemų auditoriai“. Pažymėtina, kad iki šiol nepatvirtinta šių nuostatų įgyvendinimo tvarka, informacijos saugumo valdymo audito priemonių nenumatyta ir aptartose Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos įgyvendinimo priemonėse.

Bendruosiuose elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimuose įtvirtinta nuostata, kad saugos politikos dokumentus valstybės institucijos su Vidaus reikalų ministerija privalo derinti prieš juos patvirtindamos ir kad „saugos dokumentai valstybės institucijoje turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per metus ... po rizikos analizės ar informacinių technologijų saugos atitikties vertinimo atlikimo arba valstybės institucijoje įvykus esminiams organizaciniams, sisteminiams ar kitiems pokyčiams“. Taigi galima teigti, kad egzistuoja administracinės priemonės, užtikrinančios informacijos saugumo auditą instituciniu lygmeniu, tačiau atkreiptinas dėmesys, kad nenumatyta procedūra, kaip turėtų būti kontroliuo-

[8] Išankstinio tyrimo ataskaita. Strateginės informacijos sauga: http://www.vkontrole.lt/failas_senas.aspx?id=3081 [žiūrėta 2012 m. birželio 2 d.].

[9] Ten pat.

jamas nuolatinis šių reikalavimų įgyvendinimas.

Atsižvelgiant į išdėstytas aplinkybes, galima teigti, kad organizacijų lygmenyje periodinis informacijos saugumo audito privalomumas nustatytas, valstybės lygmenyje nuostata dėl periodinio informacijos saugumo audito yra įtvirtinta įstatyme, tačiau šių reikalavimų įgyvendinimo ir kontrolės tvarka nėra užtikrinta.

Informacijos saugumo valdymo veikėjai Lietuvos valstybės institucijose

Analizuojant informacijos saugumo valdymo veikėjus išskirtini šie vertinimo kriterijai: informacijos saugumo organizavimas, atsakomybės ir įgaliojimai (kompetencijos).

Išanalizavus Lietuvos Respublikos ministerijų[10] ir kitų institucijų nuostatus ir vykdomas funkcijas, vertinant informacijos saugumo valdymo organizavimą ir kontrolę galima išskirti šiuo metu didžiausią įtaką tam turinčias institucijas – Vidaus reikalų ministeriją (pagrindinės funkcijos informacijos saugumo kontekste – valstybės institucijų informacijos saugumo politikos formavimas), Susisiekimo ministeriją (ryšių saugumo politikos formavimas), Teisingumo ministeriją (asmens duomenų apsaugos politikos formavimas), Ryšių reguliavimo tarnybą (ryšių operatorių priežiūra, saugumo incidentų stebėsena), Policijos departamentą (elektroninių nusikaltimų tyrimas).

Institucijų veiklos koordinavimui dar 2006 m. Lietuvos Respublikos Vyriausybė iš minėtų institucijų atstovų sudarė nuolatinę Elektroninės informacijos saugos koordinavimo komisiją[11]. Šios komisijos sudėtis buvo ne kartą keista, tačiau vertinant komisijai pavestas funkcijas galima teigti, kad komisija vykdė koordinacines, rekomendacines ir stebėsenos funkcijas, bet neturėjo įgaliojimų tiesiogiai duoti nurodymų ar priimti sprendimų, privalomų kokiems nors ūkio subjektams. Nagrinėjant komisijos veiklą pažymėtina, kad ši komisija atliko plačią esamos situacijos analizę ir padėjo pamatus rengti naują strateginį dokumentą – Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programą. Ši programa, o kartu ir atsakingi jos įgyvendintojai buvo patvirtinti Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. sprendimu[12]. Programos įgyvendinimo koordinatoriumi paskirta Lietuvos Respublikos vidaus reikalų ministerija, kuriai pavesta vadovauti ir reorganizuotam kolektyviniam koordinaciniam organui – Elektroninės informacijos saugos (kibernetinio saugumo) koordinavimo komisijai[13] (4 pav.).

Siekiant įvertinti institucijų galimybes vykdyti pavestas informacijos saugumo valdymo koordinacines funkcijas, atlikta šių institucijų žmogiškųjų išteklių analizė. Analizės metu išnagrinėti į komisiją įeinančių institucijų ir jų padalinių, tiesiogiai

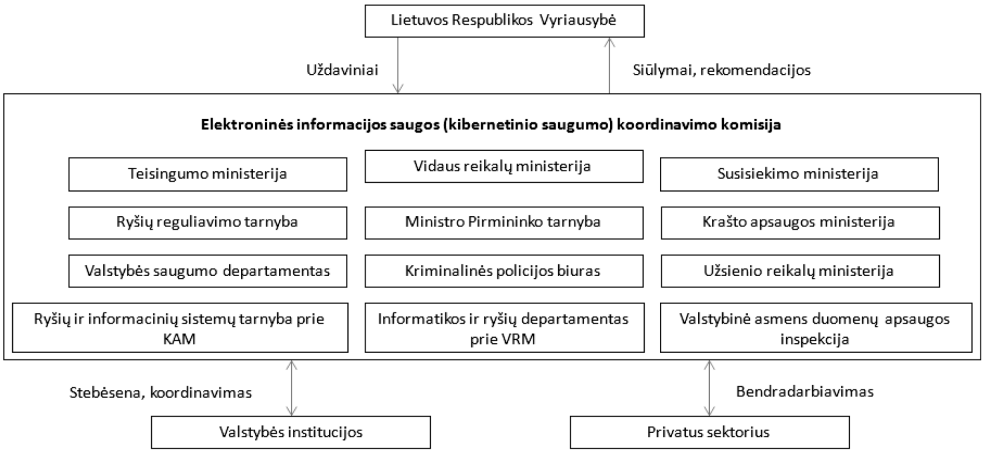
---

[10] Lietuvos Respublikos ministerijos: http://www.lrv.lt/lt/vyriausybe/apie-vyriausybe/ministerijos/, [žiūrėta 2012 m. liepos 2 d.].

[11] Lietuvos Respublikos Vyriausybės nutarimas: http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=288880&p_query=&p_tr2= [žiūrėta 2012 m. liepos 2 d.].

[12] Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programa: http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=403385&p_query=&p_tr2=2 [žiūrėta 2012 m. liepos 12 d.].

[13] Lietuvos Respublikos Vyriausybės nutarimas: http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=423568 [žiūrėta 2012 m. birželio 6 d.].



4 pav. ***Elektroninės informacijos saugos (kibernetinio saugumo) koordinavimo komisijos sudėtis ir sąsajos (sudaryta autoriaus)***

atsakingų už informacijos saugumo koordinavimo funkcijų vykdymą, nuostatai bei šių padalinių darbuotojų pareigybių aprašymai.

Išanalizavus Vidaus reikalų ministerijos (VRM) administracijos padalinių[14] nuostatus buvo identifikuotas Elektroninės valdžios politikos skyrius, kurio nuostatuose[15] tiesiogiai įrašytos atsakomybės už informacijos saugumą: „formuoti valstybės politiką informacinių technologijų saugos srityje, organizuoti, koordinuoti ir kontroliuoti jos įgyvendinimą“. Iš viso šiame skyriuje dirba 10 darbuotojų, tačiau išnagrinėjus jo valstybės tarnautojų funkcijas[16] buvo identifikuotas vienas valstybės tarnautojas, kuriam saugumo koordinavimo funkcijos priskirtos kartu su kitomis (skyriaus vadovas), ir vienas valstybės tarnautojas, kurio funkcijos tiesiogiai susijusios tik su informacijos saugumo valdymu. Informatikos ir ryšių departamente prie Vidaus reikalų misterijos (IRD prie VRM) identifikuotas Saugos skyrius[17], kurį sudaro šeši valstybės tarnautojai, tačiau, įvertinus jiems priskirtas ir įslaptintų sistemų priežiūros funkcijas, galima išskirti tris darbuotojus, kurių funkcijos tiesiogiai susijusius su informacijos saugumo valdymu.

Nagrinėjant atitinkamas Lietuvos Respublikos susisiekimo ministerijos (SM) funkcijas, buvo identifikuotas Informacinės visuomenės politikos departamento Elektroninių ryšių skyrius[18], kuriame dirba du valstybės tarnautojai, ir jų bent viena

[14] Lietuvos Respublikos vidaus reikalų ministerija: Ministerijos administracijos padaliniai: http://www.vrm.lt/index.php?id=43 [žiūrėta 2012 m. birželio 10 d.].

[15] Lietuvos Respublikos vidaus reikalų ministerijos Elektroninės valdžios politikos skyrius: http://www.vrm.lt/fileadmin/Padaliniu_failai/El_valdzios_politikos_sk/20110324_Nr1V-244_EVPS_nuostatai_pasirasyti.pdf [žiūrėta 2012 m. birželio 10 d.].

[16] Lietuvos Respublikos vidaus reikalų ministerija : Kontaktai ir struktūra: http://www.vrm.lt/index.php?id=48 [žiūrėta 2012 m. birželio 10 d.].

[17] Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos: http://www.ird.lt/viewpage.php?page_id=12 [žiūrėta 2012 m. birželio 10 d.].

[18] Lietuvos Respublikos susisiekimo ministerija: http://www.transp.lt/lt/struktura_ir_kontaktai/kontaktai/ministerijos_kontaktai [žiūrėta 2012 m. birželio 10 d.].

iš vykdomų funkcijų siejasi su dalyvavimu koordinuojant informacijos saugumo užtikrinimą (vieno bendra ir kito el. ryšių srityje). Lietuvos Respublikos teisingumo ministerijoje (TM) išskirtas Registrų departamento Registrų teisinio reguliavimo skyrius[19]. Šiame skyriuje dirba šeši valstybės tarnautojai, penkių viena iš pavestų funkcijų susijusi su asmens duomenų apsauga ir vieno valstybės tarnautojo funkcijos tiesiogiai siejasi su asmens duomenų apsauga. Ryšių reguliavimo tarnyboje (RRT), pagal interneto svetainėje skelbiamą informaciją[20], yra atskiras struktūrinis padalinys – Tinklų ir informacijos saugumo departamentas, kuriame dirba septyni darbuotojai, trijų iš jų funkcijos priskirtinos tiesiogiai informacijos saugumo problemų sprendimui, dar dviejų – iš dalies. Valstybinėje asmens duomenų apsaugos inspekcijoje (VDAI) pagal etatų sąrašą ir paskelbtus pareigybių aprašymus[21] buvo identifikuoti trys valstybės tarnautojai, kurių viena iš funkcijų – asmens duomenų, apdorojamų informacinėmis technologijomis, apsauga.

Kriminalinės policijos biure galima identifikuoti atskirą Nusikaltimų elektroninėje erdvėje tyrimo valdybą[22], tačiau jos etatų sąrašas ir konkrečios funkcijos internete neskelbiamos.

Lietuvos Respublikos Ministro Pirmininko tarnybos etatų sąrašuose[23] nepavyko identifikuoti padalinio ar valstybės tarnautojo, tiesiogiai atsakingo už informacijos saugumą. Lietuvos Respublikos krašto apsaugos ministerija (KAM), Ryšių ir informacinių sistemų tarnyba prie KAM, Lietuvos Respublikos užsienio reikalų ministerija bei Valstybės saugumo departamentas savo padalinių funkcijų ir darbuotojų pareigybių aprašymų internete neskelbia.

Bendri žmogiškųjų išteklių, atsakingų už informacijos saugumo koordinavimo funkcijų vykdymą, skaičiai pateikiami 5 lentelėje. Žmogiškieji ištekliai skaičiuoti nevertinant atitinkamų valstybės institucijų vadovų ir bendrųjų funkcijų padalinių, tokių kaip biuro administravimo, teisės ir pan., kurie prisideda prie visų organizacijos funkcijų vykdymo.

Apibendrinant Lietuvos Respublikos valstybės institucijų, atsakingų už informacijos saugumo valdymą, funkcijas galima teigti, kad funkcijos yra padalytos tarp pagrindinių institucijų, veiksmų koordinavimui užtikrinti specialiai sudaryta Elektroninės informacijos (kibernetinio saugumo) koordinavimo komisija. Išanalizavus žmogiškuosius šių institucijų išteklius akivaizdu, kad institucijos (ypač pagrindinis koordinatorius VRM), neturi pakankamai žmogiškųjų išteklių koordinuoti informacijos saugumo Lietuvos valstybės institucijose valdymą.

Vadovaujantis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu ir kitais aptartais teisės aktais, pagrindinis institucinio lygmens informacijos saugumo valdymo veikėjas – saugos

---

19 Lietuvos Respublikos teisingumo ministerija: http://www.tm.lt/struktura/kontaktineinfo/12 [žiūrėta 2012 m. birželio 10 d.].

20 Lietuvos Respublikos Ryšių reguliavimo tarnyba – Struktūra ir kontaktai » Struktūra ir kontaktai » Kontaktai: http://www.rrt.lt/lt/struktura-ir-kontaktai/struktura-ir-kontaktai_838/kontaktai.html [žiūrėta 2012 m. birželio 10 d.].

21 Valstybinė duomenų apsaugos inspekcija: http://www.ada.lt/index.php?lng=lt&action=page&id=57 [žiūrėta 2012 m. birželio 10 d.].

22 Policijos departamentas prie VRM » Kriminalinės policijos biuras: http://www.policija.lt/index.php?id=7441&ou=3053 [žiūrėta 2012 m. birželio 10 d.].

23 LR Vyriausybė – Ministro Pirmininko tarnybos kontaktai: http://www.lrv.lt/lt/kontaktai/ministro-pirmininko-tarnyba/ [žiūrėta 2012 m. birželio 10 d.].

5 lentelė. ***Žmogiškieji ištekliai Lietuvos valstybės institucijose, atsakingose už informacijos saugumo valdymo koordinavimą (sudaryta autoriaus)***

Institucija	Darbuotojų, tiesiogiai vykdančių funkcijas, susijusias su informacijos saugumu, skaičius	Darbuotojų, kurių funkcijos iš dalies susijusios su informacijos saugumu, skaičius
VRM	1	1
IRD prie VRM	3	-
SM	1	1
TM	1	5
RRT	3	2
VDAI	3	-

įgaliotinis, kurį privalo paskirti kiekvienos valstybės institucijos, valdančios informacinius išteklius, vadovas. Saugos įgaliotinis atsako už saugos reikalavimų vykdymą ir atlieka kitas teisės aktuose nustatytas funkcijas.

Informacijos saugumo valdymo branda Lietuvos valstybės institucijose

Analizuojant informacijos saugumo valdymo brandą išskirtini šie vertinimo kriterijai – informacijos saugumo brandos lygiai; informacijos saugumo brandos vertinimas.

Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programoje numatyta, kad bus vertinamas informacinių sistemų valdytojų elektroninės informacijos saugos valdymo brandos lygis, tačiau Lietuvos valstybės institucijoms informacijos saugumo brandos lygiai teisės aktuose neapibrėžti, vertinimo sistema nenumatyta.

Informacijos saugumo valdymo kokybinio tyrimo rezultatų analizė

Empirinio tyrimo metodologijoje pažymėta, kad atvejo dokumentų turinio analizės rezultatams pagrįsti tikslinga juos patikrinti kokybiniu tyrimu. Kaip kokybinio tyrimo metodas pasitelkta ekspertų apklausa. Ekspertams buvo formuluojamos penkios pagrindinės klausimų grupės.

1. Informacijos saugumo valdymo objektas ir tikslai.

Ekspertai pripažino esamo informacijos saugumo valdymo objekto – informacijos, valdomos valstybės informaciniais ištekliais, – trūkumus. Pažymėta, kad objektu galėtų būti ir kompiuterių tinklai, taip siekiant apsaugoti informaciją, perduodamą tarp informacinių sistemų. Ekspertų manymu, informacijos saugumo objektas galėtų būti ir bet kuri institucijos tvarkoma informacija, tačiau šią istoriškai susiklosčiusią situaciją labai sudėtinga pakeisti, tam reikėtų nemažai išteklių ir pastangų.

Informacinėse sistemose ir registruose valdoma svarbiausia valstybei informacija, tačiau iki 2012 m. sausio 1 d. reikalavimai privalomai buvo taikomi tik Lietuvos Respublikos Vyriausybei pavaldžioms institucijos. Taip pat būta neapibrėžtumo dėl informacijos saugumo valdymo reikalavimų taikymo vidaus administravimo informaciniams ištekliams. Sudėjus bendrą institucijose valdomos informacijos kiekį, kuriam saugumo reikalavimai nebuvo taikomi, tai galima suvokti kaip labai didelę

saugumo spragą. Naujasis Valstybės informacinių išteklių valdymo įstatymas apėmė daug didesnį išteklių skaičių ir praktiškai dengia visas informacijos valdymo formas institucijose, o vertinant tai, kad institucijos, valdančios kelis ar keliolika informacijos išteklių, gali jungti jų saugos reglamentavimą vienu pagrindiniu dokumentu (t. y. išvengti atskiro dokumento kiekvienam informaciniam ištekliui), šis įstatymas sudaro geras prielaidas informacijos saugai užtikrinti.

Ekspertai taip pat pažymėjo, kad diskusijos, kas turėtų būti informacijos saugumo objektas, kyla ir Europos Sąjungos mastu, tačiau vienareikšmiško atsakymo nėra. Kai kuriose šalyse kaip saugumo objektas labiau ryškinami kompiuterių tinklai, kibernetinė erdvė.

Ekspertų manymu, informacijos saugumo tikslai turėtų labiau priklausyti nuo institucijų valdomų informacinių išteklių, turėtų būti leidžiama pačioms institucijoms spręsti, kuris tikslas galėtų būti jų aukštesnis prioritetas. Net keli ekspertai pareiškė nuomonę, kad detaliuose techniniuose reikalavimuose per daug sureikšmintas prieinamumo tikslas, pavyzdžiui, 15 min. sistemos atkūrimo reikalavimas pirmos kategorijos informacinėms sistemoms (svarbiausioms) Šis reikalavimas neproporcingai didelis net ir labai pažengusioms institucijoms, turinčioms patikimus duomenų centrus, todėl dažnai įgyvendinamas tik formaliai, nes realus jo įgyvendinimas būtų labai brangus. Išsiskyrė ekspertų nuomonės, kurie kriterijai institucijoms galėtų būti svarbūs: pareikšta nuomonė, kad tai nėra tirta ir būtų labai aktualu išsiaiškinti, o kitų ekspertų teigimu, institucijoms svarbesni vientisumo ir konfidencialumo tikslai.

2. Informacijos saugumo valdymo organizavimas, kompetencijos ir atsakomybės.

Ekspertai pažymėjo, kad neseniai iš naujo sudaryta Elektroninės informacijos saugos (kibernetinio saugumo) koordinavimo komisija, joje atsirado Užsienio reikalų ministerijos, Valstybės saugumo departamento atstovų. Tai leidžia tikėtis naujų darbų. Komisijai vadovauti paskirta pagrindinė informacijos saugumo koordinatorė – Vidaus reikalų ministerija. Sudarytas sąrašas teisės aktų, kuriuos būtina parengti naujam Valstybės informacinių išteklių valdymui įgyvendinti, tarp jų yra ir susijusių su saugumu.

Beveik visi ekspertai pažymėjo bendrą tendenciją – kompetencijos ir žmonių stygių. Pagrindinė koordinatorė Vidaus reikalų ministerija, turėjusi specialius informacijos saugumo valdymo problemų koordinavimo ir sprendimo padalinius, per pastaruosius keletą metų dėl įvairių reorganizacijų ir kitų priežasčių beveik visai išbarstė sukauptą informacijos saugumo kompetenciją. Panašios tendencijos pastebimos ir kitose institucijose, atsakingose už atskiras su saugumu sietinas funkcijas. Turint esamą etatų skaičių, sunku tikėtis proveržio ar didelių darbų. Jau kurį laiką pastebimas lėtas reikalingų teisės aktų rengimas, užtrunkantis nuostatų ir kitų saugos dokumentų derinimas. Taip pat išdėstyta nuomonė, kad saugos atsakomybė po truputį išdalyta daugeliui institucijų, atskirų sričių koordinatorių apstu, o realius darbus dirbti nėra kam. Turint po kelis žmones institucijose, ypač vertinant biurokratinio darbo mastus, tikrai negalima nuveikti didelių darbų. Tad iki naujų rinkimų mažai tikėtinas koks nors proveržis. Galbūt daugiau tvarkos padėtų įnešti ir Valstybės

kontrolės aktyvesnė veikla analizuojant saugos įgyvendinimą institucijose. Ekspertai pastebėjo Valstybės kontrolės indėlį į informacijos saugumo kokybės gerėjimą, atskiri (nors ir ne sisteminio pobūdžio) valstybės institucijų patikrinimai mobilizuoja, rastų trūkumų šalinimo priemonių planai padeda institucijoms geriau tenkinti galiojančius informacijos saugumo reikalavimus ir sekti „gerosios praktikos“ pavyzdžiais.

Kita tendencija – ekspertai pastebėjo tiek verslo, tiek akademinio sluoksnių pageidavimus dalyvauti platesnio pobūdžio konsultaciniame procese. Nauda būtų veikianti idėjų generavimo, konsultacinė struktūra. Čia būtų galima pasimokyti iš Estijos, kurioje labai sėkmingai dirba savanoriška organizacija – Saugumo lyga. Ši organizacija aktyviai veikia iškilus įvairiems incidentams, padeda su sunkumais susidūrusioms organizacijoms, veikia kaip reagavimo į incidentus (CERT) padalinio rezervas. Pažymėtina, kad nors ji savanoriška, tačiau į šią organizaciją priimami tik kompetentingi saugos profesionalai, institucija sukarinta, veikia pagal griežtas taisykles, o valstybė išlaiko tik nedidelę administraciją, visi kiti dirba neatlygintinai. Beje, šiuo pavyzdžiu ketina sekti ir kaimynai latviai, susidomėjo ir kitos šalys.

Ekspertai taip pat pastebėjo, kad kritinės (ypatingos svarbos) infrastruktūros klausimai sprendžiami netinkamai – nėra ne tik vienareikšmiškai atsakingos institucijos, bet net ir šios infrastruktūros apibrėžimo.

3. Informacijos saugumo brandos vertinimo kriterijai ir poreikis. Institucijų situacija.

Ekspertų teigiamu, pagal Kibernetinio saugumo programą numatytas brandos kismo stebėjimas, tačiau kol kas nėra bendros metodikos brandai vertinti, nevykdomi platesni tyrimai. Tokia metodika galėtų remtis COBIT, ITIL ar kitos tarptautinės metodikos principais. Iš ekspertų vertinimo galima numanyti, kad maždaug du trečdaliai Lietuvos institucijų atitinka pirmą, trečdalis – antrą brandos lygį (iš penkių), galbūt su labai retomis išimtimis. Ekspertai pastebi ir tai, institucijos paliktos savieigai, stipresnės juda, silpnesnėms labai sunku. Informacijos saugumo vertinimai – labiau proginės veiklos nei sistema. Net ir didelės institucijos, investavusios nemažai lėšų į informacinių sistemų saugumą, nesugeba išvengti incidentų, o taip neturėtų būti. Taigi, galima numanyti, kad institucijų branda labai įvairi: tikrai yra smarkiai pažengusių institucijų, tačiau kas dedasi, pavyzdžiui, savivaldybėse (ypač mažesnėse), labai sunku pasakyti. Tyrimai šiame kontekste nedaryti ir išties būtų aktualūs.

Brandos lygis ar jo siekimas taip pat galėtų būti siejamas su institucijų valdomų informacinių išteklių svarba (kategorija). Kuo svarbesnius išteklius valdo institucija, tuo aukštesnio brandos lygio ji turėtų siekti.

4. Informacijos saugumo funkcijų centralizavimo poreikis ir apimtys.

Ekspertų teigimu, jau dabar Valstybės informacinių išteklių valdymo įstatyme yra įteisintas kai kurių veiklų koncentravimas ir centralizavimas valstybės informacinių išteklių sąveikumo platformoje.

Iš esmės funkcijos galėtų būti centralizuojamos įvairiai, pavyzdžiui, „vyriausybės debesis“ (angl. *Government Cloud*), apsaugotas valstybės ryšių tinklas, kolektyvinės ryšių gynybos sistemos ar kitos infrastruktūrinės priemonės. Argumentuotam tokių funkcijų sąrašo sudarymui rei-

kėtų detalios valstybės institucijų turimų priemonių analizės.

Kitas labai svarbus veiksnys – stipri koordinavimo institucija, turinti pakankamai kompetencijos koordinuoti darbus, rengti metodinius dokumentus, mokymus, pagal vieną metodiką ir vertinimo kriterijus organizuoti centralizuotus saugos vertinimą, auditą, rizikos analizę ir pan.

Esant tokiai kompetencijos situacijai viešajame sektoriuje, ekspertų nuomone, reikia galvoti apie kompetencijų centrus, nes ilgainiui institucijos nesugebės kiekviena sau išlaikyti aukštos kompetencijos specialistų. Kompetencijos centrai galėtų būti kuriami ir pagal funkcines sritis, pavyzdžiui, savo kompetenciją ir kitus pajėgumus galėtų sujungti Valstybinė mokesčių inspekcija, SODRA, Muitinės departamentas.

Ekspertų manymu, brandesnės institucijos galbūt gali „savimi pasirūpinti“, tačiau mažiau brandžioms tikrai praverstų centralizuota pagalba. Būtų verta svarstyti ir galimybę centralizuotai paskirti kokiai nors institucijai tokią funkciją kaip finansinių išteklių paieška.

5. Informacijs saugumo stebėsenos ir kontrolės sistemos kūrimas bei vertinimo kriterijai.

Tokia sistema turėtų būti esminis koordinavimo institucijos darbo įrankis. Numatytos kelios priemonės Kibernetinio saugumo programos įgyvendinimo plane, iš tiesų tokios sistemos poreikis yra, tačiau su esama kompetencija ir ištekliais sunkiai tikėtina reikšminga stebėsena ir kontrolė. Galėtų būti stebimas ir organizacijų brandos lygis bei jo kitimas.

Ekspertų pastebėta, kad šiuo metu jau taikoma automatizuota incidentų ir anomalijų tinkluose stebėsenos sistema.

Empirinio tyrimo rezultatų aptarimas

Išanalizavus informacijos saugumo valdymą Lietuvos valstybės institucijose, galima teigti, kad teorinio integralaus informacijos saugumo valdymo modelio pagrindu suformuota vertinimo prieiga leido identifikuoti informacijos saugumo valdymo trūkumus visuose lygiuose.

Informacijos saugumo politikos lygmeniu buvo identifikuota, kad informacijos saugumo politiką valstybėje nustato Lietuvos Respublikos Valstybės informacinių išteklių valdymo įstatymas, institucijose – saugumo politikos dokumentas (duomenų saugos nuostatai). Šie dokumentai informacijos saugumo valdymo objektu įvardija informaciją, valdomą pasitelkiant informacinius išteklius. Lietuvos valstybės institucijoms galiojantys informacijos saugumo valdymo reikalavimai šiuo metu tiesiogiai netaikomi vienai informacinių išteklių rūšiai – vidaus administravimo sistemoms. Kokybinio tyrimo rezultatai išryškino vyraujančią ekspertų nuomonę, kad nors informacijos saugumo valdymo objektas remiasi valstybės informaciniais ištekliais ir turi trūkumų, tačiau jo pakeitimas kainuotų daug lėšų. Ekspertų nuomone, tinkamesnis sprendimas – patvirtinti trūkstamus informacijos saugumo valdymo reikalavimus, kompleksiškai taikyti vidaus administravimo sistemos ir informacijos saugumo valdymą reglamentuojančius dokumentus visiems konkrečios institucijos valdomiems informacijos ištekliams.

Dokumentų turinio analizė leido identifikuoti, kad informacijos saugumo valdymo reikalavimai tiesiogiai apima tik du iš trijų informacijos saugumo valdymo tikslų – konfidencialumą ir vientisumą, tačiau neapima prieinamumo. Šio tikslo siekis

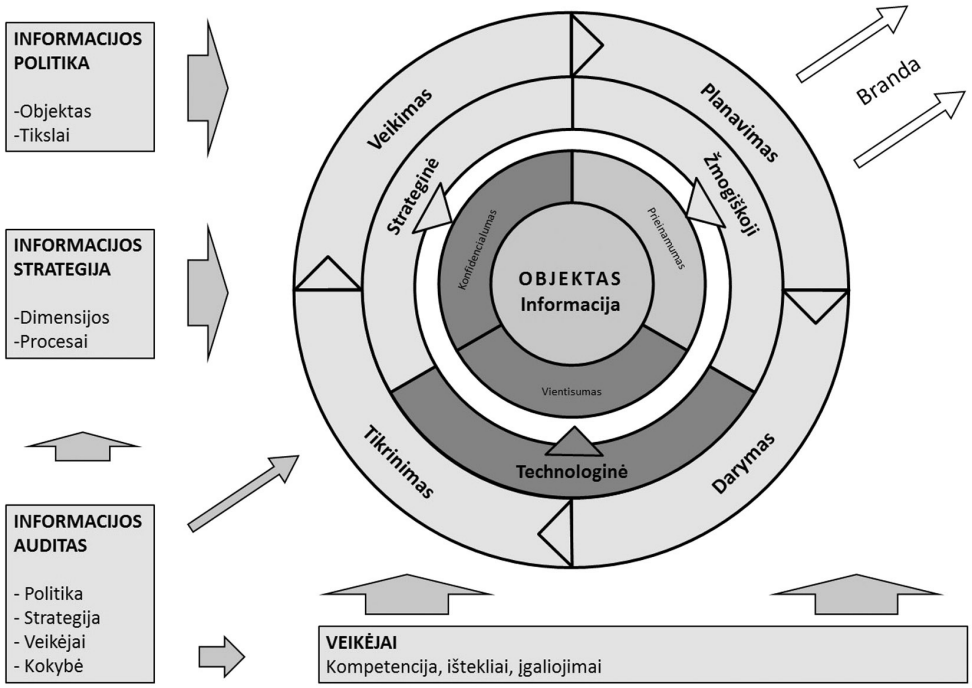
tampa ypač aktualus vertinant pastarųjų metų tendencijas – įvairias kibernetinės erdvės atakas, kurioms pavykus informacijos ištekliai tampa neprieinami. Ekspertai taip pat išsakė abejonių dėl tapačiai taikomų informacijos saugumo tikslų visoms valstybės institucijoms. Jų manymu, institucijos turėtų turėti galimybę nustatyti šių tikslų taikymo prioritetus, atsižvelgdamos į institucijoje valdomos informacijos specifiką.

Informacijos saugumo strategijos lygmeniu dokumentų turinio tyrimo metu buvo identifikuota, kad valstybės institucijos neįpareigotos rengti atskiros informacijos saugumo strategijos, o valstybės lygmeniu ši strategija parengta, tačiau dar nėra patvirtintų detalių įgyvendinimo planų. Vertinant taikomų informacijos saugumo valdymo priemonių turinį informacijos saugumo dimensijų (strateginės, žmogiškosios, technologinės) kontekste, svarbios ekspertų įžvalgos dėl kompetencijos trūkumo (žmogiškosios dimensijos sudedamoji dalis), nevertinamo ekonominio konteksto nustatant racionaliai nepagrįstų, brangiai kainuojančių techninių priemonių privalomą taikymą (strateginės dimensijos sudedamoji dalis). Taip pat paminėta, kad informacijos saugumo valdymo procesas apibrėžtas tiek įstatymų, tiek jų įgyvendinamųjų aktų, tačiau nėra užtikrinama proceso nuolatinio taikymo ir kontrolės tvarka.

Informacijos saugumo audito lygmeniu teorinis tyrimas leido nustatyti, kad institucijos privalo vykdyti periodinius auditus – Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas bei kiti reikalavimai apibrėžia informacijos saugumo audito vykdymą valstybės ir institucijų lygmeniu, tačiau šių reikalavimų įgyvendinimo ir kontrolės tvarka nėra nustatyta. Kokybiniame tyrime dalyvavę ekspertai taip pat pabrėžė šį trūkumą. Minima problema lemia tai, kad valstybės institucijos daugumą informacijos saugumo valdymo pareigų atlieka tik formaliai, neužtikrinama informacijos saugumo reikalavimų įgyvendinimo kontrolė, nežinoma reali situacija Lietuvos valstybės institucijose, nevaldomi informacijos saugumo procesai.

Informacijos saugumo brandos lygmeniu atvejo analizė parodė, kad informacijos saugumo brandos lygiai ir vertinimo sistema nėra nustatyti. Kokybinio tyrimo metu ekspertai beveik vieningai pabrėžė brandos lygių nustatymo ir vertinimo pranašumus. Pagal institucijų brandos lygį galėtų būti parenkamos informacijos saugumo valdymo priemonės, svarbesnius išteklius valdančios institucijos turėtų siekti aukštesnio brandos lygmens.

Informacijos saugumo veikėjų (kompetencijos) lygmeniu dokumentinis tyrimas atskleidė, kad atsakingos už informacijos saugumo valdymą institucijos yra paskirtos, tačiau išanalizavus kompetentingų institucijų funkcijas ir etatų sąrašus tapo akivaizdu, kad koordinuojančios institucijos nėra pajėgios vykdyti joms iškeltų uždavinių. Kokybinis tyrimas patvirtino šiuos rezultatus, ekspertai pažymėjo, kad nors yra sudarytas kolegialus koordinavimo organas, paskirtos kompetentingos institucijos, tačiau informacijos saugumo organizavimas pasižymi menka institucijų kompetencija, specialistų trūkumu, lėtu paskirtų užduočių vykdymu. Ekspertų manymu, šią situaciją padėtų spręsti kompetencijos centrų kūrimas, pagrįstas funkcijų optimizavimas ir centralizavimas, visuomeninės konsultacinės tarybos sukūrimas.



5 pav. ***Integralaus informacijos saugumo valdymo modelio įgyvendinimas Lietuvos valstybės institucijose***

Apibendrinti informacijos saugumo valdymo Lietuvos valstybės institucijose tyrimų rezultatai pateikiami 5 paveiksle. Šiame paveiksle tamsiai pilka spalva išskirti integralaus informacijos saugumo valdymo modelio elementai, kurie yra apibrėžti ir taikomi Lietuvos valstybės institucijose, šviesiai pilka spalva – ne iki galo apibrėžti arba apibrėžti, tačiau neįgyvendinami, balta spalva – neapibrėžti ir neįgyvendinami.

Išvados ir siūlymai

1. Remiantis teoriniu integralaus informacijos saugumo valdymo modeliu suformuota vertinimo prieiga Lietuvos valstybės institucijose ir identifikuotos spragos visuose informacijos saugumo valdymo lygmenyse leidžia teikti šiuo siūlymus:
   a) Informacijos saugumo valdymo politikos lygmuo – apibrėžti trūkstamus gyvavimo ciklo ir informacijos saugumo valdymo reikalavimus vidaus administravimo informacinėms sistemoms. Į informacijos saugumo valdymo reikalavimus įtraukti informacijos prieinamumo tikslą;
   b) Informacijos saugumo strategijos lygmuo – patvirtinti valstybinių strategijų įgyvendinimo priemonių planus. Nustatant konkrečias informacijos saugumo valdymo priemones atsižvelgti į informacijos saugumo valdymo dimensijų kontekstą, ypač strateginės

ir žmogiškosios, kurios apima šiuo metu nereglamentuojamus ekonominio naudingumo, kompetencijos ir kitus aspektus. Užtikrinti, kad nustatytas informacijos saugumo valdymo procesas vyktų nuolat, apibrėžti proceso ciklišKumo kontrolę;

c) Informacijos saugumo audito lygmuo – nustatyti informacijos saugumo valdymo audito įgyvendinimo ir kontrolės tvarką;
d) Informacijos saugumo veikėjų lygmuo – sustiprinti įgaliotas institucijas, užtikrinant, kad jos galėtų kokybiškai vykdyti pavestas funkcijas. Konkrečiai valstybės institucijai nustatyti aiškius įgaliojimus ir pareigą kontroliuoti, kaip Lietuvos valstybės institucijos įgyvendina informacijos saugumo valdymo reikalavimus. Suburti visuomeniniais pagrindais veikiančią informacijos saugumo valdymo konsultacinę tarybą, jungiančią viešojo, akademinio bei privataus sektorių atstovus;
e) Informacijos saugumo brandos lygmuo – apibrėžti informacijos saugumo brandos lygius ir nustatyti jų vertinimo tvarką.

Apibendrintai įvertinus informacijos saugumo valdymą Lietuvos valstybės institucijose, galima teigti, kad šiuo metu valdomos tik atskiros informacijos saugumo užtikrinimo dalys, trūksta visuminio požiūrio, netaikomi įrankiai, kurie leistų sukurti ir išlaikyti valdomą informacijos saugumą, kaip objektyvią saugumo būseną.

2. Patvirtinus pagrindinius teorinio dokumentinio tyrimo rezultatus empirinio tyrimo rezultatais, galima teigti, kad suformuota informacijos saugumo valdymo prieiga padeda objektyviai įvertinti informacijos saugumo valdymą bei suformuoti siūlymus efektyviam informacijos saugumo valdymui užtikrinti.
3. Atliktų empirinių tyrimų rezultatai leidžia konstatuoti, kad teorinis integralus informacijos saugumo valdymo modelis gali būti taikomas identifikuoti ir pašalinti informacijos saugumo valdymo trūkumus bei užtikrinti kompleksišką ir efektyvų informacijos saugumo valdymą praktiniu lygmeniu.

LITERATŪRA IR ŠALTINIAI

ASHENDEN, Debi (2008). Information Security management: A human challenge? *Information Security Technical Report*, 2008 November, vol. 13, Issue 4, p. 195–201.

ANDERSON, Ross; MOORE, Tyler (2009). *Information security*: where computer science, economics and psychology meet [interaktyvus]. [žiūrėta 2010 m. liepos 16 d.]. Prieiga per internetą: <http://rsta.royalsocietypublishing.org/content/367/1898/2717.short? rss=1>.

BAKHSHI, Taimur; PAPADAKI, Maria; FURNELL, Steven (2009). Social engineering: assessing vulnerabilities in practice. *Information Management & Computer Security*, vol. 17 (1), p. 53–63.

BOTHA, Hannerí; BOON, J. A. (2003). *The Information Audit: Principles and guidelines*. Libri, Munich: Saur Verlag, vol. 53, p. 23–38.

CHAFFEY, Dave; WHITE, Gareth (2011). *Business information management: improving performance using information systems*. Harlow: Financial Times Prentice Hall. 620 p.

CHANG, Shuchih Ernest; LIN, Chin-Shien (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems*, vol. 107, issue 3, p. 438–458.

CHOO, Chun Wei (2002). *Information management for intelligent organisation: the art of scanning the environment*. Medford: Information Today, Inc. 325 p.

CRESWELL, John W.; CLARK, Vicki L. Plano (2006). *Designing and Conducting Mixed Methods Research.* Sage Publications, Inc. 296 p.

DAVENPORT, Thomas; PRUSAK, Laurence (1997). *Information Ecology: Mastering the Information and Knowledge Environment.* New York: Oxford University Press. 272 p.

DEMING, William, Edwards (2000). *Out of the Crisis*. Cambridge: MIT Press. 523 p.

DLAMINI, M. T.; ELOFF, J. H. P.; ELOFF, M. M. (2009). Information security: The moving target. *Computers & Security*, vol. 28, issues 3–4, p. 189–198.

ENGLISH, P. Larry (2004). *Information Quality Management Matyrity: Toward the Intelligent Learning Organization* [interaktyvus]. [Žiūrėta 2012 m. liepos 5 d.]. Prieiga per internetą: <http://www.tdan.com/view-special-features/5409>.

GORDON, Lawrence; LOEB, Martin (2006). Economic aspects of information security: An emerging field of research. *Information Systems Frontiers*, vol. 8 (5), p. 335–337.

JAPERTAS, Saulius; ČINČIKAS, Gediminas; ŠESTAVISKAS, Ramūnas (2012). Company's Information and Telecommunication Networks Security Risk Assesment Algorithm. *Electronics and Electrical Engineering*, vol. 5(121), p. 33–36.

JASTIUGINAS, Saulius (2011). Informacijos saugumo valdymas Lietuvos viešajame sektoriuje. *Informacijos mokslai*, t. 57, p. 7–25.

JASTIUGINAS, Saulius (2012). Integralus informacijos saugumo valdymo modelis. *Informacijos mokslai*, t. 61, p. 7–30.

KAZANAVIČIUS, Egidijus; PAŠKEVIČIUS, Rokas; VENČKAUSKAS, Algimantas; KAZANAVIČIUS, Vygintas (2012). Securing web application by embedded firewall. *Electronics and Electrical Engineering*, vol. 3(119), p. 65–68.

McCUMBER, John (2005). *Assessing and Managing Security Risk in IT Systems: A Structured Methodology.* Auerbach Publications. 261 p.

ORNA, Elizabeth (2004). *Information Strategy in Practice*. Gower Pub Co. 164 p.

PARKER, B. Donn (1981). *Computer Security Management*. Reston, VA: Reston Publishing Company Inc.

SCHLÖGL, Chirstian (2005). Information and knowledge management: dimensions and approaches. *Information Research*, 10(4) [interaktyvus]. [žiūrėta 2012 m. rugsėjo 2 d.]. Prieiga per internetą: <http://InformationR.net/ir/10-4/paper235.html>.

ŠTITILIS, Darius; PAŠKAUSKAS, Žydrūnas (2007). Valstybės elektroninės informacijos saugos strategija – vienas iš pagrindinių elektroninės informacijos saugos reguliavimo instrumentų: lyginamoji analizė. *Jurisprudencija*, nr. 2(92), p. 37–45.

TIDIKIS, Rimantas (2003). *Socialinių mokslų tyrimų metodologija*. Vilnius. 427 p.

TRCEK, Denis (2006). *Managing Information Systems Security and Privacy*. Berlin: Springer Verlag, 2006.

von SOLMS, Basie (2010). *The 5 Waves of Information Security – From Kristian Beckman to the Present*. Invited Key note presentation at IFIP/Sec Conference, Brisbane, Australia, 2010. To be published in the Conference Proceedings.

WEISE, Joel (2009). Why Security Standards? *ISSA Journal*, August, p. 29–32.

INTEGRAL INFORMATION SECURITY MANAGEMENT MODEL FOR LITHUANIAN STATE INSTITUTIONS

Saulius Jastiuginas

S u m m a r y

The information security management research analysis shows that for a long time the technological solutions of research problems have dominated, but lately more relevant have become the human, economic and other issues, and there is a need for a more managerial approach. It is obvious that the current practice of information security management tools is no longer adequate for information security management. As a new instrument to address this problem, a theoretical integral information security governance model

could be used. It combines the information security management and information management tools.

The article aims to discuss empirical study as a theoretical integral information security management model that could be applied in practice. The practical applicability of the model was checked in in the Lithuanian state institutions. The paper discusses the study which has the following objectives: development of information security management in the Lithuanian state institutions evaluation approach, analysis of a case – the content analysis method to examine the legislative databases published in normative documents concerning information security management and proving the results through qualitative research (expert interview).

The paper presents the research results which confirm the validity of the integral theoretical information security management model and allows to assess information security management in the Lithuanian state institutions, to identify the shortcomings, to make suggestions for practical problem-solving and create conditions for the further research.

Priedas

INFORMACIJOS SAUGUMĄ REGLAMENTUOJANTYS LIETUVOS TEISĖS AKTAI

Šiame straipsnio priede pateikiami svarbiausi įstatymai ir įstatymų įgyvendinamieji aktai, reglamentuojantys informacijos saugumą. Šie dokumentai naudoti kaip šaltinis atvejo analizei nagrinėjant informacijos saugumo valdymą Lietuvos valstybės institucijose.

1996 m. birželio 11 d. buvo priimtas **Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas**, 2003 m. ir 2008 m. išdėstytas nauja redakcija. Šis įstatymas aktualus tuo, kad reglamentuoja fizinių asmenų, kaip duomenų subjektų, teises, šių teisių apsaugos tvarką, juridinių ir fizinių asmenų teises, pareigas ir atsakomybę tvarkant asmens duomenis. Pažymėtina, kad asmens duomenis galima rinkti tik apibrėžtais ir teisėtais tikslais, tokios apimties, kuri būtina asmens duomenims tvarkyti. Įstatymas taip pat reglamentuoja ir kitus informacijos saugumo aspektus: asmens duomenų saugojimą ir teikimą, duomenų saugumui būtinas priemones. Pagal šį įstatymą išankstinę duomenų patikrą atlieka Valstybinė duomenų apsaugos inspekcija, kuriai ir pavesta prižiūrėti ir kontroliuoti šio įstatymo vykdymą.

1996 m. rugpjūčio 13 d. buvo priimtas **Lietuvos Respublikos valstybės registrų įstatymas** (2004 m. nauja redakcija). Šis įstatymas nustato registrų steigimo, tvarkymo, naudojimo, pertvarkymo ir likvidavimo tvarką; reglamentuoja valstybės registrų tvarkymo įstaigų, joms vadovaujančių ir jų priežiūrą atliekančių institucijų, valstybės registrams duomenis teikiančių bei valstybės registrų duomenis naudojančių juridinių ir fizinių asmenų pareigas ir teises, juridinių ir fizinių asmenų, kurių duomenys yra registro objektas, pareigas ir teises, šių teisių apsaugą. Aktualiausia įstatymo dalis – duomenų, tvarkomų registre, saugumo reglamentavimas. Įstatyme nustatoma pareiga užtikrinti duomenų saugą, vadovaujantis Lietuvos Respublikos Vyriausybės patvirtintais reikalavimais.

1997 m. rugsėjo 4 d. buvo priimtas Lietuvos Respublikos Vyriausybės nutarimas Nr. 952 „Dėl duomenų apsaugos valstybės ir vietos savivaldos informacinėse sistemose“, 2002 m., vėliau 2007 m. įsigaliojo naujos šio nutarimo redakcijos. Nutarimu patvirtinami **Bendrieji duomenų saugos reikalavimai**. Šie reikalavimai taikomi

registrų ir informacinių sistemų valdytojams.

2001 m. gruodžio 22 d. Lietuvos Respublikos Vyriausybės nutarimu Nr. 1625 buvo patvirtintas pirmasis informacijos saugumo valdymą Lietuvos valstybės institucijose strategiškai apibrėžiantis dokumentas – **Informacijos technologijų saugos valstybinė strategija**.

Vadovaujantis Informacijos technologijų saugos valstybinė strategija:

1. 2002 m. gruodžio 31 d. nutarimu Nr. 2105 Lietuvos Respublikos Vyriausybė patvirtino naują Bendrųjų duomenų saugos reikalavimų redakciją. Šių reikalavimų tikslas – sudaryti sąlygas saugiai tvarkyti duomenis valstybės registruose ir kitose valstybės informacinėse sistemose.

2. 2003 m. sausio 27 d. įsakymu Nr. 1V-33 Lietuvos Respublikos vidaus reikalų ministras patvirtino **Informacijos klasifikavimo pagal duomenų grupes rekomendacijas**. Rekomendacijose duomenų svarbumas buvo apibrėžtas informacinės sistemos kategorija, kuri nustatoma pagal informacinės sistemos duomenų grupes ir tų grupių savybių įtaką informacinės sistemos darbui.

3. 2003 m. liepos 16 d. įsakymu Nr. 1V-272 Lietuvos Respublikos vidaus reikalų ministras patvirtino **Tipinius duomenų saugos nuostatus**. Juose nurodoma, kad valstybės registro ar kitos valstybės institucijos informacinės sistemos valdytojas, kuris vadovaujasi šiais nuostatais, rengia ir suderinęs su Vidaus reikalų ministerija tvirtina savo informacinės sistemos duomenų saugos nuostatus, kurie kartu su rengtinomis detaliomis instrukcijomis, procedūrų aprašymais ir saugaus darbo su duomenimis tvarkos taisyklėmis apibrėžia informacinės sistemos saugumo politiką.

4. 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 Lietuvos Respublikos vidaus reikalų ministras patvirtino **Informacinių technologijų saugos atitikties vertinimo metodiką**. Ši metodika parengta vadovaujantis Bendraisiais duomenų saugos reikalavimais, ja siekiama sudaryti sąlygas įvertinti informacinių technologijų saugos valstybės registruose arba kitose informacinėse sistemose sutikimą su šiais reikalavimais.

5. 2004 m. gegužės 14 d. įsakymu Nr. V-167 Lietuvos Respublikos vidaus reikalų ministras patvirtino **Saugaus valstybinio duomenų perdavimo tinklo (toliau – SVDPT) nuostatus ir paslaugų teikimo taisykles**. SVDPT funkcijas pavesta vykdyti valstybės įmonei „Infostruktūra“. SVDPT paskirtis – sudaryti sąlygas saugiai keistis duomenimis tiek Lietuvos Respublikos valstybės institucijoms tarpusavyje, tiek su Europos Sąjungos institucijomis.

6. 2004 m. gegužės 21 d. įsakymu Nr. 1V-176 Lietuvos Respublikos vidaus reikalų ministras patvirtino **Interneto tarnybinių stočių apsaugos rekomendacijas**. Jomis siekiama užtikrinti interneto tarnybinių stočių saugą, apibrėžiant visumą bendro pobūdžio priemonių tarnybinėms stotims valstybės institucijose ir įstaigose apsaugoti nuo išorinių ir vidinių grėsmių.

7. 2002 m. liepos 1 d. įsigaliojo **Lietuvos standartas „Informacijos technologija. Praktiniai informacijos saugumo valdymo aspektai“**, tapatus tarptautiniam standartui ISO/IEC 17799:2000, kurį Lietuvos standartizacijos departamentas patvirtinimo būdu perėmė iš Tarptautinės standartizacijos organizacijos ir Tarptautinės elektrotechnikos komisijos.

8. 2004 m. balandžio 19 d. nutarimu Nr. 451 Lietuvos Respublikos Vyriausybė patvirtino **Valstybės informacinių siste-**

mų steigimo ir įteisinimo taisykles. Taisyklėse pažymėtina, kad informacinės sistemos steigėjas Vidaus reikalų ministerijai turi pateikti steigiamos sistemos nuostatus ir šios sistemos duomenų saugos nuostatus, kurie turi būti parengti pagal pirmiau nurodytus Tipinius duomenų saugos nuostatus.

2006 m. birželio 19 d. Lietuvos Respublikos Vyriausybė priėmė nutarimą, kuriuo patvirtino **Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinę strategiją iki 2008 metų** bei Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinės strategijos iki 2008 metų įgyvendinimo priemonių planą. Įgyvendinant šią strategiją buvo priimti šie sprendimai ir teisės aktai:

1. 2006 m. gruodžio 13 d. nutarimu Nr. 1266 Lietuvos Respublikos Vyriausybė sudarė **Elektroninės informacijos saugos koordinavimo komisiją**.

2. 2007 m. balandžio 25 d. nutarimu Nr. 410 Lietuvos Respublikos Vyriausybė nauja redakcija patvirtino **Bendruosius duomenų saugos reikalavimus**.

3. 2007 m. gegužės 8 d. įsakymu Nr. 1V-172 Lietuvos Respublikos vidaus reikalų ministras patvirtino **Saugos dokumentų turinio gaires**, kurios pakeitė Tipinius duomenų saugos nuostatus.

4. 2007 m. birželio 29 d. įsakymu Nr. 1V-241 Lietuvos Respublikos vidaus reikalų ministras patvirtino **Saugaus elektroninės informacijos teikimo sutarties pavyzdinę formą**.

5. 2007 m. liepos 11 d. įsakymu Nr. 1V-247 Lietuvos Respublikos vidaus reikalų ministras nauja redakcija patvirtino:

a. **Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gaires**;
b. **Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos saugos reikalavimus**.

6. 2008 m. spalio 27 d. įsakymu Nr. 1V-384 Lietuvos Respublikos vidaus reikalų ministras pripažino netekusiais galios **Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos saugos reikalavimus** ir patvirtino **Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techninius saugos reikalavimus**.

2011 m. birželio 29 d. Lietuvos Respublikos Vyriausybė patvirtino naują strateginį dokumentą – **Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programą**. Šio dokumento tikslas – apimti ne tik viešąjį, bet ir kitus sektorius.

2012 m. sausio 1 d. įsigaliojo **Valstybės informacinių išteklių valdymo įstatymas**. Šio įstatymo tikslas – užtikrinti tinkamą valstybės informacinių išteklių kūrimą, tvarkymą, valdymą, naudojimą, priežiūrą, sąveiką, planavimą, finansavimą ir saugą.