VILNIAUS UNIVERSITETAS

SAULIUS JASTIUGINAS

INFORMACIJOS SAUGUMO VALDYMAS: LIETUVOS RESPUBLIKOS VALSTYBĖS INSTITUCIJŲ ATVEJIS

Daktaro disertacija

Humanitariniai mokslai, informacija ir komunikacija (06 H)

Vilnius, 2012

Disertacija rengta 2008–2012 metais Vilniaus Universiteto Komunikacijos fakultete.

Mokslinė vadovė:

Prof. dr. Zenona Atkočiūnienė (Vilniaus universitetas, humanitariniai mokslai, komunikacija ir informacija – 06 H).

Mokslinis konsultantas:

Doc. dr. Povilas Abarius (Vilniaus universitetas, humanitariniai mokslai, komunikacija ir informacija – 06 H).

TURINYS

ĮVADAS

Temos aktualumas

Informacijos saugumo svarba ir aktualumas sietini su pirmaisiais poreikiais tvarkyti informaciją. Vos atsiradus raštui, buvo ieškoma laiko ir gamtos reiškinių poveikiui atsparių priemonių informacijai fiksuoti ir išsaugoti. Iškilus poreikiui informaciją perduoti, radosi ir poreikis užtikrinti, kad ji pasiektų tik tuos, kam ji skirta. Tai sudarė sąlygas formuotis kriptografinių saugumo priemonių užuomazgoms. Pirmieji metraštininkai, archyvų bei bibliotekų darbuotojai taip pat gali būti priskirti informacijos saugumo vystytojams, pavyzdžiui, jų naudoti vaško antspaudai buvo taikomi siekiant užkirsti kelią neteisėtai prieigai prie informacijos ir ją pastebėti; kodai – apsaugoti informaciją nuo atskleidimo; kopijų darymas – išvengti informacijos praradimo (Denning, 1999; Lomas, 2010; Rusell ir Gangemi, 1991).

Informacijos saugumo turinys reikšmingai keitėsi pradėjus vystytis kompiuteriams ir kitoms informacinėms technologijoms. Pirmieji kompiuteriai, nors ir buvo naudojami tiek nacionalinio saugumo, tiek sudėtingų komercinių uždavinių sprendimams, nebuvo laikyti nei saugumo problema, nei jos sprendimu. Šie kompiuteriai dažniausiai buvo naudoti vieno vartotojo konkrečių uždavinių sprendimams, todėl vartotojui baigus darbą realiai buvo rūpinamasi tik informacijos laikmenų (magnetinių juostų, perfokortų) bei patalpų, kuriose buvo kompiuterinė sistema, fiziniu saugumu (užrakinimu). Informacijos saugumo problemos pradėjo ryškėti po 1960 metų pradėjus keistis kompiuterių naudojimo pobūdžiui, atsiradus personaliniams kompiuteriams ir technologijoms, leidusioms naudoti tą patį kompiuterį keliems vartotojams įvairiems skaičiavimams atlikti vienu metu, o ypač pradėjus vystytis kompiuterių tinklams (Brinkley ir Schell, 1995).

Šiuolaikinėje visuomenėje informacijos saugumo problemų aktualumas tampa kritinis. XX a. antroje pusėje kylant poreikiui valdyti informaciją ir žinias pasitelkiant modernias technologijas ir vadybos metodus, vis daugiau

informacijos ir kasdienės veiklos procesų persikėlė į globalią elektroninę erdvę. Vykstantys dinamiški pokyčiai pavertė visuomenę labai priklausomą nuo patikimo informaciją apdorojančių technologijų veikimo, bet kokie šių technologijų veiklos sutrikimai turi neigiamos įtakos tiek pavienių jos individų, tiek ir organizacijų ar net visos visuomenės socialiniam ir ekonominiam gyvenimui. Aktualiomis informacijos saugumo problemomis tapo nepageidaujami laiškai, virusai, įsilaužimai į informacines sistemas, interneto svetainių sutrikimai, tapatybės pasisavinimas, asmens duomenų ar verslo informacijos vagystės, slaptos informacijos nutekėjimas (pvz., Wikileaks) ar Tūkstantmečio klaidos (Y2K) sukeltas ažiotažas visame pasaulyje (Amaral, 2007; Atkočiūnienė, 2009a; Kuttschreuter, Gutteling, 2004).

Aktualių informacijos saugumo problemų gausa lėmė poreikį informacijos saugumui valdyti. Kylančioms problemoms spręsti buvo parengta įvairių dokumentų – gerųjų praktikų pavyzdžiai, vertinimo metodikos, rekomendacijos pavienėms verslo šakoms, sukurtas ne vienas tarptautinį pripažinimą pelnęs informacijos saugumo valdymo standartas. Šių dokumentų pagrindu organizacijoms suteikiama metodinė pagalba kompleksiškai ir suderintai taikyti informacijos saugumo valdymo metodus bei technologijas, laikytis geriausių praktikų, atitikti teisinius reikalavimus ir kitų privalumų (Amaral, 2007; Gorge, 2009; Weise, 2009). Kaip rodo praktika, pavieniai individai ar organizacijos ne visada nori ir gali spręsti kylančias saugumo problemas, čia išryškėja valstybių valdžios institucijų įsikišimo būtinybė. Valstybės, supratusios informacijos saugumo problemų kritiškumą ir valdymo svarbą (pvz., JAV, Didžioji Britanija, Japonija, Australija ir kt.), nustatė privalomus informacijos saugumo reikalavimus organizacijoms, veiklos sritims (sektoriams), valdančioms jautrią informaciją (asmens ar sveikatos duomenis, finansinę ar karinę informaciją ir kitą). Šie reikalavimai dažnai remiasi susiformavusiomis gerosiomis praktikomis ir (ar) tarptautiniais informacijos saugumo valdymo standartais.

Nepaisant bandymų spręsti informacijos saugumo keliamus iššūkius, pastarųjų metų tendencijos rodo, kad informacijos saugumas tampa globalaus

masto problema, kurios aktualumą iliustruoja nuolat augantys informacijos saugumo incidentų atvejai ir mastai[1]. Šie incidentai kelia grėsmę ne tik pavienėms organizacijoms ar valstybėms, bet ir globaliai kibernetinei erdvei. Pasaulinės interneto infrastruktūros, kuriai priskiriami didžiausi elektroninių ryšių paslaugų tiekėjai, interneto srautų paskirstymo įranga, vardų sričių saugyklos ir kita milijonus vartotojų bei milijardus užklausų visame pasaulyje aptarnaujanti įranga, sutrikimai ar tikslingos atakos gali smarkiai sulėtinti tarptautinių duomenų srautą, atkirsti pavienius tinklus ar jų grupes bei kitus išteklius nuo likusių vartotojų (Ryan, 2007). Problemos realumą ir galimą žalą parodė įvykiai Estijoje perkeliant „bronzinio kario skulptūrą“. Pasaulinės ryšių infrastruktūros priemonėmis organizuoto puolimo prieš šią šalį metu buvo atkirstos visos valstybės galimybės susisiekti su pasauliu, gauti ar pranešti informaciją apie šalyje vykstančius procesus, paralyžuotas valstybės institucijų ir verslo organizacijų darbas bei galimybė tvarkyti verslo ar kasdienio gyvenimo poreikius elektroninėje erdvėje. Šis įvykis sukėlė plačią tarptautinę diskusiją, į kurią buvo įtrauktos ir NATO bei Europos Sąjungos atitinkamos struktūros, dėl esamų tokio masto pažeidžiamumų ir kolektyvinių veiksmų tokiais atvejais būtinybės (Janeliūnas, 2007; Lorents, Rain, Rikk, 2009).

Aplinkos kaita ir joje vykstantys procesai rodo, kad informacijos saugumo problemų specifiškumas gali būti išskiriamas individo ar organizacijos, valstybės bei tarptautiniame lygmenyse. Įvertinus informacijos saugumo incidentų mastą ir galimą neigiamą poveikį bet kuriame iš šių lygmenų, teigtina, kad sugebėjimas valdyti informacijos saugumą turi tapti

[1] Jungtinėse Amerikos Valstijose per penkerius pastaruosius metus kompiuterinių incidentų skaičius išaugo daugiau nei 650 procentų (GAO ataskaita, 2011).

Didžiojoje Britanijoje 93 % didžiųjų bendrovių praneša apie rimtus saugumo incidentus, patirtus 2011 metais (palyginti su 2008 metais – 72 %), ir išaugusius vidutinius didžiausio incidento padarytus nuostolius, kurie apytiksliai nuo 90–170 tūkst. svarų sterlingų (2008 m.) išaugo iki 110–250 tūkst. svarų sterlingų (2011 m.) (Infosecurity Europe, 2010, 2012).

Lietuvoje su incidentais susiduria 85 proc. internetu besinaudojančių įmonių, o 27,2 proc. gyventojų ir 23 proc. įmonių nurodo, kad dėl incidentų patyrė nuostolių (Tinklų ir informacijos saugumo..., 2009).

strateginiu tiek organizacijų, tiek valstybių, tiek ir valstybes jungiančių tarptautinių aljansų ar kitų institutų tikslu. Kiekviename lygmenyje galima ieškoti konkrečių informacijos saugumo valdymo įrankių, tačiau didžiausia atsakomybė šiame kontekste turi tekti valstybėms, kurios, pasiremdamos suteiktomis galiomis, gali ir privalo nustatyti priemones, užtikrinančias informacijos saugumo valdymą jų viduje (t. y. individų ir organizacijų lygmenyje), bei turėti įtakos kitoms valstybėms ar jų dariniams imtis informacijos saugumo priemonių ir taip prisidėti prie tarptautinio lygmens problemų sprendimo (CIO, CSO ir PwC tyrimas, 2010, 2012; Ernst & Young's 12th Annual Global Information Security Survey; NATO, 2010).

Analizuojant aptarto globalaus informacijos saugumo valdymo problemų konteksto atspindį Lietuvoje, galima teigti, kad Lietuvai taip pat aktualios globalios informacijos saugumo problemos: esame susidūrę su internetinės bankininkystės sistemų sutrikimais ir atakomis, registrų ir valstybės informacinių sistemų duomenų nepasiekiamumu, asmens duomenų nutekėjimu iš verslo ir valstybinių organizacijų, plataus atgarsio susilaukė įsilaužimai į ryšių paslaugų tiekėjų serverius, kada nukentėjo tiek privačių bendrovių, tiek ir valstybės institucijų interneto svetainės, buvo sutrikdytas jų darbas ir pan. (Gamulis, Kiškina, 2009; Janeliūnas, 2007; RRT, 2010). Sprendžiant šias problemas Lietuvoje, kaip ir kitose šalyse, priimta įvairių strateginių dokumentų ir kitų teisės aktų, reglamentuojančių informacijos saugumo valdymą. Šių informacijos saugumo dokumentų turinys parengtas ir nuolat tobulinamas informacijos saugumo specialistų praktikų, remiamasi tarptautinėmis gerosiomis praktikomis ir metodikomis.

Aptarus informacijos saugumo problematikos raidą bei priemones, kurių imamasi valdant informacijos saugumo problemas įvairiuose lygmenyse, galima konstatuoti, kad nors informacijos saugumas tampa vienu svarbiausiu veiklos prioritetu tiek organizacijoms, tiek ir valstybėms, tačiau informacijos saugumo incidentų skaičius, kartu su dėl jų patiriamų nuostolių mastais, nevaldomai auga visame pasaulyje. Šios tendencijos leidžia daryti išvadas, kad: 1) informacijos saugumo incidentai gali būti įvardyti kaip pagrindinis

indikatorius, suponuojantis sisteminių informacijos saugumo problemų egzistavimą; 2) sprendžiant informacijos saugumo problemas, didžiausia atsakomybė turi tekti valstybėms; 3) informacijos saugumo užtikrinimas nėra tinkamai valdomas ir išlieka aktualia praktine problema.

Taigi esama situacija verčia ieškoti giluminių informacijos saugumo valdymo problemų priežasčių bei galimų jų sprendimų būdų, taikytinų Lietuvos atvejui.

Temos ištirtumas

Informacijos saugumo apibrėžties kaitai įtaką darė daugybė mokslinių tyrimų. Tyrinėjant informacijos saugumo problematiką, analizuota informacijos saugumo suvoktis (Parker, 1981; Trcek, 2006; McCumber, 2005; Zafar ir Clark, 2009; Mikalauskienė ir Brazaitis, 2010 ir kiti), įvairūs techniniai (Anderson, 1994; Anderson ir Moore, 2009; D'Archy ir Hovav, 2009; Mikučionis, Toldinas ir Venčkauskas, 2007 ir kiti), ekonominiai (Anderson, 2001; Caelli, 2002; Gordon ir Loeb, 2006; Johnson, 2009 ir kiti), vadybiniai (Abbas et al., 2011; Chang ir Lin, 2007; Dlamini, Eloff ir Eloff, 2009; Eloff ir Eloff, 2003; Hong et al., 2003; Knapp et al., 2006; Parakkattu ir Kunnathur, 2010 ir kiti), komunikaciniai (Janeliūnas, 2007 ir kiti), saugos priemonių taikymo (Kazanavičius et al., 2012; Japertas, Činčikas ir Šestaviskas, 2012; Paulauskas, 2009 ir kiti), standartų taikymo (Amaral, 2007; Gorge, 2009; Smith et al., 2010; Weise, 2009 ir kiti), psichologiniai (Nohlberg, 2008; Whitten ir Tygar, 1999; Anderson ir Moore, 2009; Asch, 1952 ir kiti), žmogiškojo faktoriaus (Ashenden, 2008; Timko, 2008 ir kiti), socialinės inžinerijos (Bakhshi, Papadaki ir Furnell, 2009; Workman, 2008; Kelly 2007; Mitnick ir Simon 2002 ir kiti), teisinio reglamentavimo ir reguliavimo (Čėsna ir Štitilis, 2000; McFadzean, Ezingeard ir Birchall, 2007; Paškauskas, 2007; Smith et al., 2010; Štitilis ir Paškauskas, 2007 ir kiti), kompetencijos ir mokymų (Venčkauskas, Krivickienė ir Toldinas, 2009; Choi, Kim ir Goo, 2008; Chang ir Ho, 2006; Tsohou et al., 2008; White, 2009 ir kiti) bei kiti informacijos saugumo aspektai.

Analizuojant ir vertinant informacijos saugumo teorijos raidą ir praktinio taikymo patirtį daug prisidėjo M. Sipponen ir H. Oinas-Kukkonen (2007), J. D'Archy ir A. Hovav (2009), F. Bjorck ir L. Yngstrom (2001), H. Zafar ir J. Clark (2009), M. Dlamini, J. Eloff ir M. Eloff (2009), von Solms (2010), J. Choobineh, G. Dhillon ir M. Grimaila (2007) ir kiti. Informacijos saugumo mokslinių tyrimų tendencijoms analizuoti pasitelkti įvairūs metodai, pavyzdžiui, tikslines specialistų apklausas pasitelkė R. Werlinger, K. Hawkey ir K. Beznosov (2009), G. Burell ir G. Morgan socialines paradigmas – G. Dhillon ir J. Backhouse (2001), E. McFadzean, J. Ezingeard ir D. Birchall (2006) ir kiti.

Išanalizavus teorinius tyrimus ir praktinio taikymo patirtį, galima teigti, kad informacijos saugumo problematika gana plati, tačiau dauguma informacijos saugumo tyrimų koncentruota ties technologinėmis problemomis. Egzistuoja daug išsamiais moksliniais tyrimais pagrįstų, patikimų informacijos saugumo užtikrinimo priemonių, bet dažnai dėl savo technologinio sudėtingumo, ekonominių veiksnių, kompetencijos trūkumo ar kitų priežasčių šios priemonės nėra tinkamai taikomos, taigi stebimas didelis atotrūkis tarp mokslo ir praktikos, stokojama konceptualių informacijos saugumo valdymo tyrimų.

Nagrinėjant mokslinius tyrimus, aiškiai pastebimas net ir naudojamų informacijos saugumo sąvokų nuoseklumo trūkumas. Tyrimų objekto lygmenyje mokslo darbuose tiek anglų kalba, tiek lietuvių kalba dažnai sinonimiškai naudojamos informacijos saugumo (angl. *information security*), informacijos technologijų saugumo (angl. *information technology security*), informacinių sistemų saugumo (angl. *information systems security*) sąvokos. Saugumo proceso lygmenyje nėra nusistovėjusios aiškios takoskyros tarp angliškų sąvokų *management* ir *governance* bei jų vertimo į lietuvių kalbą, pavyzdžiui, tarptautinio informacijos saugumo valdymo standarto ISO pavadinimas „ISO/IEC 27001:2005 Information technology – Security techniques – Information security *management* systems – Requirements", oficialiai verčiamas „LST ISO/IEC 27001:2006 Informacijos technologija.

Saugumo metodai. Informacijos saugumo *valdymo* sistemos. Reikalavimai“, o analogiška sąvoka kokybės vadybos kontekste „ISO/IEC 19796-1:2005 Information technology – Learning, education and training – Quality *management,* assurance and metrics – Part 1: General approach“, verčiama kaip „LST EN ISO/IEC 19796-1:2009 Informacinės technologijos. Mokymasis, ugdymas ir rengimas. Kokybės *vadyba*, užtikrinimas ir metrologija. 1 dalis. Bendrasis požiūris“. Reikėtų pažymėti, kad Lietuvoje nėra griežtai nusistovėjęs ir net šiame kontekste anglų kalboje vartojamo termino *security* vertimas – *saugumas, sauga, apsauga* (pavyzdžiui, COBIT metodikos vertime naudojamos visos trys sąvokos). Šiuo metu terminas *apsauga* dažniausiai sutinkamas asmens duomenų teisinės apsaugos, privatumo kontekste (Asmens duomenų.., 2008), *sauga* – valstybės informacinių išteklių (registrų ir informacinių sistemų) kontekste (Valstybės informacinių.., 2011), *saugumas* vartojamas plačiausiai, kaip apimantis visus išvardytus aspektus. Vertinant aptartą kontekstą, *informacijos saugumo valdymo* sąvoka labiausiai tinka siekiant atskleisti įvairialypį informacijos saugumo valdymo kontekstą ir disertacijoje toliau bus naudojama kaip apimanti (bendrąja prasme) saugumo, saugos ir apsaugos bei vadybos ir valdymo aspektus.

Remiantis bendru mokslinių tyrimų kontekstu, galima daryti prielaidą, kad pagrindinis saugumo tikslas (objektas, kurį siekiama apsaugoti) yra informacija, tačiau, analizuojant informacijos, tvarkomos informacinių technologijų priemonėmis, saugumą, dažnai saugumo objektu virsta pačios informacinės technologijos ar informacinės sistemos. Šioje disertacijoje daroma esminė mokslinė prielaida, kad svarbiausias informacijos saugumo objektas yra informacija, todėl informacijos saugumas turėtų būti tiriamas kaip sudėtinė informacijos vadybos ir kitų gretimų koncepcijų (informacijos išteklių vadybos, informacijos sistemų vadybos, informacijos įrašų vadybos) dalis.

Žvelgiant į informacijos vadybos mokslų raidą, ypač informacijos vadybos ištakas, taip pat galima įžvelgti pradines, gan techniškas, informacijos vadybos užduotis sprendžiant duomenų apdorojimo problemas. Vėliau šios užduotys plėstos efektyvaus informacinių technologijų išnaudojimo linkme bei

tapo plačia vadybine koncepcija, apimančia informacijos valdymą visuose organizacijos veiklos procesuose ir gyvavimo srityse. Šiuolaikinės informacijos vadybos kontekste informacinių technologijų naudojimas vertinamas kaip konkrečių efektyviai organizacijos veiklai parengtų procesų paramos priemonė (įrankis), o informacijos vadybos uždaviniais tampa siekis organizacijai padėti efektyviai valdyti informaciją, optimizuoti visus veiklos procesus (siejant juos su organizacijos veiklos strategija) bei prisitaikyti prie aplinkos pokyčių (Choo, 2002, 2008; Wilson, 1997; Vodacek 1998; Schlögl, 2005).

Išanalizavus pagrindinių informacijos vadybos teoretikų darbus, galima išskirti T. Wilson (1997), E. Macevičiūtės ir T. Wilson (2002), D. Chaffey ir S. Wood (2005), D. Chaffey ir G. White (2011) mokslinius tyrimus, kuriuose šie autoriai mini, kad informacija turi būti saugi, pristatyta reikiamam subjektui, tačiau detaliau informacijos saugumo nenagrinėja. Nagrinėjant pagrindinius informacijos vadybos procesinį (Choo, 2002) ir ekologinį modelius (Davenport ir Prusak, 1997), galima konstatuoti, kad informacijos saugumo aspektas neišryškintas. Plečiant analizę į gretimas informacijos vadybos koncepcijas, galima aptikti, kad išryškinus informacijos valdymo technologinį aspektą ir apie 1970 m. susiformavus informacijos išteklių vadybos sampratai, šiek tiek plačiau informacijos saugumo problematika nagrinėta informacijos išteklių vadybos kontekste. D. Skyrme (1999), J. Hoven (2001), N. Willard (1993, 2003), Z. Atkočiūnienės ir L. Markevičiūtės (2005) sudaryti informacijos išteklių vadybos modeliai, kaip viena iš informacinės veiklos sričių, išskiria ir informacijos išteklių saugumo užtikrinimo aspektą.

Apibendrinus išanalizuotus mokslinius informacijos saugumo tyrimus, konstatuotina, kad požiūris į informacijos saugumą nuo pirmųjų kompiuterių pasirodymo iki šių dienų iš esmės evoliucionavo – siaurą informacijos saugumo, kaip technologinės problemos, supratimą plečia ekonominių, vadybinių, psichologinių, teisinių ir kitų susijusių aspektų įtakos informacijos saugumui tyrimų rezultatai, kyla platesnio vadybinio požiūrio poreikis, tampa akivaizdu, kad esamos informacijos saugumo valdymo priemonės nebėra

pakankamos informacijos saugumui valdyti. Ryškėja platesnės informacijos saugumo valdymo suvokties poreikis ir sisteminių informacijos saugumo valdymo tyrimų trūkumas. Aptartų mokslinių tyrimų kontekste, gretinant informacijos saugumo valdymo ir informacijos vadybos raidą, galima įžvelgti paralelių abiejų diskursų slinktyje nuo technologijų vadybos link, numanyti tyrimų objekto sąsajas, tačiau informacijos vadybos modelių, metodų bei valdymo įrankių tyrimuose neišryškinta informacijos saugumo dedamoji, o informacijos saugumo valdymas nesiejamas su informacijos vadyba.

Mokslinės literatūros analizė leido nustatyti mokslinių darbų, skirtų informacijos saugumo valdymo visumai apibrėžti ir sąsajumui su informacijos vadyba išryškinti, trūkumą.

Sprendžiama mokslinė problema

Temos aktualumas ir teorinis ištirtumas leidžia įžvelgti spręstiną mokslinę problemą.

Informacijos saugumo valdymo mokslinės problemos laukas nėra visiškai susiformavęs, stebėtina tyrimų plėtra, tačiau vyrauja diskretyvi pavienių aspektų (ypač technologinių) analizė. Valdant informacijos saugumą identifikuotinas technologinių aspektų ryškinimas. Stokojama moksliškai pagrįstų visybiškų informacijos saugumo valdymo konceptų, kurie praplėstų informacijos saugumo valdymo teorinių tyrimų lauką bei lemtų teorinių paradigmų taikymą sprendžiant ryškėjančias praktines informacijos saugumo valdymo problemas tiek Lietuvoje, tiek ir globaliu mastu. Tampa akivaizdu, kad moksliškai neįtvirtintas informacijos saugumo valdymas sukelia problemų, kurios išryškėja ir praktiniame lygmenyje.

Ieškant esamos informacijos saugumo valdymo problematikos sprendinių bei darant esminę mokslinę prielaidą, kad informacijos saugumo valdymo objektas yra informacija, tikėtina, jog informacijos saugumas turėtų būti sudėtinė informacijos vadybos dalis, todėl, valdant informacijos saugumą, galėtų būti tikslinga pasitelkti teorinius informacijos vadybos konceptus ir įrankius. Moksliškai pagrįstas informacijos vadybos įrankių pasitelkimas,

tikėtina, padėtų užtikrinti visapusišką ir efektyvų informacijos saugumo valdymą.

Pastebėta, kad nors mokslinėse įžvalgose informacija akcentuojama kaip kritinis resursas, tačiau teoretikų dėmesys šio resurso saugumui užtikrinti yra menkas. Iki šiol informacijos saugumo valdymo ir informacijos vadybos sąsajos nėra pakankamai išplėtotos ir pagrįstos, todėl nėra argumentuoto teorinio mokslinio pagrindo informacijos saugumo valdymui taikyti informacijos vadybos modelius, metodus bei valdymo įrankius ir tai tampa aktualia moksline problema.

Išanalizavus informacijos saugumo valdymo problemines sritis, galima teigti, kad egzistuojančios informacijos saugumo valdymo priemonės, kilusios iš technologinių mokslų, neužtikrina visapusiško, integruojančio vadybinius aspektus informacijos saugumo valdymo. **Disertacijoje keliamas pagrindinis probleminis klausimas – kaip integruoti informacijos saugumo valdymo priemones ir informacijos vadybos įrankius ir užtikrinti visapusiškai valdomą informacijos saugumą Lietuvos valstybės institucijose?**

Tyrimo objektas – informacijos saugumo valdymas.

Tyrimo tikslas – sukurti ir pagrįsti integralų informacijos saugumo valdymo modelį, taikytiną Lietuvos Respublikos valstybės institucijoms.

Tyrimo uždaviniai:

1. Išanalizuoti vyraujančius mokslinius požiūrius į informacijos saugumą ir suformuoti informacijos saugumo valdymo turinį.
2. Išryškinti informacijos saugumo vietą informacijos vadybos mokslų kontekste, išskirti informacijos vadybos įrankius, taikytinus informacijos saugumo valdymui.
3. Sudaryti integralų, teoriškai pagrįstą informacijos saugumo valdymo modelį.

4. Suformuoti informacijos saugumo valdymo vertinimo prieigą ir atlikti šaltinių, formuojančių informacijos saugumo valdymo reikalavimus Lietuvos valstybės institucijoms, turinio analizę.
5. Ištirti, kaip Lietuvos valstybės institucijos įgyvendina galiojančius informacijos saugumo valdymo reikalavimus.

Ginamieji teiginiai:

1. Informacijos saugumas yra sudėtinė informacijos vadybos dalis, todėl informacijos saugumo valdymui pasitelkiant informacijos vadybos įrankius gali būti užtikrintas efektyvus informacijos saugumo valdymas.
2. Informacijos saugumas Lietuvos valstybės institucijose nėra tinkamai valdomas dėl informacijos saugumo reikalavimų fragmentiškumo ir vyraujančio formalaus techninio požiūrio.
3. Integralus informacijos saugumo valdymo modelis, jungiantis informacijos saugumo valdymo priemones ir informacijos vadybos įrankius, leidžia spręsti esamas informacijos saugumo valdymo problemas, praplečia informacijos vadybos ribas ir gali būti sėkmingai naudojamas tiek tolesniuose teoriniuose tyrimuose, tiek praktinėje Lietuvos valstybės institucijų veikloje.

Tyrimo metodai

Suformuluotas mokslinio darbo tikslas ir iškelti uždaviniai leidžia apibrėžti svarbiausias tyrimų sritis, duomenų, reikalingų mokslinio darbo objektui nagrinėti bei iškeltiems uždaviniams spręsti, poreikį ir apimtis.

Teorinėse darbo dalyse, formuojant visybiško požiūrio į informacijos saugumą turinį, atlikta mokslinių tyrimų, nagrinėjančių informacijos saugumo problematiką, turinio analizė taikant lyginimo, apibendrinimo ir sintezės metodus, taip pat suformuluotos informacijos saugumo apibrėžtys. Nagrinėjant plačiausiai taikomas informacijos saugumo valdymo priemones ir jų turinį, pasitelkta lyginamoji analizė. Sisteminė informacijos vadybos mokslinės

literatūros analizė, lyginimo, abstrakcijos, analogijos ir apibendrinimo metodai leido išryškinti informacijos saugumo ir informacijos vadybos sąsajumą, išskirti informacijos vadybos įrankius, taikytinus informacijos saugumo valdymui, bei suformuoti integralų informacijos valdymo modelį.

Empirinėje darbo dalyje integralaus informacijos saugumo valdymo modelio praktiniam pritaikomumui nustatyti ir pagrįsti pasitelkta mišrių metodų prieiga derinant kiekybinių ir kokybinių tyrimų metodus – dokumentų turinio analizę, anketinę institucijų apklausą ir ekspertų interviu. Derinant šiuos metodus galima užtikrinti visapusiškai argumentuotus ir patikimus tyrimo rezultatus teorinio integralaus informacijos saugumo valdymo modelio praktinei realizacijai ir pagrindimui. Empirinio tyrimo duomenims analizuoti taikyta nuoseklių procedūrų tyrimo strategija. Kokybiniai ir kiekybiniai duomenys renkami nuosekliai vieni po kitų, renkamais duomenimis detalizuoti, praplėsti bei papildyti anksčiau surinktų duomenų pagrindu gauti rezultatai. Remiantis teoriniu integraliu informacijos saugumo valdymo modeliu, buvo suformuota informacijos saugumo vertinimo prieiga, išskirti informacijos saugumo valdymo įrankiai ir apibrėžti vertinimo kriterijai. Ši prieiga taikyta identifikuotų šaltinių, formuojančių informacijos saugumo valdymo reikalavimus Lietuvos valstybės institucijoms, turinio analizei. Analizės rezultatai panaudoti formuluojant klausimus ekspertams, o kartu su ekspertų interviu įžvalgomis (iškeltais probleminiais klausimais) – sudarant kiekybinio tyrimo (institucijų apklausos) anketas.

Informacijos saugumo dokumentų, reglamentuojančių informacijos saugumo valdymą Lietuvos valstybės institucijose, turinio analizė taikyta pagrįsti informacijos saugumo valdymo Lietuvos valstybės institucijose trūkumus. Analizės rezultatai parodė, kad informacijos saugumo Lietuvos valstybės institucijose valdymas tik su išlyga gali būti pavadintas modeliu, todėl įvardijant esamą būklę naudotina *diskretaus* (atskiro nuo visumos) *informacijos saugumo modelio* sąvoka, kurios turinį nusako informacijos saugumo valdymo reikalavimų taikymas ne visai organizacijos informacijai, o atskiroms organizacijos informacijos sistemoms.

Ekspertų interviu metodas taikytas kaip pavienių Lietuvos valstybės institucijų ir ekspertinio konteksto įvesties įrankis į atliktą teorinio integralaus informacijos saugumo valdymo modelio taikymo Lietuvos valstybės institucijoms dokumentų turinio analizės rezultatų vertinimą.

Atliekant Lietuvos valstybės institucijų apklausą buvo siekiama ištirti praktinį informacijos saugumo valdymo reikalavimų įgyvendinimą. Kiekybiniams duomenims, kaip Lietuvos valstybės institucijos įgyvendina informacijos saugumo reikalavimus, surinkti buvo suformuotas originalus informacijos saugumo valdymo įvertinimo valstybės institucijose klausimynas. Šiuo klausimynu surinkti duomenys padėjo detaliai įvertinti informacijos saugumo valdymo situaciją Lietuvos valstybės institucijose ir suformuluoti sudaryto teorinio integralaus informacijos saugumo valdymo modelio įgyvendinimo prielaidas.

Darbo naujumas ir mokslinė reikšmė

Darbo naujumą ir teorinį reikšmingumą lemia pasiekti informacijos vadybos mokslui svarbūs rezultatai. Darbas leido sumažinti neapibrėžtumą informacijos vadybos mokslų sistemoje, išplėtoti teorinę informacijos vadybos paradigmą informacijos vadybos mokslų sistemoje išryškinant informacijos saugumo valdymo dedamąją.

Disertacijoje, išanalizavus informacijos saugumo mokslinių tyrimų įžvalgų kismą, susisteminus informacijos saugumo sąvokas ir nustačius jų ryšius bei atlikus lyginamąją tarptautiniame lygmenyje vyraujančių informacijos saugumo valdymo priemonių analizę, suformuota ir pagrįsta informacijos saugumo valdymo turinio apibrėžtis.

Aptartas informacijos saugumo valdymo objekto diskursas ir išryškinta informacija, kaip informacijos saugumo valdymo objektas suformavo teorines prielaidas informacijos saugumo valdymui pasitelkti informacijos vadybos įrankius. Šių įrankių analizė leido išskirti informacijos vadybos įrankius, taikytinus informacijos saugumo valdymui.

Sujungiant disertacijos teorinėse dalyse atliktų mokslinių tyrimų rezultatus suformuotas teorinis integralus informacijos saugumo valdymo modelis, taikytinas tiek tolesniuose teoriniuose moksliniuose tyrimuose, tiek praktiniam taikymui. Integralaus informacijos saugumo valdymo modelio praktinis pritaikomumas patikrintas vertinant informacijos saugumo valdymą Lietuvos valstybės institucijose. Atlikto empirinio tyrimo rezultatai pagrindė teorinio modelio reikšmingumą efektyviam informacijos saugumo valdymui užtikrinti.

Disertacijos tyrimo ribos

Disertacijos tyrimas apsiriboja informacijos saugumo valdymo modelio Lietuvos valstybės institucijoms kūrimu. Tokias mokslinio darbo ribas lemia dvi pagrindinės priežastys.

1. Lietuvoje galiojantys informacijos saugumo valdymo reikalavimai plačiausiai taikomi išskirtinai valstybės institucijoms, todėl šiame sektoriuje yra didžiausia erdvė tyrimams, o įvertinant, kad Lietuvos Respublikos Vyriausybė yra deklaravusi siekį plėsti informacijos saugumo valdymo reikalavimų taikymą ir visiems kitiems sektoriams, išsamus esamos situacijos mokslinis įvertinimas būtų kaip tik laiku; pagrįstos rekomendacijos galėtų sukurti ir praktinę mokslinio darbo vertę.

2. Šis sektorius pasirinktas atsižvelgiant ir į viešosios teisės principus, nusakančius, kad viešajam sektoriui leidžiama tik tai, kas nurodyta, t. y.: 1) viešojo administravimo subjektams leidžiama tik tai, kas numatyta teisės aktuose; 2) viešojo administravimo subjektams privaloma atlikti tai, kas numatyta teisės aktuose, t. y. viešasis sektorius yra įpareigotas aiškių rėmų ir negali laisvai rinktis, kaip reaguoti į informacijos saugumo rizikas. Dėl šios priežasties Lietuvos valstybės institucijų informacijos saugumas tiesiogiai priklauso nuo galiojančių informacijos saugumo valdymo reikalavimų, o tai suponuoja, kad šie reikalavimai turi būti tinkamai pagrįsti.

Disertacijos struktūra

Disertacija sudaryta iš įvado, trijų dalių, išvadų, literatūros sąrašo ir priedų.

Pirmoje disertacijos dalyje išanalizuotos ir susistemintos informacijos saugumo apibrėžtys, atskleista informacijos saugumo sampratos genezė, išanalizuota Lietuvos ir užsienio tyrėjų informacijos saugumo tyrimų aprėptis ir problematika. Šios analizės pagrindu suformuotas informacijos saugumo valdymo turinys.

Šioje dalyje taip pat aprašytos informacijos saugumo valdymo priemonės – tarptautiniai informacijos saugumo valdymo standartai, metodikos ir modeliai, atlikta šių priemonių lyginamoji analizė.

Remiantis teoriniame tyrime suformuluotomis informacijos saugumo valdymo prielaidomis bei turiniu, atliktas žvalgomasis tyrimas: dokumentų turinio analizės metodu ištirti informacijos saugumo valdymo reikalavimai Lietuvos valstybės institucijoms ir įvertintas šių reikalavimų laikymasis konkrečioje Lietuvos valstybės institucijų grupėje – Lietuvos Respublikos ministerijose. Šio žvalgomojo tyrimo rezultatai leido pagrįsti darbo temos ir ginamųjų teiginių aktualumą, apibrėžti tolesnių tyrimų poreikį ir kryptis.

Antroje disertacijos dalyje, siekiant atskleisti saugumo valdymo ir informacijos vadybos mokslų sąsajumą, išanalizuoti ir įvertinti informacijos vadybos tyrėjų darbai, išskirti informacijos vadybos įrankiai, kuriuos būtų galima taikyti informacijos saugumui valdyti.

Apibendrinus atliktą teorinį tyrimą, sudarytas integralus informacijos saugumo valdymo modelis, jungiantis informacijos saugumo valdymo priemones ir informacijos vadybos įrankius.

Trečioje disertacijos dalyje atliktas teorinio integralaus informacijos saugumo valdymo modelio praktinio pritaikomumo galimybių empirinis tyrimas. Remiantis teoriniu modeliu, buvo suformuota informacijos saugumo valdymo prieiga ir atliktas informacijos saugumo valdymo Lietuvos valstybės institucijose tyrimas. Tyrimui taikyta mišrių metodų prieiga derinant dokumentų turinio analizės, institucijų anketinės apklausos ir ekspertų interviu

metodus. Empirinio tyrimo rezultatai leido identifikuoti trūkumus ir suformuluoti siūlymus, kaip, remiantis integraliu informacijos saugumo valdymo modeliu, efektyviai valdyti informacijos saugumą Lietuvos valstybės institucijose.

Disertacijos aprobavimas

Tyrimo prielaidos pristatytos šiose mokslinėse konferencijose:

2008 m. lapkričio mėn. 7–8 d. Lisabonoje mokslinėje konferencijoje *Skaitmeninio Saugumo Forumas (Digital Security Forum)* pristatytos informacijos saugumo valdymo Lietuvos valstybės institucijose aktualijos, moksliniame seminare aptarta informacijos saugumo ir informacijos vadybos sąsajumo problematika.

2010 m. gruodžio 17 d. Vilniaus universiteto Komunikacijos fakulteto mokslinėje praktinėje konferencijoje „Komunikacijos ir informacijos vadybos raiškos ir modeliai“ skaitytas pranešimas „Informacijos saugumo valdymas Lietuvos valstybės institucijose: problemos ir galimybės“.

2011 m. gruodžio 16 d. Vilniaus universiteto Komunikacijos fakulteto mokslinėje konferencijoje „Informacijos ir komunikacijos teorijos ir praktikos raiškos“ skaitytas pranešimas „Informacijos saugumas informacijos vadyboje: teorija ir praktika Lietuvos viešajame sektoriuje“.

Pagrindiniai disertacijos teiginiai aptarti:

S. Jastiuginas. Informacijos saugumo valdymas Lietuvos viešajame sektoriuje. Informacijos mokslai. 2011, t. 57, p. 7–24.

S. Jastiuginas. Integralus informacijos saugumo valdymo modelis. Informacijos mokslai. 2012, t. 61, p. 7–30.

S. Jastiuginas. Integralaus informacijos saugumo valdymo modelio taikymas Lietuvos valstybės institucijoms. Informacijos mokslai. 2012, t. 61, p. 31–58.

I DALIS. INFORMACIJOS SAUGUMO VALDYMAS

Informacijos saugumo valdymas, kaip objektyvi saugumo būsena, visų pirma turi turėti aiškiai apibrėžtą valdymo objektą. Tiek mokslinių tyrimų, tiek praktinio taikymo kontekste sutinkamas informacijos, informacinių sistemų, informacijos technologijų ir kitų saugumo objektų gan sinonimiškas naudojimas. Vertinant šias interpretacijas, vienareikšmis objekto išgryninimas padėtų tiksliau identifikuoti objekto saugumui aktualius veiksnius bei nustatyti kriterijus, kurie leistų įvertinti, ar objekto saugumas yra valdomas.

Siekiant apibrėžti informacijos saugumo valdymo sąvokos turinį, tikslinga apžvelgti informacijos saugumo problematikos lauką bei mokslinių tyrimų aprėptis, išanalizuoti tyrėjų ryškintas teorines informacijos saugumo paradigmas, ištirti naudojamų informacijos saugumo sampratų turinį ir informacijos saugumo suvokties kaitą bei susisteminti aktualius mokslinių tyrimų aspektus, išskiriant, kurie iš jų yra informacijos saugumo valdymo dedamosios dalys.

Informacijos saugumo valdymui užtikrinti nepakanka apibrėžti informacijos saugumo valdymo turinį, būtina numatyti ir priemones, kuriomis jis galėtų būti valdomas. Šiuo metu egzistuoja platus ratas informacijos saugumo valdymo priemonių – tarptautiniai informacijos saugumo valdymo standartai, metodikos bei modeliai. Lyginamoji šių priemonių turinio analizė leistų atskleisti jų tinkamumą informacijos saugumui valdyti.

Aptariama informacijos saugumo valdymo problematika aktuali ir Lietuvoje. Šiam teiginiui pagrįsti atliktas žvalgomasis tyrimas – esamos informacijos saugumo užtikrinimo situacijos Lietuvos valstybės institucijose analizė.

1.1. Informacijos saugumo apibrėžtys

Informacijos saugumo sampratai apibrėžti ir geriau suvokti nagrinėjamą reiškinį būtina susisteminti užsienio ir Lietuvos mokslininkų informacijos saugumo teorinių įžvalgų visumą, aptarti nagrinėjamų *informacijos saugumo* ir su ja glaudžiai susijusių sąvokų turinį bei šių sąvokų ryšius, įvertinti informacijos saugumo suvokties pokyčius ir tendencijas, atskleisti informacijos saugumo problematikos mokslinių tyrimų kryptis ir, gretinant teorinių tyrimų objektus ir požiūrius, išskirti aktualiausius informacijos saugumo aspektus.

1.1.1. Informacijos saugumo sąvokos

Darbo objektui nagrinėti išskirtinos šios pagrindinės sąvokos, formuojančios informacijos saugumo sampratą, – *saugumas*, *informacijos saugumas*, *informacijos saugumo valdymas*.

Remiantis B. Buzan (1997) saugumo studijomis, galima pažymėti, kad nors *saugumo* sąvoka yra daugiareikšmė ir sunkiai apibrėžiama, iš esmės *saugumas* gali būti suprantamas kaip būsena, kuri gali reikšti apsisaugojimą nuo pavojaus (objektyvus saugumas) ir saugumo jausmą (subjektyvus saugumas). Siekiant sumažinti neapibrėžtumą, aptariant *saugumo* sąvoką būtina įvardyti objektą, t. y. kas turi būti (tapti) saugiu, o vykdant saugumo objekto paiešką turi vykti ir saugumo sąlygų paieška.

Disertacijoje kaip pagrindinis *saugumo* objektas nagrinėjama informacija, tačiau nagrinėjant *informacijos saugumą* aptariamas ir su tuo glaudžiai susijęs platesnis kontekstas – informacinių sistemų, informacinių technologijų, organizacijų, nacionalinis ir tarptautinis saugumas. Moksliniame darbe remiamasi nuostata, kad *informacijos saugumo* sąlygos (pavojai, kurių reikia saugotis) nuolat kinta, todėl būtina apibrėžti veiksmingas priemones, kurios užtikrintų nuolatinį reagavimą į šių sąlygų kismą, t. y. užtikrinti *informacijos saugumo valdymą* kaip nuolatinę objektyvaus saugumo būseną.

Dauguma *informacijos saugumo* apibrėžčių jau daugiau kaip dvidešimt metų remiasi trimis informacijos saugumo tikslais (CIA triada). Pagal CIA

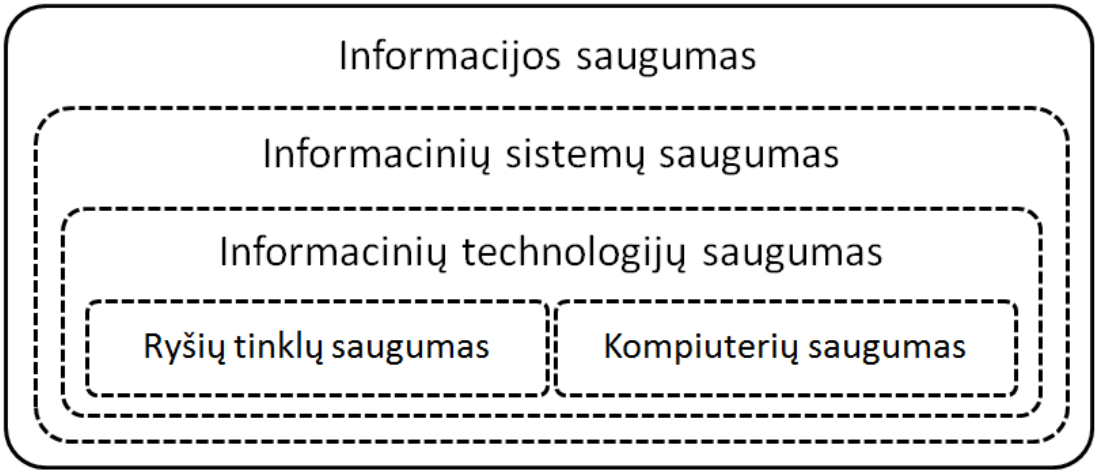
triadą įvardijama, kad *informacijos saugumo* tikslas – užtikrinti informacijos *konfidencialumą* (angl. *confidentiality*), *vientisumą* (angl. *integrity*) ir *prieinamumą* (angl. *availability*), kur *konfidencialumas* suprantamas kaip informacijos slaptumas, t. y. informacija turi būti prieinama tik tiems, kam ji skirta; *vientisumas* apima pradinės informacijos tikrumą, patikimumą bei autentiškumą, t. y. informacija ir jos šaltinis turi būti apsaugoti nuo bet kokio klaidingo ar nesankcionuoto pakeitimo, o visi pakeitimai yra žinomi; *prieinamumas* – užtikrinta galimybė pasinaudoti informacija, t. y. sankcionuoti vartotojai turi turėti galimybę pasiekti informaciją tada, kada jos jiems reikia. Kai kurie autoriai, pavyzdžiui, Donn Parker (1998), pristatydamas savo saugumo heksadą, bandė plėsti informacijos saugumo tikslus pridėdamas autentifikavimo, autorizavimo, atskaitomybės, neatsisakymo ir kitus aspektus, tačiau sistemiškai analizuojant informacijos saugumo mokslinius tyrimus, galima konstatuoti, kad šiuos naujai įvardijamus aspektus apima CIA triada. Pavyzdžiui, autentifikavimas (tapatybės patvirtinimas), autorizavimas (nustatytų teisių apdoroti informaciją suteikimas), atskaitomybė (vartotojo veiksmų stebėjimas) yra prieigos valdymo etapai ir juos apima informacijos *konfidencialumo* ir *vientisumo* tikslai, neatsisakymas (negalėjimas paneigti įvykusios transakcijos ar kito veiksmo) yra taip pat *vientisumo* sudėtinė dalis (Parker, 1981, 1998; McCumber, 2005; Zafar ir Clark, 2009; Trcek, 2006; ISO 27000 standartų grupė ir kiti).

Informacijos saugumo srityje naudojami įvairūs terminai: *informacijos, duomenų, kompiuterių, ryšių tinklų, informacijos technologijų, informacinių sistemų saugumas (apsauga);* ir nors šie terminai skiriasi savo objektu ir turiniu, literatūroje dažnai sutinkamas jų sinonimiškas vartojimas. Išanalizavus Markus Nohlberg, Basie von Solms, Denis Trcek, Audronės Mikalauskienės ir Zenono Brazaičio bei kitų tyrėjų darbus, labiausiai techniniams ir siauriausiems terminams galima priskirti terminus – *kompiuterių saugumas* ir *ryšių tinklų saugumas*, kurie apibrėžiami kaip priemonių, skirtų apsaugoti informaciją, tvarkomą kompiuteryje ar perduodamą ryšių tinklais, nuo atsitiktinių ar tyčinių grėsmių, visuma. Sąvokos *informacijos technologijų*

saugumas ir *informacinių sistemų saugumas* taip pat dažnai vartojamos sinonimiškai, tačiau reikėtų pastebėti, kad *informacinių technologijų saugumas* apima daugiau technologinius aspektus, o *informacinių sistemų saugumas* apima dar ir žmogiškąjį veiksnį (Nohlberg, 2008; von Solms, 2000; Trcek, 2006; Mikalauskienė, Brazaitis, 2010 ir kiti).

Išnagrinėjus mokslinėje literatūroje naudojamus terminus galima konstatuoti, kad *informacijos saugumo* sąvoka apima visus išvardytus aspektus ir veiksnius, todėl ši sąvoka labiausiai tinka siekiant atskleisti įvairialypį informacijos saugumo kontekstą ir bus toliau naudojama disertacijoje.

Aptartų informacijos saugumo sąvokų sąsajos ir jų hierarchinė schema pavaizduota 1 paveiksle. Šios sąvokos formuoja bendrą informacijos saugumo sampratą.



1 pav. Informacijos saugumo sąvokų hierarchinė schema (sudaryta autoriaus).

1.1.2. Informacijos saugumo sampratos genezė

Vertinant *informacijos saugumo* sampratos genezę, galima pastebėti, kad kinta tiek informacijos saugumo aktualumas, tiek ir pačios informacijos saugumo sampratos turinys. Informacijos saugumo aktualumui nuolat augant, požiūris į informacijos saugumą nuo pirmųjų kompiuterių pasirodymo iki šių

dienų iš esmės evoliucionavo – nuo siauro informacijos saugumo supratimo kaip tik technologinės problemos iki plačios informacijos saugumo valdymo poreikio suvokties (Denning, 1999; Dlamini, Eloff ir Eloff, 2009; Rusell ir Gangemi, 1991). Nagrinėjant mokslinių tyrimų rezultatus, galima identifikuoti ir šio kismo priežastis.

Informacijos saugumo aktualumo pokyčius nesunkiai galima identifikuoti viešojoje erdvėje – visuomenei vis labiau priklausant nuo informacijos konfidencialumo, prieinamumo bei vientisumo, bet kokie informacijos saugumo incidentai traukia tiek žiniasklaidos, tiek ir jos auditorijos dėmesį. Žvelgiant į mokslinius tyrimus taip pat stebimas aiškus susidomėjimo informacijos saugumu kismas. Bendrą mokslinių tyrimų informacijos saugumo tematika augimą per paskutinius trisdešimt metų vaizdžiai atskleidžia 2009 metais publikuota studija, kurios autoriai nagrinėjo informacijos saugumo tyrėjų straipsnius labiausiai vertinamuose žurnaluose, skirtuose informacinių sistemų problematikai (*MIS Quarterly, Information Systems Research, Journal of Management Information Systems, European Journal of Information Systems, Information & Management, Communications of the Association for Information Systems, Information Systems Journal, Journal of the Association for Information Systems ir Journal of Information Systems Security*). Šiuose žurnaluose buvo identifikuoti ir suklasifikuoti straipsniai informacijos saugumo tema pradedant nuo žurnalo pirmo numerio iki 2007 metų pabaigos. Temų klasifikacijai buvo naudotas IBM pasiūlytas informacijos saugumo modelis (IBM, 2006), integruojantis 9 informacijos saugumo temines sritis: valdymą, privatumą, grėsmių mažinimą, transakcijos ir duomenų integralumą, tapatybės ir prieigos valdymą, programų saugumą, fizinį saugumą, personalo saugumą ir ekonominius klausimus. Studijos rezultatai atskleidė, kaip keitėsi tiek pavienių informacijos saugumo teminių sričių, tiek ir bendras informacijos saugumo aktualumas, kuris ypač išaugo paskutiniais metais (Zafar ir Clark, 2009, 1 lentelė).

Vertinant informacijos saugumo tyrimų temų pokyčius galima pastebėti, kad, nors daugiau technologinė *transakcijų ir duomenų integralumo* tematika

išlaiko aktualumą, paskutinį dešimtmetį ryškėja vadybinių temų plėtotė – *valdymas*, *privatumas*, *grėsmių mažinimas*, *personalo saugumas* bei *ekonominiai klausimai* tampa vyraujančiomis temomis.

1 lentelė. Pagrindinės informacijos saugumo tyrimų temos (Zafar ir Clark, 2009).

Teminės sritys \ Metai	**1977–1979**	**1980–1989**	**1990–1999**	**2000–2007**	**Iš viso**
Valdymas		2	7	22	**31**
Privatumas	1	2	1	18	**22**
Grėsmių mažinimas			3	19	**22**
Transakcijos ir duomenų integralumas	2	7	3	24	**36**
Tapatybės ir prieigos valdymas			1	4	**5**
Programų saugumas		1	1	2	**4**
Fizinis saugumas		2	1		**3**
Personalo saugumas			3	5	**8**
Ekonominiai klausimai				6	**6**
Iš viso	**3**	**14**	**20**	**100**	**137**

Informacijos saugumo tyrimų temų kismas turėjo įtakos ir informacijos saugumo turinio suvokties pokyčiams. Šiuos pokyčius ir jų priežastis organizacijų lygmenyje detaliai analizavo Johanesburgo universiteto profesorius Basie von Soms, kuris savo mokslinėse publikacijose išskyrė tris *saugumo bangas*, o vėliau pristatė ir ketvirtąją bei penktąją (von Solms, 2000, 2006, 2010, 2 paveikslas).

Pirmoji banga, besitęsusi iki devintojo dešimtmečio, charakterizuojama kaip *techninė banga* (angl. *Technical Wave*) – informacijos saugumo užtikrinimas buvo suprantamas kaip technologijų problema, kuria rūpinosi tik techninis personalas.

Antroji banga pasižymėjo organizacijų vadovybės įtraukimu į saugumo užtikrinimo procesus, buvo pradėti formalizuoti saugumo tikslai ir uždaviniai, kuriuos tvirtindavo vadovybė, kartu įpareigodama atsakingus už saugumą pareigūnus pateikti ataskaitą apie situaciją ir pažangą užtikrinant saugumą

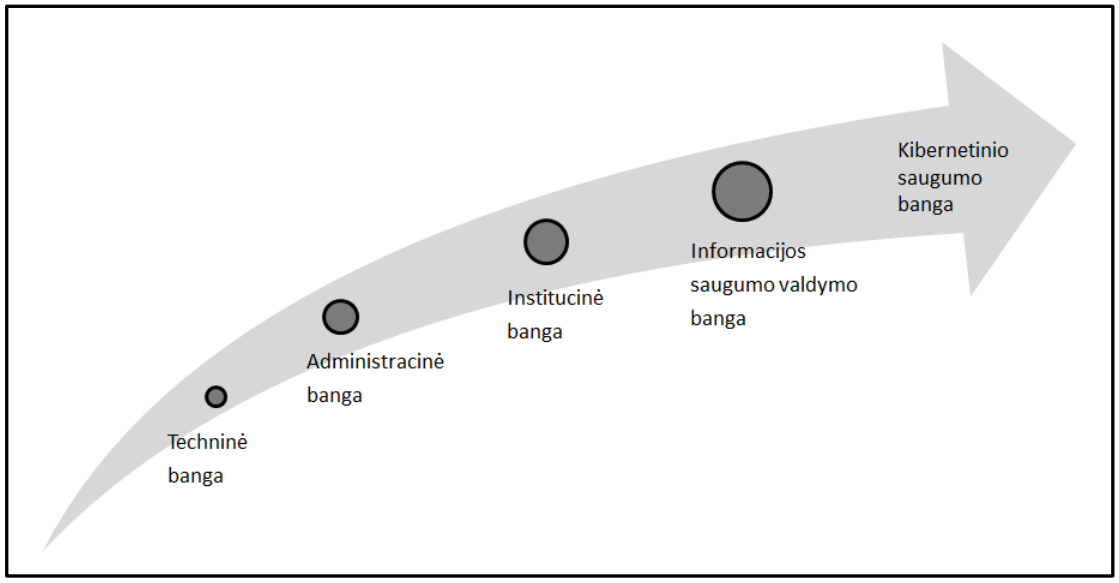
organizacijoje. Ši banga galėtų būti pavadinta *administracine banga* (angl. *Management Wave*), kuri tęsėsi maždaug iki dešimtojo dešimtmečio vidurio.

Trečiosios, institucinės bangos (angl. *Institutionalization Wave*), susiformavimą lėmė glaudesnis organizacijų vadovybės įsitraukimas sprendžiant saugumo problemas; tai leido iš esmės pagerinti saugumo situaciją ir nuolat įtraukti saugumo klausimus į kasdienę organizacijos veiklą. Organizacijos pradėjo lyginti savo saugumo lygį su kitomis, taikyti geruųjų praktikų pavyzdžius ir standartus, o pripažinus žmogiškojo faktoriaus įtaką saugumui, organizacijose pradėtas skatinti saugumo kultūros formavimas.

Ketvirtoji, informacijos saugumo valdymo (angl. *Information Security Governance*), banga pradėjo formuotis po 2000-ųjų metų. Didėjantis organizacijų poreikis vertinti ir tarpusavyje lyginti informacijos saugumo situaciją padėjo formuotis praktikai plačiau taikyti atsiradusius informacijos saugumo valdymo standartus (pvz., ISO 27000 standartų grupė), informacinių technologijų valdymo metodikas (pvz., Cobit, ITIL). Šie dokumentai nustato, kad organizacijos turi sugebėti valdyti rizikas, susijusias su tinkamu informacijos technologijų veikimu, visą jų gyvavimo ciklą, o organizacijos vadovybė yra tiesiogiai atsakinga už rizikų valdymo sistemos ir atitinkamų kontrolės priemonių įdiegimą bei nuolatinį saugos kultūros skatinimą organizacijoje.

Prie glaudaus valdymo funkcijų integravimo į informacijos saugumo valdymo sąvoką ypač prisidėjo informacijos saugumo valdymo reikalavimų įteisinimas pavienių šalių teisės aktais, kurie įtvirtino privalomą informacijos saugumo valdymo priemonių, besiremiančių saugos standartais ir metodikomis, taikymą bei nustatė asmeninę organizacijos vadovų atsakomybę. Šiame kontekste aktualūs Didžiosios Britanijos ir Švedijos sprendimai taikyti ISO 27000 informacijos saugumo valdymo standartus viešajame sektoriuje (Cyber Security Strategy of the United Kingdom (2009), Swedish Administrative Development Agency Regulation of Government Agencies (VERVAFS, 2007)); JAV patvirtinti Sarbanes-Oxley Act (SOX, 2002), kuris įtvirtino reikalavimus privačiam sektoriui, ir Federal Information Security

Management Act (FISMA, 2002), kuris nustatė privalomus informacijos saugumo valdymo įpareigojimus visam JAV viešajam sektoriui. Saugumo valdymo reikalavimai ilgainiui taip pat buvo nustatyti ir specifinėms verslo bei veiklos šakoms: medicininę informaciją tvarkančioms organizacijoms – Health Insurance Portability and Accountability Act (HIPAA, 1996), finansinę informaciją – Payment Card Industry Data Security Standard (PSI, 2008)), kurie dėl savo universalumo taikomi kaip saugumo valdymo metodikos ir kitose srityse.



2 pav. Informacijos saugumo sąvokos raida (pagal von Solms 2000, 2006, 2010).

Pristatytų informacijos saugumo bangų skiriamasis bruožas – jų orientacija į organizacijos vidinę veiklą ir valdomą informaciją, tačiau įvertinant, kad organizacijos nuotoliniam darbui, elektroninei komercijai ir kitai veiklai vis labiau išnaudoja interneto ir kitas organizacijos tiesiogiai nekontroliuojamas viešojo tinklo technologijas, Basie von Solms išskyrė *penktąją, kibernetinio saugumo* (angl. *Cyber Security*), bangą. Prie šios bangos susiformavimo taip pat prisidėjo ir besitransformuojantis rizikos šaltinis; autorius įvertino, kad vis didesnę grėsmę pradeda kelti ne dažnai pakankamai stipriai apsaugotais organizacijos ištekliais bandantys neteisėtai pasinaudoti

asmenys, o paprasti, „naivūs“ vartotojai, kurie taip pat yra ir organizacijų elektroninių paslaugų klientai ar darbuotojai, dirbantys iš įvairiausių nutolusių kompiuterių, mobiliųjų ar kitų įrenginių, tačiau skiria nepakankamai dėmesio šių įrenginių (ypač asmeninių) saugumui ir taip tampa grėsme organizacijų informaciniams ištekliams. Taigi kibernetinio saugumo banga pasižymi dėmesiu ir organizacijos išorinės aplinkos poveikiui (von Solms, 2010).

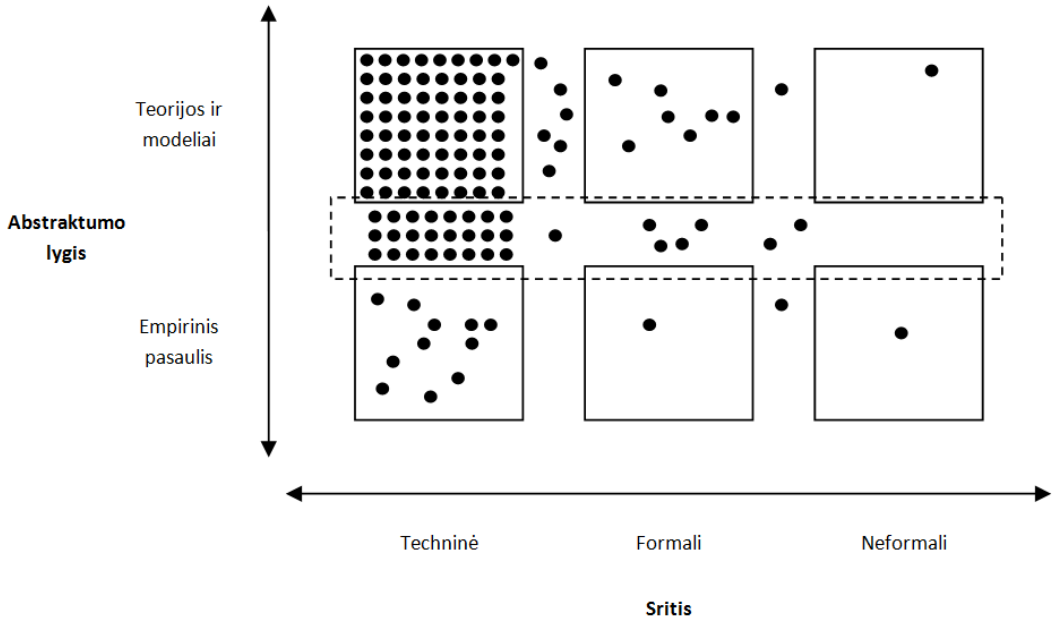
Apibendrinant informacijos saugumo sampratos genezę galima pastebėti slinktį dviem kryptimis: *visų pirma* akivaizdžiai augantis informacijos saugumo, kaip mokslinių tyrimų objekto, aktualumas – tyrėjų skaičiavimais, mokslų darbų skaičius per paskutinį dešimtmetį išaugo kelis kartus; *antra* – plečiasi informacijos saugumo sampratos turinys, kurio dedamąsias tikslinga nagrinėti įvertinat platesnį informacijos saugumo tyrimų aprėpties kontekstą.

1.1.3. Informacijos saugumo tyrimų aprėptys

Siekiant atskleisti informacijos saugumo turinio kompleksiškumą tikslinga išnagrinėti mokslinę literatūrą ir sujungti į bendrą visumą informacijos saugumo tyrėjų nagrinėjamus pavienius informacijos saugumo aspektus ir jų tarpusavio sąsajumą, analizuojamas besiplečiančias informacijos saugumo turinio aprėpties ribas ir informacijos saugumo problemų kilmę bei informacijos saugumo užtikrinimo būdų ir priemonių paieškas.

Nagrinėjant mokslinių publikacijų, skirtų informacijos saugumo problematikai, visumą, galima konstatuoti, kad didžiausias yra įvairių *technologinių* informacijos saugumo aspektų teorinis ištirtumas. Šią tendenciją patvirtino F. Bjorck ir L. Yngstrom (2009), kurie sudarė savo informacijos saugumo tyrimų klasifikavimo modelį ir pagal jį išnagrinėjo ir suklasifikavo 2000 metų Tarptautinės informacijos apdorojimo federacijos (International Federation for Information Processing (IFIP) Kompiuterių kongreso, skirto informacijos saugumui (IFIP Word Computer Congress / SEC 2000), straipsnius. Šis modelis leido sudaryti konferencijos medžiagoje publikuotų 125 straipsnių matricą pagal jų *abstraktumo lygį* (x ašyje) nuo *teorinių* iki *praktinių* darbų bei nagrinėjamą *sritį* (y ašyje), kurioje buvo išskirtos *techninė,*

formalioji ir *neformalioji sritys*. *Techninei sričiai* autoriai priskyrė straipsnius, kurių pagrindinės nagrinėjamos temos – kompiuterių techninė ir programinė įranga, ryšių protokolai, kriptografiniai algoritmai, įvairios techninio įvertinimo metodikos ir pan.; *formaliai sričiai* buvo priskirti straipsniai, nagrinėjantys įvairias žmonių elgesį formalizuojančias procedūras, pavyzdžiui, saugumo politikos, teisės aktai ir pan.; *neformaliai sričiai* – įvairūs mokslo darbai, nagrinėjantys socialinius ryšius, etiką, saugumo poveikį tarpasmeniniam bendravimui bei neformalų žmonių elgesį. Straipsniai, nagrinėjantys teorinius modelius ir jų praktinį įgyvendinimą, buvo pažymėti punktyru išskirtoje zonoje (3 paveikslas). Ši analizė parodė, kad iš 125 konferencijos medžiagoje publikuotų straipsnių, net 83 procentai priskirtini techninei sričiai, 14 procentų formaliajai ir 3 procentai neformaliajai sritims.



3 pav. Informacijos saugumo tematikos mokslinių publikacijų matrica (Bjorck ir Yngstrom, 2009).

Panašios tendencijos ryškėja ir išanalizavus Lietuvos autorių teorinius ir empirinius informacijos saugumo tyrimus. Lietuvos mokslų žurnalų turinio analizė leidžia konstatuoti, kad daugiausia informacijos saugumo mokslinių tyrimų publikuota Kauno Technologijos universiteto kartu su Lietuvos Mokslų

Akademija, Vilniaus Gedimino Technikos universitetu bei Rygos ir Talino technikos universitetais leidžiamame mokslo žurnale „Elektronika ir elektrotechnika“ ir Kauno technologijos universiteto mokslo žurnale „Information technology and control“. Absoliuti dauguma Lietuvos tyrėjų nagrinėja įvairius techninius informacijos saugumo aspektus (Garšva, 2006; Mikučionis et al. 2007; Paulauskas, 2009 ir kiti). Galima išskirti dar kelis daugiau Lietuvos tyrėjų dėmesio sulaukusius informacijos saugumo aspektus, pavyzdžiui, teisinio reglamentavimo ir reguliavimo (Čėsna, Štitilis, 2000; Štitilis, Paškaukas, 2007; Paškauskas, 2007 ir kiti), informacijos nuosavybės teisių apsaugos (Kasperavičius ir Žilinskas, 2004; Kiškis, 2009; Stonkienė, 2009 ir kiti), saugos priemonių naudojimo (Kazanavičius et al. 2012; Japertas, Činčikas ir Šestaviskas, 2012; Paulauskas, 2009; Šerpenskas, 2001 ir kiti), komunikacinius (Janeliūnas, 2007 ir kiti), mokymų (Venčkauskas, Krivickienė, Toldinas, 2009 ir kiti).

Globalių informacijos saugumo tyrimų tendencijų kontekste *technologinių aspektų* tyrimų gausą veikė tai, kad tokie tyrimai prasidėjo dar 1970 metais. Šiuose tyrimuose daug dėmesio skirta techninės ir programinės įrangos architektūros tyrimams, kriptografinėms priemonėms, slaptažodžių, biometrijos ir kitų identifikavimo ir prieigos prie informacinių sistemų priemonių patikimumui nagrinėti, saugios komunikacijos, tinklų topologijos, ugniasienių ir kitoms informacijos saugumo technologijoms analizuoti. Remiantis išnagrinėtais literatūros šaltiniais, informacijos saugumo mokslo šaknis galima kildinti iš karinės ir panašių griežtai struktūrizuotų sričių, kaip kompiuterių mokslai ir programinės įrangos inžinerija; labiausiai su šiais tyrimais susijusios matematikos ir matematinės arba filosofinės logikos mokslo šakos, tyrimams daugiausiai naudojami šių mokslų metodai, o plačiausiai aptartos teminės grupės – prieiga prie informacinės sistemos ir saugi komunikacija (Dhillon ir Backhouse, 2001; McFadzean, Ezingeard ir Birchall, 2006; Siponen ir Oinas-Kukkonen, 2007; D‘Archy ir Hovav, 2009; Zafar ir Clark, 2009).

Ross Anderson ir Tyler Moore taip pat pažymi, kad iki pat 2000 metų informacijos saugumas daugiausiai buvo suprantamas tik kaip technologijų srities disciplina, tačiau šie Kembridžo ir Harvardo universitetų tyrėjai teigia, kad nusistovėjęs požiūris ėmė kisti, kai mokslininkai ir praktikai pradėjo suvokti *ekonominių veiksnių* įtaką; tuomet šalia „tradicinių“ saugumo iššūkių, tokių kaip privatumas, programinės įrangos klaidos ar vartotojų tapatybės pasisavinimas (angl. *phishing*), atsiranda informacijos sistemų patikimumas, strateginis planavimas, finansų ir investicijų valdymas ir kiti *ekonominiai veiksniai* (Anderson ir Moore, 2009; D'Archy ir Hovav, 2009). *Ekonominiai veiksniai* taip pat spaudžia informacinių technologijų sprendimų kūrėjus skubėti išleisti į rinką vis naujus produktus, skirtus informacijos saugumui užtikrinti, dažnai neskiriant pakankamai laiko šiems produktams tinkamai pabaigti, paliekant klaidų šalinimą būsimiems programinės įrangos patobulinimams. Iš esmės pačių informacinių technologijų produktų gamintojų *ekonominių veiksnių* nulemti sprendimai ir per menkas dėmesys mokslo įžvalgoms suformavo dabartinę informacijos saugumo situaciją (Anderson, 2001; Caelli, 2002; Gordon ir Loeb, 2006; Johnson, 2009). Tampa akivaizdu, kad *ekonominių veiksnių* atžvilgiu išlaidos informacijos saugumui vertinamos kaip nebūtini kaštai, neatnešantys aiškios pridėtinės finansinės naudos. Ekonominiai veiksniai šalia sudėtingų technologijų ir kompetencijos trūkumo vertintini kaip viena giluminių informacijos saugumo valdymo problemų priežasčių (Audestad, 2005; Helms, Ettkin ir Morris, 2000; Schell, 2001 ir kiti), todėl, siekiant išvengti neigiamos *ekonominių veiksnių* įtakos informacijos saugumui, būtina rasti svertus, kurie subalansuotų ekonominio rezultato ir informacijos saugumo tikslus. *Ekonominiai veiksniai* neturi būti pagrindinis ar net vienintelis veiksnys, sąlygojantis sprendimų priėmimą tiek kuriant informacijos saugumo produktus, tiek priimant bet kokius kitus organizacijos veiklos valdymo sprendimus.

Technologinių, ekonominių veiksnių sąsajumas su psichologiniais ir kitais žmogiškojo faktoriaus veiksniais išryškėja nagrinėjant pačių informacijos saugumo valdymo technologijų sudėtingumą. JAV Carnegie Mellon ir

Kalifornijos universitetų mokslininkų grupės, vadovaujamos Alma Whitten ir J. D. Tygar, atlikta studija atskleidė didžiulę properšą tarp saugumo programų kūrėjų lūkesčių ir vartotojų veiksmų – ekspertų sukurtos saugumo programos, skirtos eiliniams vartotojams, yra per sudėtingos, vartotojai nesupranta šių programų siūlomų galimybių ir panaudojimo tikslų ir, klaidingai jas interpretuodami, palieka saugumo spragų, o pačių programų turėjimas vartotojams suformuoja klaidingą saugumo jausmą įsivaizduojant, kad jų naudojamos technologijos yra saugios (Whitten, Tygar, 1999). Panašius rezultatus atskleidė ir kiti tyrimai, kurių išvadose pabrėžiami saugumo programų kūrėjų įsivaizduojamų teorinių problemų ir realios šių programų diegimo ir valdymo praktikos skirtumai ir net pačių programų kūrėjų netikrumas dėl jų kuriamų produktų saugumo (Anderson, 1994; Anderson ir Moore, 2009).

Psichologinių ir kitų žmogiškųjų aspektų aktualumą dar labiau išryškina paskutinio dešimtmečio tendencijos. Organizuojant saugumo atakas ar kitą nusikalstamą veiklą, vis dažniau saugumo spragų ieškoma ne įvairiomis sudėtingomis priemonėmis apsaugotose informacinėse sistemose, o nusitaikoma į „silpniausią saugumo grandį“ – informacinių sistemų vartotojus. Siekiant iš vartotojų surinkti jautrią informaciją, kuri galėtų būti panaudota apeiti technines, programines ir kitas informacinių sistemų apsaugos priemones, vis labiau išnaudojamos įvairios psichologinės priemonės bei kiti socialinės inžinerijos instrumentai. Tam prielaidas sudaro kelios priežastys: 1) žmonės dažnai yra patiklūs, kaip rodo socialinės psichologijos studijų eksperimentai, kartais net ir neigdami akivaizdžią realybę; 2) *žmogiškasis veiksnys* ilgą laiką nebuvo nagrinėjamas kaip sudėtinė informacijos saugumo valdymo dalis; 3) egzistuoja informacijos saugumo ekspertų glaudaus dialogo su kitais organizacijos nariais trūkumas; 4) vartotojai nesupranta saugumo problemų svarbos, nemano, kad informacija apie organizacijos informacijos saugumo organizavimą yra vertinga (Asch, 1952; Ashenden, 2008; Bakhshi, Papadaki ir Furnell, 2009; Kelly 2007; Mitnick ir Simon 2002; Timko, 2008).

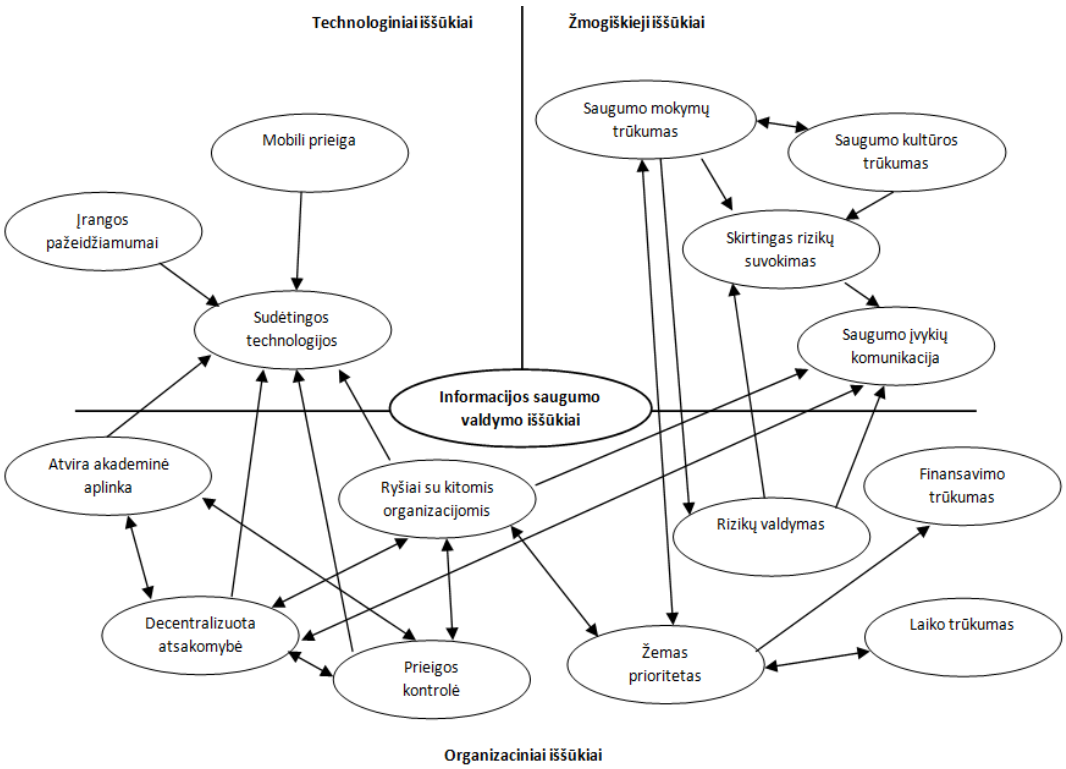
Šalia aptartų *techninių, ekonominių, psichologinių ir kitų žmogiškojo faktoriaus aspektų* svarbus ir jau minėto Basie von Solms, pristačiusio *informacijos saugumo bangas*, ir kitų tyrėjų pabrėžiamas informacijos saugumo multidisciplininiškumas, apimantis *organizacijos valdymo, saugumo politikos, etikos, sertifikavimo, teisinius, mokymų, vertinimo ir stebėjimo* bei kitus informacijos saugumo valdymui svarbius aspektus (Eloff ir Eloff, 2003; Higgins, 1999; von Solms 2001). Vertinant tyrėjų įžvalgas analizuojant *saugumo politikų, standartų* ir kitų valdymo priemonių taikymo sėkmingumą tiek verslo organizacijose, tiek valstybės institucijose, galima pastebėti keletą tendencijų: 1) sėkmingiausi informacijos saugumo valdymo priemonių taikymo pavyzdžiai yra tose organizacijose, kurios sugebėjo sujungti strateginius pačios organizacijos veiklos tikslus su informacijos saugumo tikslais ir diegdamos informacijos saugumo valdymo priemones kartu aktyviai skatino organizacijos saugumo kultūros kėlimą bei vykdė plačias mokymo programas; 2) svarbus valstybės koordinuojantis indėlis tiek nustatant informacijos saugumo valdymo priemonių privalomumą, tiek imantis lyderio vaidmens diegiant šias priemones, tiek skiriant pakankamą finansavimą valstybės institucijų kontekste ar taikant kitas skatinimo priemones verslo organizacijų kontekste (Hall, Sarkani ir Mazzuchi, 2010; Fulford ir Doherty, 2003; Doherty ir Fulford, 2006; Ghormley, 2009; Kayworth ir Whitten, 2010; Knapp et al., 2006; Loukis ir Spinellis, 2001; Rathnam, Johnsen ir Wen, 2004; Sharma ir Gupta, 2009; Smith et al., 2010 ir kiti).

Plačiau nagrinėjant paskutinio dešimtmečio informacijos saugumo mokslinių tyrimų tendencijas atskleidžiančias ir praktinio informacijos saugumo valdymo problemas, ryškėja, kad vis daugiau informacijos saugumo iššūkių kyla sprendžiant *organizacinius aspektus*; šiuo metu svarbiausiomis informacijos saugumo temomis tampa atitiktis teisės aktų reikalavimams; standartų, reguliavimo, gerųjų praktikų įtakos saugumo technologijų raidai; organizacijos valdymo kultūros ir gerų praktikų sėkmingo įdiegimo santykis; ekonominiai saugos priemonių pasirinkimo ir diegimo aspektai; saugumo technologijų įtaka vartotojų elgesiui; pažeidimų ir informacijos saugos

valdymo efektyvumo vertinimas; rizikų ir informacijos saugumo valdymas; informacijos saugumo sąmoningumo kėlimas, mokymai ir kiti žmogiškieji aspektai; incidentų valdymas ir atstatymas po nelaimingų atsitikimų bei saugių informacinių sistemų kūrimo ir saugumo valdymo problematika. Šių aspektų įtaka nagrinėjama pasitelkiant psichologijos, sociologijos, semiotikos ir filosofijos mokslus (Siponen ir Oinas-Kukkonen, 2007; D'Archy ir Hovav, 2009; Dlamini et al, 2009).

Bandant susisteminti informacijos saugumo tyrimų kryptis, tikslinga grupuoti aptartus informacijos saugumo aspektus. Šiame kontekste vertinga pasiremti ir JAV, Kanados bei Taivano mokslininkų informacijos saugumo valdymo kaip multidisciplininio tyrimų objekto poziciją išryškinančiais tyrimais. Tyrėjai savo empirinėse studijose atkreipia dėmesį, kad nors mokslinėje literatūroje plačiai tebediskutuojama apie *technologinius aspektus,* tačiau pabrėžia, jog būtina vertinti organizacijos kultūros ir valdymo principų sąsajas. Atlikti kokybiniai aktualių informacijos saugumo valdymo iššūkių tyrimai, pasitelkiant saugumo profesionalus iš akademinio ir privataus sektorių, leido identifikuoti platų spektrą aktualių informacijos saugumo iššūkių, o sugrupavus šiuos iššūkius į žmogiškuosius, organizacinius ir technologinius nustatyti iššūkių priklausomybes (4 paveikslas). Šios įžvalgos išryškino, kad efektyvus informacijos saugumo valdymas turi remtis subalansuotu *technologinių*, *žmogiškųjų* ir *organizacinių* veiksnių koordinavimu (Chang ir Lin, 2007; Parakkattu ir Kunnathur, 2010; Werlinger et al, 2009).

Apibendrinant mokslinius tyrimus, galima teigti, kad nors techniniai klausimai tebėra aktualūs, pastebima ryški informacijos saugumo konteksto slinktis platesnio, apimančio vis daugiau aspektų, vadybinio požiūrio link. Šiuos pokyčius M. Dlamini, J. Eloff ir M. Eloff charakterizavo judėjimu strateginio požiūrio, kuris pasireiškia informacijos saugumo administravimo *(information security management)* virtimu informacijos saugumo valdymu *(information security governance),* kryptimi (Dlamini, Eloff ir Eloff, 2009). Plačiau informacijos saugumo valdymo apibrėžtis nagrinėjama kitame disertacijos poskyryje.



4 pav. Informacijos saugumo iššūkių sąsajos (Werlinger et al. 2009).

1.1.4. Informacijos saugumo valdymo apibrėžtis

Nagrinėjant saugumo sąvoką, kaip objektyvaus saugumo būseną, kyla poreikis įvardyti ne tik objektą, kuris turi būti (tapti) saugus, bet sąlygas, kurios leidžia įvardyti objektą, esantį (tapusį) saugų. Išanalizavus informacijos saugumo sampratą, jos genezę bei tyrimų aprėptis, aiškėja platus bei nuolat kintantis informacijos saugumo sąlygų kontekstas. Taigi norint pasiekti ir išlaikyti informacijos saugumą (valdyti objektyvaus saugumo būseną), būtina aiškiai identifikuoti informacijos saugumo sąlygas ir procesą, kuris leistų reaguoti į šių sąlygų kaitą, t. y. apibrėžti informacijos saugumo valdymo turinį ir priemones.

Remiantis teorinių įžvalgų, pateiktų pirmuose šios disertacijos dalies poskyriuose, visuma, galima konstatuoti mokslinėse diskusijose nagrinėjamų aktualių informacijos saugumui aspektų plėtrą. Informacijos saugumo valdymo turiniui išryškinti svarbią reikšmę įgyja nuo devinto dešimtmečio (lygiagrečiai

siauriems pavienių informacijos saugumo aspektų tyrimams) pradėję vystytis tarpdisciplinai informacijos saugumo tyrimai. Išanalizavus Lietuvos ir užsienio informacijos saugumo mokslinių tyrimų aprėptis, galima aiškiai įvardyti, kad informacijos saugumo sąvokos turinys formavosi techninių ir technologinių problemų sprendimo kontekste. Techninės (informacinių technologijų) problemos informacijos saugumo aspektu nagrinėtos plačiausiai ir išlieka labai svarbios, tačiau galima pastebėti, kad šios informacijos saugumo problemoms spręsti nebeužtenka techninių priemonių. Informacijos saugumo apibrėžtis, apimdama ekonominius, žmogiškuosius, organizacinius ir kitus aspektus bei išryškindama jų tarpusavio sąryšius, tampa vadybine disciplina ir aktualia moksline problema.

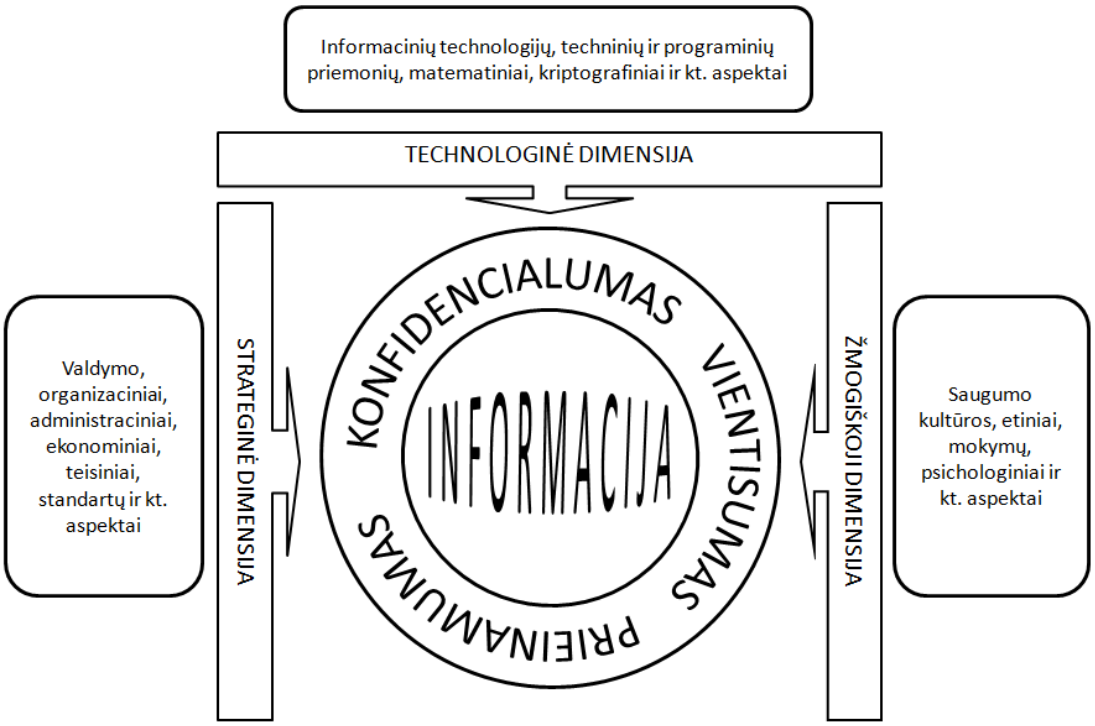
Apibendrinant ankstesniuose disertacijos poskyriuose aptartus informacijos saugumo tyrimus ir juose analizuotus informacijos saugumo aspektus, galima konstatuoti, kad informacijos saugumo valdymas apima tris dimensijas – strateginę, žmogiškąją ir technologinę:

- strateginė dimensija jungia administracinius, organizacinius, valdymo, ekonominius, standartų, teisinius, gerųjų praktikų ir pan. aspektus;
- žmogiškoji – saugumo kultūros, etinius, kompetencijų, mokymų, psichologinius ir pan. aspektus;
- technologinė – informacinių technologijų, techninių ir programinių priemonių, matematinius, kriptografinius ir pan. aspektus.

Visuminiam požiūriui į informacijos saugumo valdymo turinį apibrėžti tikslinga sujungti informacijos saugumo valdymo objektą, tikslus ir dimensijas. Remiantis aptarta teorine medžiaga ir sudaryta informacijos saugumo sąvokų hierarchine schema (pateikta disertacijos 1.1.1 poskyryje, 1 paveikslas), pagrindiniu informacijos saugumo valdymo objektu įvardytina informacija. Informacijos saugumo valdymo tikslais, pasiremiant disertacijos 1.1.1 poskyryje aptartomis įžvalgomis, įvardytina CIA triada – konfidencialumas, vientisumas ir prieinamumas. Visuminį požiūrį į informacijos saugumo

valdymo kontekstą išreiškia ir informacijos saugumui aktualius veiksnius sujungia strateginė, žmogiškoji ir technologinė informacijos saugumo valdymo dimensijos.

Taigi informacijos saugumo valdymo turinys gali būti apibrėžiamas kaip siekis užtikrinti informacijos konfidencialumą, vientisumą ir prieinamumą subalansuotai derinant strateginę, žmogiškąją ir technologinę dimensijas (5 paveikslas).



5 pav. Informacijos saugumo valdymo turinys (sudaryta autoriaus).

Siekiant valdyti informacijos saugumą nepakanka apibrėžti informacijos saugumo valdymo turinį, tačiau būtina numatyti ir priemones, kuriomis jis galėtų būti valdomas. Analizuodami galimybes užtikrinti sistemišką ir subalansuotą informacijos saugumo valdymą, tyrėjai nagrinėjo informacijos saugumo valdymo sistemų, gerųjų praktikų, standartų ir kitų valdymo priemonių, pavyzdžiui, Demingo rato (Planuok–Daryk–Tikrink–Veik), taikymo galimybes (Gorge, 2009; Weise, 2009; Eloff ir Eloff, 2003; von Solms

2001 ir kiti). Kitame disertacijos skyriuje detaliai nagrinėjamos plačiausiai taikomos informacijos saugumo valdymo priemonės.

1.2. Informacijos saugumo valdymo priemonės

Platus informacijos saugumo valdymo apibrėžties turinys inspiravo atitinkamų jo valdymo priemonių poreikį. Tarptautiniame lygmenyje formavosi reikmė nustatyti informacijos saugumo vertinimo kriterijus, apibrėžti palyginamus dydžius, užtikrinti suderinamumą, nustatyti bendras sertifikavimo metodikas, geriausias praktikas ir jų įgyvendinimo gaires. Šie poreikiai iššaukė formalizuotų informacijos saugumo užtikrinimo priemonių atsiradimo būtinybę, tokiomis priemonėmis tapo šiame skyriuje aptariami vyraujantys tarptautiniai informacijos saugumo valdymo standartai, metodikos ir modeliai.

1.2.1. Informacijos saugumo valdymo standartai

Pagrindinėmis informacijos saugumo valdymo priemonėmis susiformavo standartai, kurių šaltiniais tapo pavienių verslo šakų generuojamos metodikos, vyriausybių nustatomi reikalavimai bei nacionalinių ir tarptautinių standartizacijos organizacijų tvirtinami sutarimai (Amaral, 2007; Weise, 2009 ir kiti).

Pasauliniu mastu aktualiausi Tarptautinės Standartizacijos Organizacijos *(International Organisation for Standardisation (ISO)* priimti tarptautiniai susitarimai, kurie skelbiami kaip tarptautiniai standartai. Ši organizacija, kurdama informacijos ir ryšių technologijų srities standartus, bendradarbiauja su Tarptautine Elektrotechnikos Komisija (*International Electrotechnical Commission (IEC)* ir Tarptautine Telekomunikacijų Sąjunga *(International Telecommunication Union (ITU).*

Analizuojant ISO standartų katalogą[2], galima rasti per 350 standartų, susijusių su įvairiais informacijos saugumo valdymo aspektais, tačiau

[2] ISO. Standards Catalogue. http://www.iso.org/iso/catalogue_ics. (žiūrėta 2012 m. liepos 16 d.)

išanalizavus šiame kataloge pateiktus jų turinio aprašymus bei vertinant bendrą informacijos saugumo srities standartų aprėptį, galima konstatuoti, kad daugiausiai standartų susiję su įvairiomis techninėmis saugumo užtikrinimo priemonėmis. Vertinant informacijos standartų vystimąsi, pabrėžtina, kad tik 1995 metais pasirodė pirmasis informacijos saugumo standartas, plačiau išryškinęs vadybines dedamąsias (tokiu standartu tapo Didžiosios Britanijos standartizacijos įstaigos patvirtintas standartas BS 7799[3]). Tarptautinėje erdvėje vis labiau ryškėjant suderintam informacijos saugumo valdymo poreikiui, 2000 metais, pripažinus britiškojo standarto privalumus, jo pagrindu buvo parengtas tarptautinis ISO 17799 standartas, vėliau išsivystęs į atskirą informacijos saugumo valdymo standartų grupę ISO 27000. Šios grupės standartai skirti tiesiogiai informacijos saugumo valdymui, informacijos saugumo valdymo sistemai kurti, praktinėms priemonėms diegti, įvertinti ir organizacijai sertifikuoti (plačiau šios grupės standartai pristatyti disertacijos 2 priede). Remiantis J. Weise, M. Gorge ir kitų informacijos saugumo valdymo standartų taikymo tyrėjų įžvalgomis, pažymėtina, kad ISO 27000 grupės standartai yra pripažinti *de facto* informacijos saugumo valdymo gerosios praktikos pavyzdžiu (Gorge, 2009; Weise, 2009; Susanto, Almunawar ir Tuan, 2011 ir kiti).

Svarbiausias ISO 27000 grupės standartas, numatantis informacijos saugumo sistemos įgyvendinimo priemones, – ISO 27002. Šiame standarte išskirta 11 priemonių grupių (dimensijų) informacijos saugumo valdymui:

1. Saugumo politika. Apibrėžiamas informacijos saugumo politikos, kaip pagrindinio organizacijos informacijos saugumo dokumento, sukūrimas ir šio dokumento gyvavimo ciklo peržiūra.

2. Saugumo organizavimas. Aptariamas informacijos saugumo organizavimas ir valdymas organizacijoje.

3. Vertybių klasifikavimas ir kontrolė. Apibrėžiama turimų vertybių peržiūra, naudojimas, klasifikacijos sistema. Pagal ISO 27000 standartų šeimą

[3] BSI // http://www.bsigroup.co.uk/, (žiūrėta 2012 m. birželio 1 d.)

informacija skirstoma į keturias grupes: elektronines bylas, popierinius dokumentus, įrašus ir komunikacijas.

4. Personalo saugumas. Akcentuojamas saugos kultūros ugdymas visoje organizacijoje bei siekis, kad organizacijos nariai suprastų, jog informacijos saugumas yra viena kertinių organizacijos egzistavimo sąlygų ir jo užtikrinimas turi būti visų organizacijos narių bendra atsakomybė.

5. Fizinis ir aplinkos saugumas. Svarbu užtikrinti patalpų, kuriose yra techninė įranga, ir pačios techninės įrangos saugumą.

6. Komunikacijos ir operacijų valdymas. Organizacija turi formalizuoti ir sistematizuoti visas informacijos saugumo procedūras bei vidines komunikacijas.

7. Prieigos kontrolė. Apibrėžiami priėjimo prie informacijos principai, metodai, užtikrinimo priemonės ir jų kontrolė.

8. Sistemų kūrimas ir priežiūra. Aptariama veikla susijusi su organizacijos informacinių sistemų ir programinės įrangos gyvavimo ciklo priežiūra.

9. Incidentų valdymas. Aptariamos procedūros, kurios turi būti vykdomos įvykus informacijos saugumo pažeidimui.

10. Veiklos tęstinumo valdymas. Užtikrinamas plano ir procedūrų parengimas, šių dokumentų aktualumo priežiūra, darbuotojų mokymai ir įgyvendinimo kontrolė.

11. Atitikimas. Siekiama užtikrinti organizacijos veiklos atitiktį išoriniams reikalavimams, teisės aktams ir kitiems įsipareigojimams.

Apibendrinant informacijos saugumo valdymo standartų genezę, joje galima įžvelgti labai ryškų, ankstesniuose disertacijos skyriuose aptarto, mokslinių informacijos saugumo tyrimų tendencijų atspindį, t. y. informacijos saugumo akcentų slinktį nuo technologijų vadybos link.

1.2.2. Informacijos saugumo valdymo metodikos

Valdant informacinių sistemų projektus bei diegiant įvairius informacinių technologijų sprendimus susiklostė gerų praktikų pavyzdžiai,

kurie ilgainiui tapo plačiai pripažįstamomis, nuolat tobulinamomis metodikomis, savo turinyje integravusiomis ir informacijos saugumo valdymo priemones. Daugiausia tarptautinio dėmesio sulaukė COBIT ir ITIL metodikos, kurios taip pat apima ir informacijos saugumo valdymą.

COBIT (Control Objectives for Information and Related Technologies)[4] – pasaulyje pripažintas metodikų rinkinys Informacijos ir ryšių technologijų ūkio valdymui, kuris remiasi rinkos standartais ir geriausiomis praktikomis. Pirmoji metodikų rinkinio versija išleista 1996 metais, ją nuolat tobulina Informacinių technologijų valdymo institutas *(IT Governance Institute (ITGI)* ir Informacinių sistemų audito ir valdymo asociacija *(Information Systems Audit and Control Association (ISACA).* Integruotas šios metodikos požiūris į visą organizacijos informacinių technologijų procesų tvarkymą apima ir informacijos saugumo valdymą.

COBIT metodika (4.1. versija, išleista 2007 metais) išversta į daugiau nei dešimt įvairių kalbų, 2011 m. lapkričio mėn. buvo pristatytas COBIT metodikos vertimas ir į lietuvių kalbą[5]. Ši COBIT metodikos versija susideda iš septynių dalių: Santrumpa vadovui *(Executive overview),* COBIT principai *(COBIT framework),* Planavimas ir organizavimas *(Plan and Organise, PO),* Įsigijimas ir įdiegimas *(Acquire and Implement, AI),* Paslaugų teikimas ir palaikymas *(Deliver and Support, DS)*, Stebėjimas ir įvertinimas *(Monitor and Evaluate, ME*), ir Priedai *(Appendices).* Visas metodikos turinys padalintas į pagrindines 4 sritis *(PO, AI, DS ir ME)* ir 34 procesus, kuriuose labiau akcentuojama tai, kas turi būti daroma, mažiau dėmesio skiriant įgyvendinimo būdams.

COBIT pagrindinės informacijos saugumo valdymo priemonės koncentruotos Paslaugų teikimo ir palaikymo (DS) srities Sistemų saugos užtikrinimo procese (DS5), kuris susideda iš šių kontrolės objektų:

[4] COBIT // http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx, (žiūrėta 2011 m. kovo 10 d.)
[5] Lietuviška COBIT versija // http://www.cobit.lt/, (žiūrėta 2012 m. vasario 1 d.)

1. Saugumo valdymas. Saugumą turi valdyti aukščiausio, tinkamo lygio organizacijos darbuotojai ir saugumo veiksmų valdymas turi atitikti veiklos poreikius.

2. Saugumo planas. Veiklos, rizikos ir atitikties reikalavimai turėtų integruotis į bendrąjį informacinių technologijų saugumo planą, kurį įgyvendina saugumo politika ir procedūros kartu su atitinkamomis investicijomis į paslaugas, darbuotojus, programinę ir techninę įrangą. Suinteresuotų šalių naudotojai turi būti informuoti apie saugumo politiką ir procedūras.

3. Tapatybės valdymas. Visi naudotojai (vidaus, išorės ir laikini) ir jų veiksmai visų lygių informacinių technologijų sistemų aplinkose (testavimų, gamybinėje) tiek jas kuriant, tiek prižiūrint turi būti unikaliai identifikuojami, dokumentuojami, tinkamai įgyvendinami, privalo atitikti veiklos poreikius ir būti kontroliuojami.

4. Naudotojo paskyros valdymas. Turi būti nustatytos naudotojo paskyros valdymo procedūros, taikomos visiems naudotojams (administratoriams (privilegijuotiems naudotojams) bei vidaus ir išorės naudotojams tiek įprastais, tiek avariniais atvejais).

5. Saugumo testavimas, priežiūra ir stebėsena. Informacinių technologijų saugumas turi būti testuojamas, stebimas, laiku perakredituojamas, kad būtų užtikrintas patvirtintų organizacijos informacijos saugumo bazinių rodiklių išlaikymas.

6. Saugumo incidento apibrėžimas. Turi būti apibrėžti ir iškomunikuoti galimų saugumo incidentų požymiai, kad incidentų ir problemų valdymo procesas galėtų juos tinkamai klasifikuoti ir apdoroti.

7. Saugumo technologijų apsauga. Saugumo technologijos turi būti atsparios tiek tyčiniams, tiek ir netyčiniams pažeidimams (gadinimui). Be reikalo neturėtų būti viešai skelbiami dokumentai, detaliai aprašantys saugumo užtikrinimo priemones.

8. Kriptografinio rakto valdymas. Turi būti sukurta politika ir procedūros, skirtos tvarkyti kriptografinių raktų generavimą, keitimą,

panaikinimą, sunaikinimą, platinimą, patvirtinimą, saugojimą, įvedimą, naudojimą ir archyvavimą.

9. Kenksmingos programinės įrangos prevencija, aptikimas ir koregavimas. Visoje organizacijoje apsaugai turi būti taikomos kenksmingos programinės įrangos prevencinės, detekcinės ir korekcinės priemonės (pvz., virusų, kirminų, šnipinėjimo programų, elektroninio pašto šiukšlių).

10. Tinklo saugumas. Suteikiant prieigą ir kontroliuojant informacijos srautus iš tinklų ir į juos, turi būti taikomi saugumo metodai ir susijusios valdymo procedūros (pvz., ugniasienės, saugumo įranga, tinklo segmentacija, įsibrovimo aptikimas).

11. Keitimasis diskretiškais duomenimis. Diskretiškais operacijų duomenimis turi būti keičiamasi tik per patikimą maršrutą ar laikmeną taikant kontrolės priemones, užtikrinančias turinio autentiškumą, įrodymus apie duomenų pateikimą, gavimą ir negalėjimą nepripažinti duomenų kilmės.

Pateikti DS5 saugumo kontrolės objektai nėra vieninteliai, susiję su saugumo užtikrinimu. Daug svarbių kontrolės objektų yra ir kituose 33 COBIT metodikos informacinių technologijų valdymo procesuose. Paminėtini kiti Paslaugų teikimo ir palaikymo (DS) dalies kontrolės objektai – saugos incidentų apibrėžimas, mokymai apie saugos supratimą, informacinių technologijų saugos planas ir politika; Planavimo ir organizavimo (PO) dalies – duomenų klasifikacijos, technologinių standartų, rizikos vertinimo, saugos grėsmių ir silpnųjų vietų kontrolės objektai; Įsigijimo ir įdiegimo (AI) dalies – taikomųjų programų saugos kontrolės priemonių specifikacijų, reikalingų saugos pakeitimų kontrolės objektai.

Vertinant COBIT metodikos vystimąsi, galima konstatuoti, kad kiekvienoje versijoje informacijos saugumui valdyti skiriamas vis didesnis dėmesys, o informacijos saugumo užtikrinimas vis glaudžiau integruojamas į bendrus informacinių technologijų sėkmingo valdymo procesus. Ši tendencija tęsiama ir šiuo metu rengiama COBIT metodikos 5-oji versija[6], kurios projekte

[6] COBIT metodikos 5 versijos projektas // http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-5-Initiative-Status-Update.aspx, (žiūrėta 2012 m. vasario 1 d.)

saugumas išryškinamas kaip vienas svarbiausių uždavinių. Naujos metodikos versijos laukiama pasirodant 2012 metais.

ITIL (Information Technology Infrastructure Library)[7] – verslo valdymo metodologija, orientuota į darbo optimizavimą bei kokybės užtikrinimą informacinių ir ryšių technologijų kompanijose ar įmonių informacinių ir ryšių technologijų padaliniuose. ITIL yra kompleksinė informacinių ir ryšių technologijų valdymo metodologija, paremta geriausių praktikų pavyzdžiais. Metodikos pagrindinis vystytojas – Didžiosios Britanijos Vyriausybės Prekybos rūmai *(Office of Government Commerce (OGC)*.

ITIL metodologija taip pat pripažinta Tarptautinės standartizacijos organizacijos standartais – ISO/IEC 20000-1:2005, ISO/IEC 20000-2:2005, ISO/IEC TR 20000-3:2009, ISO/IEC TR 20000-5:2010, kurie šiuo metu peržiūrimi pagal 3-ąją ITIL versiją.

ITIL metodika apima kontrolės priemonių diegimo reikalavimus ir saugumo valdymą. Metodikos saugumo valdymo pricipai glaudžiai siejasi su ISO 27000 standartų grupe, todėl plačiau disertacijoje nebus nagrinėjami.

Pažymėtina, kad informacinių technologijų bei informacijos saugumo sprendimų gamintojai šių metodikų pagrindu rengia savo specializuotas metodikas, pavyzdžiui, MicroSoft, Cisco, Symantec ir kitas.

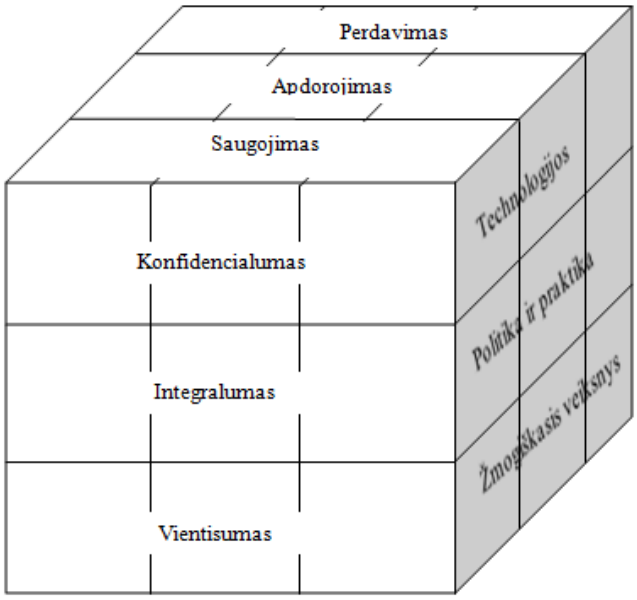
1.2.3. Informacijos saugumo valdymo modeliai

Informacijos saugumo valdymo tyrėjai, atskirų veiklos šakų asocijuotos struktūros ar net įvairių saugumo produktų gamintojai sukūrė ne vieną informacijos saugumo valdymo modelį, kurie neįvardydami konkrečių priemonių ar įgyvendinimo gairių, suformulavo apibendrintus informacijos saugumo valdymo principus.

McCumber kubas. 1991 metais John McCumber sukūrė informacijos saugumo valdymo modelį, kurį sudaro trimačio kubo ląstelės. Trys kubą sudarančios dimensijos yra šios: informacijos charakteristikos (informacijos

[7] ITIL// http://www.itil-officialsite.com/, (žiūrėta 2011 m. kovo 10 d.)

saugumo tikslai) – konfidencialumas, vientisumas, prieinamumas; informacijos būsena – apdorojimas, saugojimas, perdavimas; informacijos apsaugos priemonės – technologinės, politika ir praktika, žmogiškasis veiksnys (McCumber, 2005, 6 paveikslas).



6 pav. McCumber kubas (McCumber, 2005).

Modelio autorius pabrėžia šio modelio universalumą ir atsiribojimą nuo technologinio informacijos saugumo požiūrio. McCumber teigimu, šio modelio unikalumą užtikrina tai, kad informacija gali būti tik trijų būsenų, ir kiekvienu konkrečiu atveju yra arba apdorojama, arba perduodama, arba saugojama. Modelis apima visus tris informacijos saugumo tikslus: vientisumą, konfidencialumą ir prieinamumą bei tai, kad modelyje apibendrintos visos galimos saugumo užtikrinimo priemonės – politinės, technologinės ir žmogiškojo faktoriaus.

Analizuojant šio modelio taikymo privalumus, galima pastebėti, kad informacijos saugumo valdymo problematika gali būti nagrinėjama bet kuriuo aktualiu pjūviu pasitelkiant bet kurią trimačio kubo ašių susikirtimo sudedamąją dalį (ląstelę), pavyzdžiui: pasirenkant informacijos būsenos ašį – perduodama informacija; renkantis informacijos saugumo tikslų ašį – konfidencialumas; informacijos saugumo priemonių ašį – technologijos;

galima nagrinėti perduodamos informacijos konfidencialumo užtikrinimo technologijas arba, pagal analogiją pasirinkus atitinkamas ašis, – saugojamos informacijos integralumo užtikrinimo politines priemones ar kita.

Perimetro apsaugos modelis. Šio modelio objektas – organizacijos vidinis tinklas. Saugumo priemonės taikomos organizacijos vidinio tinklo ir išorinio tinklo susijungimo vietoje siekiant apsaugoti organizacijos perimetrą (Zelstser et al., 2005). Perimetro apsaugai naudojamos įvairios techninės ir programinės priemonės – įsilaužimo aptikimo ir prevencijos sistemos, virtualieji privatūs tinklai, demilitarizuotos zonos ir potinkliai, ugniasienės, specialios maršrutizatorių ir tinklo srautų skirstymo įrangos stebėjimo priemonės ir kita.

Vertinant šiuolaikinių organizacijų veiklos mastus ir pobūdį, tampa sunku griežtai išskirti organizacijos perimetrą, todėl modelio taikymas susiduria su sunkumais apibrėžiant jo taikymo ribas.

Giliosios apsaugos modelis. Kitaip nei perimetro apsaugos modelio, šio modelio tikslas – apginti informacinę sistemą nuo galimų atakų ne tik taikant saugumo priemones informacinės sistemos perimetrui, bet ir visuose gilesniuose informacinės infrastruktūros lygmenyse. Modelio esmė, taikant įvairius saugumo metodus ir priemones, siekti užlaikyti atakas, kol jos bus pastebėtos ir nukenksmintos. Šis modelis apima koordinuotą personalo, technologijų ir operacijų elementų saugumą viso informacinės sistemos gyvavimo ciklo metu (Defence in depth, 2008).

Personalo elementas suprantamas kaip administracinio lygmens problema, kuri sprendžiama suformuojant saugumo politiką ir procedūras, paskirstant pareigas ir atsakomybes, organizuojant nuolatinius personalo mokymus ir kitomis priemonėmis.

Technologijų elementas valdomas remiantis saugumo politika ir procedūromis bei siekiant laikytis pagrindinių principų: gynyba daugelyje vietų, kelių lygių apsauga, patikimos perimetro apsaugos ir įsilaužimų aptikimo priemonės, stiprūs kriptografiniai raktai ir kita.

Operacijų elementu, įgyvendinant saugumo politiką, siekiama suvaldyti kasdienius procesus ir operacijas, reaguoti į incidentus, atakas ir grėsmes, organizuoti auditus ir sertifikavimą.

Personalo, technologijų ir operacijų elementams derinti ir valdyti išskiriamas valdymo elementas, kuris užtikrina koordinuotą visų elementų veikimą.

Vertinant Giliosios apsaugos modelio griežtai struktūruotų gynybinių priemonių akcentuotę, jis gali būti plačiai naudojamas statutinėse organizacijose, pavyzdžiui, karo srityje.

Informacijos srautų saugumo modelis. Šis modelis skirtas į paslaugas orientuotos architektūros bei žiniatinklio paslaugų saugumui užtikrinti. Dažniausiai modelis taikomas konkrečioms paslaugoms, kurias teikiant dalyvauja organizacijos vidaus ir išorės subjektai (McLean). Modelio taikymas leidžia koncentruoti saugumo priemones konkrečioms prioritetinėms sistemoms ar svarbiausioms veikloms, tačiau tai siejasi su organizacijų informacinės infrastruktūros architektūra bei galimybe atskirti konkrečiai paslaugai ar veiklai reikalingas palaikymo paslaugas.

1.2.4. Informacijos saugumo valdymo priemonių analizė

Nagrinėjant informacijos saugumo mokslinius tyrimus galima išskirti platų spektrą išsamių informacijos saugumo valdymo priemonių turinio ar įgyvendinimo metodų lyginamųjų analizių (IT Governance Institute ir Office of Government Commerce, 2008; von Solms, 2005; Abu-Musa, 2009; Tsohou et al., 2010; Susanto, Almunawar ir Tuan, 2011; Gillies, 2011 ir kiti), tačiau aptarus plačiausiai taikomas informacijos saugumo valdymo priemones, tikslinga atlikti jų lyginamąją analizę siekiant išsiaiškinti, kiek jos atitinka disertacijoje suformuotą informacijos saugumo valdymo turinį. Analizei atlikti išskirtas aptartų informacijos saugumo valdymo standartų, metodikų ir modelių identifikuojamas informacijos saugumo objektas, tikslai ir dimensijos. Taip pat išskirtas šių informacijos saugumo valdymo priemonių naudojamas proceso valdymo ciklas. Atsižvelgiant į deklaruojamą priemonių paskirtį ir pilnumą

buvo lygintos šios informacijos saugumo valdymo priemonės – ISO 27000 standartų šeima, COBIT metodika, McCumber kubo modelis ir Giliosios apsaugos modelis. Analizėje plačiau nenagrinėta ITIL metodika (dėl jos aptartų glaudžių sąsajų su ISO 27000 standartų šeima), Perimetro apsaugos ir Informacijos srautų saugumo modeliai (šie modeliai apsiriboja siauresnio pobūdžio konkrečių uždavinių sprendimu). Apibendrinti analizės rezultatai pateikti 2 lentelėje.

Aptariant informacijos saugumo valdymo standartų, metodikų ir modelių turinio lyginamosios analizės rezultatus, galima teigti, kad tirtuose dokumentuose:

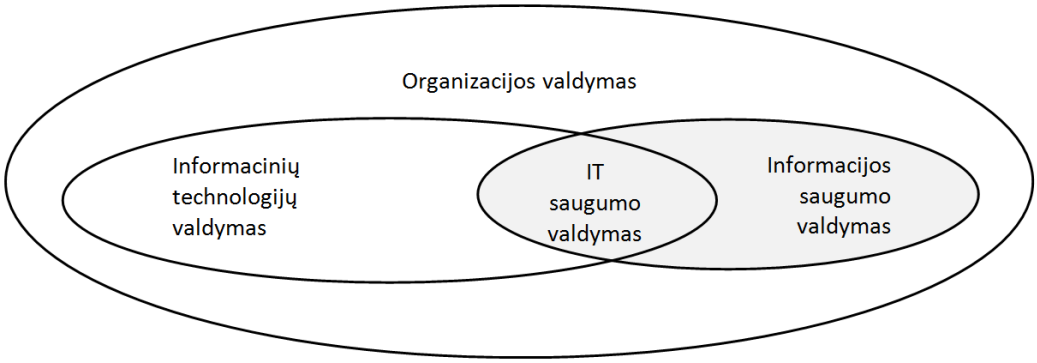
- pagrindiniu saugumo objektu įvardijama informacija (COBIT metodikos atveju pagrindinis valdymo objektas yra informacinės technologijos, kuriomis apdorojama informacija, tačiau aptariant informacijos saugumo užtikrinimą akcentuojama informacijos apsauga; Giliosios apsaugos modelio atveju, analogiškai naudojama informacinių sistemų objekto sąvoka);
- informacijos saugumo valdymo priemonių tikslai – vientisumas, konfidencialumas ir prieinamumas – sutampa;
- informacijos saugumo valdymo dimensijos turi daug bendrumų.

Lyginant analizės rezultatus su disertacijoje aptartu informacijos saugumo valdymo turiniu, galima konstatuoti, kad tirtuose dokumentuose išskirtas objektas ir tikslai visiškai sutampa su informacijos saugumo valdymo turinio objektu ir tikslais. Vertinant saugumo dimensijų kontekstą galima konstatuoti, kad tirtuose dokumentuose didžiausias dėmesys skiriamas techninių priemonių taikymui (informacijos saugumo valdymo turinio technologinės dimensijos sudedamoji dalis) bei organizaciniams ir administraciniams klausimams (informacijos saugumo valdymo turinio strateginės dimensijos sudedamoji dalis), visiškai neminimi – ekonominiai (informacijos saugumo valdymo turinio strateginės dimensijos sudedamoji dalis) ir psichologiniai (informacijos saugumo valdymo turinio žmogiškosios dimensijos sudedamoji dalis) klausimai.

2 lentelė. Apibendrinti informacijos saugumo įgyvendinimo priemonių lyginamosios analizės rezultatai (sudaryta autoriaus).

Informacijos saugumo valdymo priemonė	**ISO 27000**	**COBIT**	**McCumber kubas**	**Giliosios apsaugos modelis**
Saugumo objektas	Informacija	Informacinės technologijos	Informacija	Informacinė sistema
Saugumo tikslai	Konfidencialumas Prieinamumas Vientisumas	Konfidencialumas Prieinamumas Vientisumas	Konfidencialumas Prieinamumas Vientisumas	Konfidencialumas Prieinamumas Vientisumas
Saugumo dimensijos	Saugumo politika; saugumo organizavimas; vertybių klasifikavimas ir kontrolė; personalo saugumas; fizinis ir aplinkos saugumas; komunikacijos ir operacijų valdymas; prieigos kontrolė; sistemų kūrimas ir priežiūra; veiklos tęstinumo valdymas; atitikimas	Saugumo valdymas; saugumo planas; tapatybės valdymas; naudotojo paskyros valdymas; saugumo testavimas, priežiūra ir stebėsena; saugumo incidento apibrėžimas; saugumo technologijų apsauga; kriptografinio rakto valdymas; kenksmingos programinės įrangos prevencija, aptikimas ir koregavimas; tinklo saugumas; keitimasis diskretiškais duomenimis	Technologijos; politika ir praktikos; žmogiškasis faktorius	Technologijų; operacijų; personalo; valdymo
Saugumo valdymo ciklas	Planuoti, daryti, tikrinti, veikti	Planavimas ir organizavimas, įsigijimas ir įdiegimas, paslaugų teikimas ir palaikymas, stebėjimas ir įvertinimas	Įvertinti, kurti, įdiegti, stebėti, valdyti	Valdymo elementas

Nagrinėtos informacijos saugumo valdymo priemonės pabrėžia informacijos saugumo valdymo sistemiškumą ir taikymą visos organizacijos mastu, taigi informacijos saugumo valdymas, suderintas su informacinių technologijų valdymu, turi būti integrali visos organizacijos valdymo dalis (7 paveikslas).

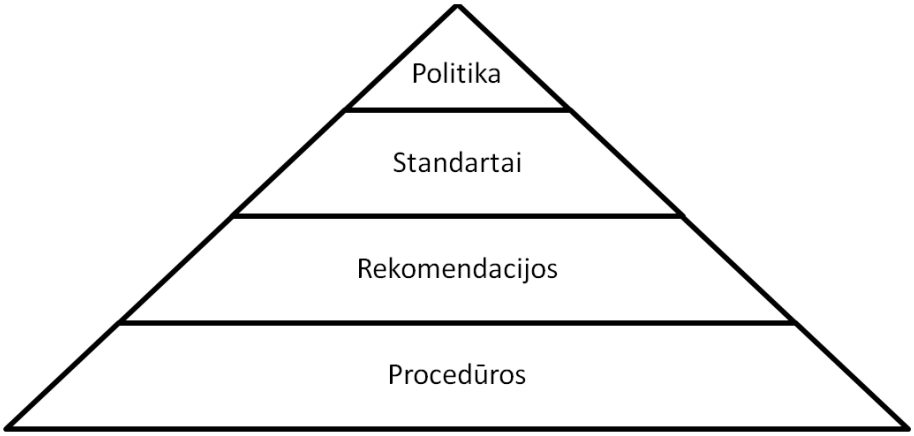


7 pav. Organizacijos, IT ir informacijos saugumo valdymo sąsajos.

Remiantis analizuojamomis informacijos saugumo valdymo priemonėmis, organizacijos (verslo ar valstybinės) siekiančios valdyti informacijos saugumą, informacijos saugumo tikslus, uždavinius ir reikalavimus informacijai tvarkyti turėtų apibrėžti pagrindiniame organizacijos saugumo valdymo dokumente, vadinamame *informacijos saugumo politikos dokumentu*. Kiekviena organizacija, nusprendusi valdyti informacijos saugumą šiomis priemonėmis, visų pirma turi turėti tokį konceptualų dokumentą, patvirtintą aukščiausios organizacijos vadovybės.

Informacijos saugumo politikos dokumento turinys individualus kiekvienai organizacijai, jame aprašoma informacijos saugumo svarba ir tikslai, siekiama informacijos saugumo būklė, bendrieji saugumo principai, įvardijama saugoma informacija ir ištekliai, nustatomi saugumo prioritetai, atsakomybės bei kontrolė. Informacijos saugumo politika įgyvendinama remiantis standartais, procedūromis, rekomendacijomis ir kitais žemesniojo valdymo lygio dokumentais, kurių paskirtis, sąryšiai ir nuorodos į juos taip pat išdėstomi informacijos saugumo politikos dokumente (8 paveikslas). Šie

dokumentai skirti konkrečių paslaugų vartotojams, informacinių technologijų specialistams bei sistemų administratoriams, jų turinys apibrėžia visas organizacijai taikytinas informacijos saugumo valdymo priemones.



8 pav. Informacijos saugumo valdymo dokumentų hierarchija.

Išanalizavus pagrindinių informacijos saugumo valdymo priemonių turinį, galima teigti, kad informacijos saugumo valdymui prielaidas sukuria informacijos saugumo integravimas į visus organizacijos procesus. Šį uždavinį realizuoti organizacijoms padeda strateginis informacijos saugumo valdymo dokumentas – informacijos saugumo politiką ir jos įgyvendinimą užtikrinantys informacijos saugumo dokumentai. Šių priemonių taikymas užtikrina organizacijas dėl strateginio požiūrio, saugumo tikslų ir uždavinių nustatymo, administracinių procedūrų įgyvendinimo ir kontrolės, taikomų informacijos saugumo technologijų patikimumo ir suderinamumo su kitomis organizacijomis, geriausių praktikų laikymosi, tinkamo įsipareigojimų valdymo, personalo kvalifikacijos užtikrinimo, galimybės būti įvertintoms ir sertifikuotoms, atitikties teisiniams reikalavimams bei aplinkai ir nusako, ko galima tikėtis iš organizacijos, įsidiegusios konkretų standartą.

Apibendrinus lyginamosios analizės rezultatus, galima teigti, jog pagrindinių plačiausiai taikomų informacijos saugumo užtikrinimo priemonių turinys, nors ir iki galo neatspindi suformuoto informacijos saugumo valdymo

turinio, turi daug tarpusavio bendrumų, o vystantis naujoms šių priemonių kartoms jų turinys tampa dar labiau panašus.

1.3. Informacijos saugumo valdymas Lietuvos valstybės institucijose

Apjungus pirmuose disertacijos skyriuose ištirtą teorinę medžiagą, suformuluotas siekiamos situacijos – informacijos saugumo valdymo kaip objektyvios saugumo būsenos – turinys. Prielaidas šiai būsenai nuolat palaikyti sudaro išskirtos informacijos saugumo valdymo priemonės – tarptautiniai informacijos saugumo valdymo standartai, metodikos ir modeliai. Nustačius šių priemonių turinio panašumus, galima teigti, kad bet kurios iš identifikuotų plačiausiai taikomų informacijos valdymo priemonių naudojimas galėtų sudaryti prielaidas informacijos saugumui valdyti.

Kaip aptarta disertacijos įvade, informacijos saugumo problemos specifiškumas pasireiškia organizacijų, valstybės bei tarptautiniame lygmenyse, tačiau didžiausia atsakomybė tenka valstybėms, kurios, pasiremdamos suteiktomis galiomis, turi nustatyti priemones informacijos saugumo valdymui savo viduje (t. y. organizacijų lygmenyje) bei gali turėti įtakos kitų šalių vyriausybėms ar tarptautinėms organizacijoms ir taip prisidėti prie tarptautinio lygmens informacijos saugumo užtikrinimo.

Šiame disertacijos skyriuje siekiama patikrinti aptartas informacijos saugumo valdymo įžvalgas ir atlikti žvalgomąjį tyrimą – įvertinti esamą informacijos saugumo valdymo situaciją Lietuvos valstybės institucijose. Lietuvos valstybės institucijų išskirtinumą lemia viešosios teisės pricipai, nusakantys, kad viešajam sektoriui leidžiama (ir privaloma) tik tai, kas nurodyta, t. y. sektorius yra įpareigotas aiškių teisinių rėmų, kurių atskiri sektoriaus subjektai negali peržengti pasirinkdami, kaip valdyti informacijos saugumą organizacijoje. Taigi valstybės institucijų atveju labai svarbu, kad nustatyti reikalavimai būtų tikslūs ir užtikrintų efektyvų ir visapusį

informacijos saugumo valdymą, t. y. atitiktų apibrėžtą informacijos saugumo valdymo turinį.

Siekiant išsiaiškinti esamą situaciją valdant informacijos saugumą Lietuvos valstybės institucijose atlikta: 1) dokumentų turinio analizė – įvertintas teisės aktais patvirtintų informacijos saugumo valdymo reikalavimų valstybės institucijoms turinys, juose ieškota taikymo objekto, nuorodų ir kitų sąsajų su išskirtomis plačiausiai taikomomis informacijos saugumo valdymo priemonėmis, analizuota, ar informacijos saugumo reikalavimai privalomai galioja visoms Lietuvos valstybės institucijoms; 2) dokumentinis atvejo tyrimas Lietuvos Respublikos ministerijose – įvertinti, ar ministerijos įgyvendina informacijos saugumo reikalavimą turėti informacijos saugumo politikos dokumentą.

Šie tyrimai buvo vykdomi 2010–2011 metais remiantis galiojančiais teisės aktais ir Vidaus reikalų ministerijos specialistų sukauptais duomenimis apie Lietuvos Respublikos ministerijas.

Informacijos saugumo valdymo dokumentų turinio analizė

Atliekant dokumentų turinio analizę, naudojantis Lietuvos Respublikos Seimo teisės aktų paieškos įrankiu[8], Vidaus reikalų ministerijos pateikta informacija[9] ir susijusiomis nuorodomis, buvo išskirti teisės aktai, reglamentuojantys informacijos saugumą Lietuvos valstybės institucijose (analizuoti teisės aktai, galiojantys tyrimo laikotarpiu). Vertinant Lietuvoje galiojančių su informacijos saugumo valdymu susijusių teisės aktų turinį, išskirtos svarbiausios teisės aktų nuostatos, nustatančios informacijos saugumo organizavimą Lietuvos viešajame sektoriuje bei numatančios informacijos saugumo įgyvendinimo priemones. Teisės aktuose taip pat buvo ieškoma nuorodų į disertacijos 1.2 skyriuje aptartas ar analogiškas informacijos saugumo įgyvendinimo priemones.

[8] Lietuvos Respublikos Seimas – Dokumentų paieška // http://www3.lrs.lt/dokpaieska/forma_l.htm, (žiūrėta 2010 m. kovo 10 d.)
[9] Lietuvos Respublikos vidaus reikalų ministerija: Teisės aktai // http://www.vrm.lt/index.php?id=1195&lang=ss%3Dl%C4%86%E2%80%9E%C4, (žiūrėta 2010 m. kovo 10 d.)

Svarbiausios teisės aktų nuostatos (priėmimo chronologine tvarka):

Pirmuosius reikalavimus informacijos saugumui Lietuvos Respublikos Vyriausybė patvirtino 1997 metais, siekdama užtikrinti duomenų patikimumą ir apsaugą nuo neteisėto panaudojimo (Bendrieji duomenų apsaugos reikalavimai, 1997), ir įpareigojo duomenų valdytojus, vadovaujantis Lietuvos standartais, atitinkančiais tarptautinius grupės „Informacijos technologija. Saugumo technika“ ISO/IEC standartus, arba kitomis rekomendacijomis, suformuluoti specialius duomenų saugos priemonių reikalavimus ir nustatyti duomenų saugos įgyvendinimo tvarką bei priemones. Pagal *Bendruosius duomenų apsaugos reikalavimus* informacijos saugumo valdymas turi būti išdėstytas duomenų saugos nuostatuose (saugumo politikos dokumente), kuriuos tvirtina informacinės sistemos valdytojas.

2001 metais į informacijos saugumą buvo pažiūrėta plačiau – strateginės valstybės IT saugos raidos kryptys ir priemonės buvo išdėstytos pirmojoje Lietuvos IT saugos valstybinėje strategijoje (Informacijos technologijų saugos..., 2001), kurioje, užtikrinant informacijos saugumą, rekomenduojama vadovautis Informacijos technologijų saugos valstybine strategija bei Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo technika“ grupės standartais.

Nuo 2006 metų valstybės elektroninės informacijos saugumo užtikrinimo tikslus ir uždavinius bei jų įgyvendinimą nustatė antrasis strateginis informacijos saugumo valdymo dokumentas – *Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinė strategija* (Elektroninės informacijos saugos..., 2006). Įgyvendinant šią strategiją, *Bendrieji duomenų apsaugos reikalavimai* buvo iš esmės atnaujinti ir išdėstyti nauja redakcija kaip *Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai* (Bendrieji elektroninės informacijos..., 2007). Šių reikalavimų aktualioje redakcijoje, užtikrinant informacijos saugumą, rekomenduojama vadovautis Lietuvos standartais LST ISO/IEC 17799:2006, LST ISO/IEC 27001:2006, taip pat kitais Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo metodai“

grupės standartais, apibūdinančiais saugų informacinės sistemos duomenų tvarkymą.

Įgyvendinant antrąją saugos strategiją buvo patvirtinti taip pat ir šie aktualūs teisės aktai: 1) informacinių sistemų klasifikavimo gairės, kurios nustatė kriterijus informacinėms sistemoms klasifikuoti nuo pirmos (svarbiausios) iki ketvirtos kategorijų; 2) detalūs elektroninės informacijos saugos reikalavimai, kurie detalizavo reikalavimus konkrečios kategorijos informacinėms sistemoms.

Vertinant reikalavimus valstybės registrams, pastebėta, kad aktuali *Lietuvos Respublikos valstybės registrų įstatymo* redakcija nustato, jog registrų informacijos saugumas taip pat užtikrinamas „*vadovaujantis Vyriausybės patvirtintais bendraisiais duomenų saugos reikalavimais“* (Lietuvos Respublikos valstybės registrų įstatymas, 2009).

2011 metų birželio 29 d. Lietuvos Respublikos Vyriausybė patvirtino naują strateginį dokumentą – *Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programą (Elektroninės informacijos saugos..., 2011).* Šio dokumento tikslas – apimti ne tik viešąjį, bet ir kitus sektorius, tačiau dar nepatvirtinti jokie dokumentui įsigalioti reikalingi teisės aktai, todėl šiuo metu nėra galimybių atlikti detalesnės dokumento analizės ir vertinimo.

Aptariant Lietuvos valstybės institucijoms galiojančius informacijos saugumo reikalavimus, svarbiausiu dokumentu, formuojančiu tokius reikalavimus, įvardintini *Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai*. Lyginant šio dokumento ir plačiausiai taikomų tarptautinių informacijos saugumo valdymo priemonių (ISO 27000, COBIT metodika) turinį, galima konstatuoti, kad tarptautinių informacijos saugumo valdymo priemonių turinys daug platesnis ir detalesnis, tačiau apskritai vertinant visų trijų dokumentų reglamentuojamas temas, galima identifikuoti labai daug panašumų, iš esmės *Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai* tiesiogiai neapima tik saugaus programinės įrangos

kūrimo, kriptografinių priemonių taikymo bei kenksmingos programinės įrangos prevencijos klausimų.

Galiojančių teisės aktų turinys, kuriuo remtasi atliekant analizę, detaliai išdėstytas disertacijos 4 priede, Lietuvos ir tarptautinių informacijos saugumo reikalavimų lyginamoji lentelė pateikta 5 disertacijos priede.

Atlikus Lietuvos valstybės institucijoms galiojančių teisės aktų turinio analizę, galima konstatuoti:

1. Teisės aktais *(Bendraisiais elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimais)* Lietuvos valstybės institucijoms yra įteisintas pagrindinis informacijos saugumo valdymo dokumentas (duomenų saugos nuostatai), kuris savo esme atitinka tarptautiniuose informacijos saugumo valdymo standartuose įvardijamą informacijos saugumo politikos dokumentą.

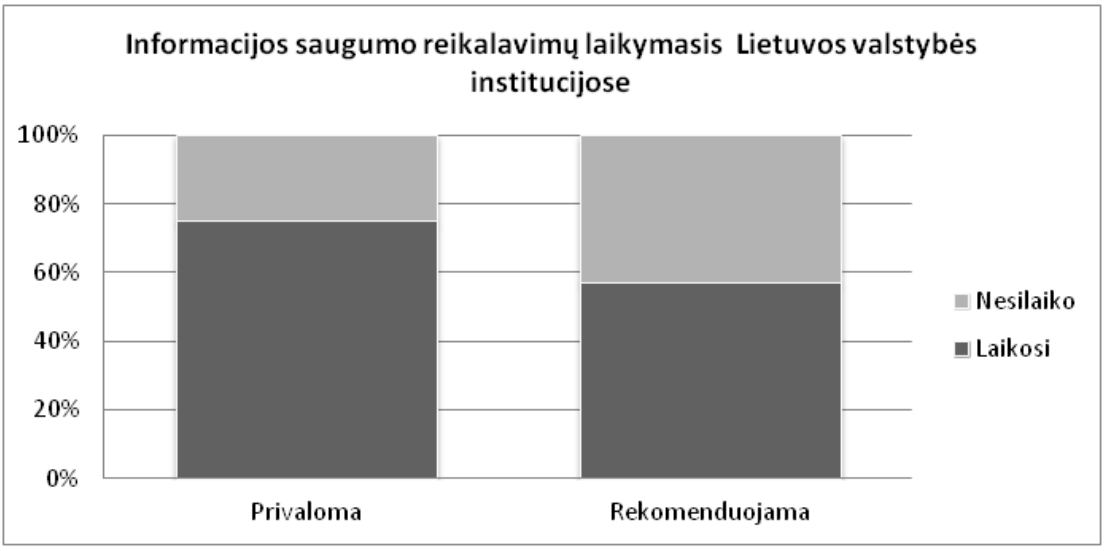
2. Teisės aktais taip pat yra nustatyta informacinių sistemų klasifikavimo pagal svarbumą tvarka, patvirtinti šioms kategorijoms taikomi minimalūs saugumo reikalavimai, kurie siejami su rekomenduojamu tarptautinių ar atitinkamų Lietuvos standartų taikymu, o privalomas Lietuvos standarte LST ISO/IEC 17799:2006 nurodytas technines priemones turi įgyvendinti tik pirmos kategorijos (svarbiausių) valstybės informacinių sistemų valdytojai. Rekomendacinio pobūdžio nuostata dėl standarto taikymo neatliekant konkrečių institucijų dokumentų analizės neleidžia įvertinti, ar (ir kaip) institucijos taiko šį standartą, tačiau konstatuotina, kad pats reikalavimo (rekomendacijos) objektas turėtų būti pakeistas, nes LST ISO/IEC 17799:2006 standartą jau pakeitė ISO 27000 grupės standartai.

3. Visi teisės aktai, reglamentuojantys informacijos saugumo valdymą (išskyrus valstybės registrų atvejį), patvirtinti Lietuvos Respublikos Vyriausybės. Pagal šalies institucinę sąrangą ir valdžios institucijų kompetencijų pasidalinimo principą Vyriausybė be įstatyminio pagrindo neturi galių reguliuoti jai nepavaldžių institucijų veiklos; tai leidžia teigti, kad visi nustatyti informacijos saugumo reikalavimai privalomi tik Lietuvos Respublikos Vyriausybei pavaldžioms institucijoms.

Galima daryti išvadą, kad *Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai* privalomai taikomi tik valstybės registrų valdytojams ir valstybės informacines sistemas valdančioms Lietuvos Respublikos Vyriausybei pavaldžioms institucijoms (ministerijoms, Vyriausybės įstaigoms, departamentams ir pan.), o institucijos, valdančios informacines sistemas, bet nepavaldžios Lietuvos Respublikos Vyriausybei (teismai, prokuratūra, savivalda ir pan.), informacijos saugumo reikalavimus gali taikyti savo nuožiūra arba jų iš viso netaikyti.

Įrodyti, kad ši situacija yra rimta saugumo užtikrinimo problema, galima pasiremiant Valstybės kontrolės išvadomis. Ši institucija turi didžiausią įdirbį vertinant informacijos saugumo valdymo reikalavimus ir jų taikymą Lietuvos valstybės institucijose (Valstybinių auditų, kurių metu buvo vertinamas ir informacijos saugumo valdymas, sąrašas pateiktas disertacijos 1 priede). Valstybės kontrolė dar 2007 metais valstybinių institucijų informacinių sistemų valdymo audito ataskaitoje konstatavo, kad 25 procentai valstybės institucijų nesilaikė privalomų informacijos saugumo reikalavimų, o vertinant institucijas, kurioms šie reikalavimai yra tik rekomendacinio pobūdžio, konstatuota, kad jų nesilaikė daugiau nei 40 procentų valstybės institucijų (Aleliūnas, Kindurytė ir Kiškina, 2007; 9 paveikslas).

4. Lietuvos valstybės institucijose informacijos saugumo valdymo reikalavimų taikymo objektu teisės aktais įtvirtinta informacinės sistemos ir registrai, todėl duomenų saugos nuostatus (informacijos saugumo politikos dokumentą) privalo parengti ir patvirtinti visi informacinių sistemų ir registrų valdytojai. Ši situacija kelia sunkumų institucijoms, kurios valdo daugiau nei vieną valstybės informacinę sistemą ar registrą, o institucijos, kurios nevaldo nė vienos formalizuotos informacinės sistemos ar registro, pasilieka už informacijos saugumo valdymo reikalavimų taikymo ribų. Šios informacijos saugumo valdymo problemos (spragos) analizei atliktas dokumentinis atvejo tyrimas.



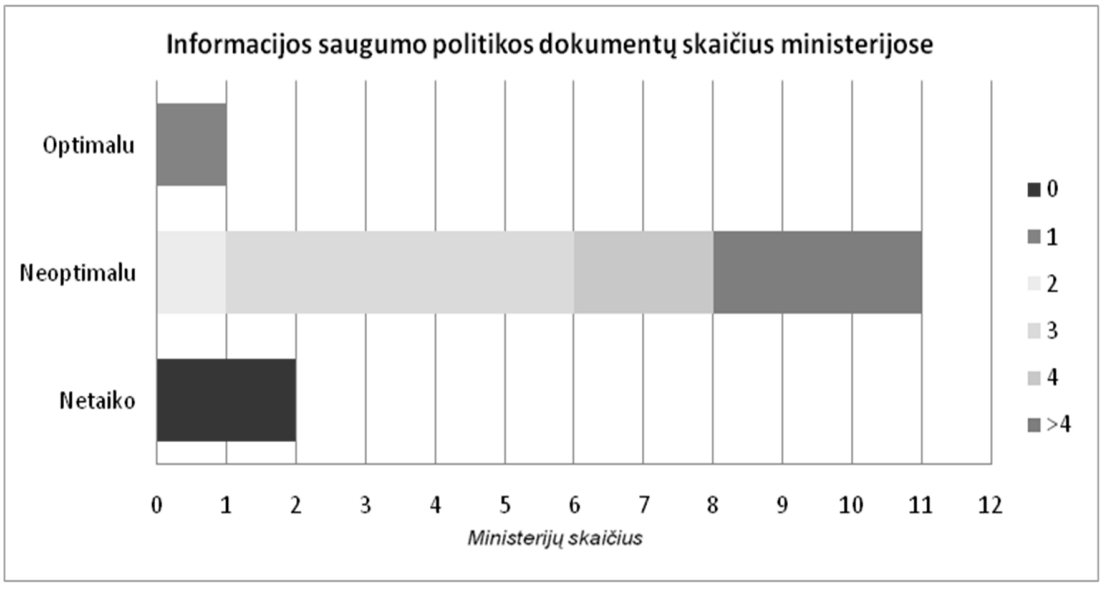
9 pav. Reikalavimų laikymasis Lietuvos valstybės institucijose (pagal Aleliūnas, Kindurytė ir Kiškina, 2007)

Informacijos saugumo valdymo dokumentinis atvejo tyrimas

Siekiant patikrinti ar informacijos saugumo valdymo dokumentų turinio analizės 4 išvada, kad „*Lietuvos valstybės institucijose informacijos saugumo valdymo reikalavimų taikymo objektu teisės aktais įtvirtinta informacinės sistemos ir registrai, todėl duomenų saugos nuostatus (informacijos saugumo politikos dokumentą) privalo parengti ir patvirtinti visi informacinių sistemų ir registrų valdytojai. Ši situacija kelia sunkumų institucijoms, kurios valdo daugiau nei vieną valstybės informacinę sistemą ar registrą, o institucijos, kurios nevaldo nė vienos formalizuotos informacinės sistemos ar registro, pasilieka už informacijos saugumo valdymo reikalavimų taikymo ribų“* pagrįsta, atliktas dokumentinis atvejo tyrimas Lietuvos Respublikos ministerijose.

Atvejo tyrimui atlikta Lietuvos Respublikos vidaus reikalų ministerijos specialistų sukauptų valstybės institucijų, kurios pagal nustatytus *Bendruosius elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimus* teikia ministerijai derinti saugos dokumentus, duomenų analizė. Buvo tiriama, kiek ir kokių galiojančių saugos dokumentų yra parengusios, suderinusios su Lietuvos Respublikos vidaus reikalų ministerija ir

pasitvirtinusios Lietuvos Respublikos ministerijos. Analizuojant Lietuvos Respublikos vidaus reikalų ministerijos sukauptuose derinimo sąrašuose esančius įrašus apie 14 Lietuvos Respublikos ministerijų, galima rasti net 45 galiojančius duomenų saugos nuostatus (saugumo politikos dokumentus). Šios analizės rezultatai pateikti 10 paveiksle. Pastebėtina, kad tik viena ministerija turi vienus, visas jos valdomas informacijos sistemas apimančius duomenų saugos nuostatus (viršutinis 10 paveiksle pateiktos diagramos stulpelis), vienuolika ministerijų turi 2 ir daugiau duomenų saugos nuostatų, kai kurios iš jų turi net po 4 ir daugiau patvirtintų saugos politikos dokumentų atskirai kiekvienai valdomai informacinei sistemai (vidurinis 10 paveiksle pateiktos diagramos stulpelis). Taip pat šiame sąraše galima rasti dvi ministerijas, kurios neturi patvirtinto jokio saugos politikos dokumento (apatinis 10 paveiksle pateiktos diagramos stulpelis) ir nevaldo jokios teisės aktų nustatyta tvarka įteisintos informacinės sistemos.



10 pav. Informacijos saugumo politikos dokumentų skaičius ministerijose

Pasiremiant prielaida, kad optimaliai organizacijoje turėtų būti vienas aukščiausio lygmens informacijos saugumo valdymo strateginis dokumentas, kuris vienareikšmiškai nustatytų organizacijos informacijos saugumo valdymo

tikslus ir uždavinius, galima daryti išvadą, kad strateginės informacijos saugumo valdymo dimensijos įgyvendinimo požiūriu (politikos dokumentų įvertinimu), tik vienoje ministerijoje iš keturiolikos yra optimali informacijos saugumo valdymo situacija, vienuolikoje neoptimali, o 2 ministerijos iš viso netaiko informacijos saugumo valdymo reikalavimų vykdydamos savo veiklą.

Apibendrintos dokumentų turinio analizės ir dokumentinio atvejo tyrimo išvados

Apibendrinant dokumentų turinio analizės ir dokumentinio atvejo tyrimo rezultatus, galima teigti, kad Lietuvos valstybės institucijoms teisės aktais yra nustatyti informacijos saugumo valdymo reikalavimai, kurie iš dalies remiasi informacijos saugumo įgyvendinimo priemonėmis, tačiau šie reikalavimai neapima visų Lietuvos valstybės institucijų. Informacijos saugumo įgyvendinimo kontekste galima išskirti tris pagrindines informacijos saugumo valdymo problemas: *pirma* – galiojantys informacijos saugumo reikalavimai iš esmės tik rekomenduoja valstybės institucijoms taikyti tarptautinius informacijos saugumo valdymo standartus, todėl, norint nustatyti, ar valstybės institucijos įgyvendina informacijos saugumo valdymo priemonių turinį, reikia atlikti papildomą detalią lyginamąją analizę ir palyginti teisės aktais įtvirtintų galiojančių informacijos saugumo valdymo reikalavimų Lietuvos valstybės institucijoms, tarptautinių informacijos saugumo valdymo priemonių ir pačių institucijų patvirtintų vidinių informacijose saugumo valdymo dokumentų turinį; *antra* – Lietuvos Respublikos Vyriausybė be įstatyminio pagrindo neturi galių reglamentuoti jai nepavaldžių institucijų veiklos, todėl tokioms viešojo sektoriaus institucijoms informacijos saugumo valdymo reikalavimų taikymas nustatytas tik kaip rekomendacija; *trečia* problema susidaro dėl informacijos saugumo valdymo reikalavimų taikymo informaciniams ištekliams (sistemoms ir registrams), o ne pačiai organizacijai (organizacijos informacijai), todėl formaliai informacinių sistemų nevaldančios institucijos informacijos saugumo reikalavimų netaiko, o valdančios kelias

sistemas turi papildomų sunkumų derindamos kelis aukščiausio lygio informacijos saugumo politikos dokumentus.

Atlikus žvalgomąjį tyrimą Lietuvos valstybės institucijoms galiojančių teisės aktais įtvirtintų informacijos saugumo valdymo reikalavimų turinio analizę bei įvertinus šių reikalavimų taikymo Lietuvos Respublikos ministerijose situaciją, galima teigti, kad Lietuvos valstybės institucijose informacijos saugumas negali būti pavadintas valdomu, t. y. Lietuvos valstybės institucijose nėra užtikrinama objektyvaus saugumo būsena. Siekiant suformuoti pasiūlymus, kaip užtikrinti efektyvų informacijos saugumo valdymą Lietuvos valstybės institucijose, tikslinga suformuoti detalią vertinimo prieigą ir atlikti gilesnius bei detalesnius tyrimus.

1.4. Pirmos darbo dalies apibendrinimas ir tolesnių tyrimų kryptys

Pirmoje disertacijos dalyje, išnagrinėjus Lietuvos ir užsienio tyrėjų teorinius konceptus, buvo susistemintos informacijos saugumo sąvokos, aptarta informacijos saugumo samprata ir jos genezė. Konstatuota informacijos saugumo valdymo turinio kaita nuo siauro techninio požiūrio iki plataus informacijos saugumo valdymo poreikio suvokimo, išryškintas informacijos saugumo objektas – informacija, išskirti informacijose saugumo tikslai – konfidencialumas, vientisumas ir prieinamumas. Išanalizavus informacijos saugumo mokslinių tyrimų aprėptis, aktualūs informacijos saugumo aspektai sugrupuoti į strateginę, žmogiškąją ir technologinę dimensijas. Apjungus informacijos saugumo valdymo objektą, tikslus ir dimensijas, apibrėžtas informacijos saugumo valdymo turinys.

Remiantis plačiausiai taikomų tarptautinių informacijos saugumo valdymo priemonių (standartų, metodikų ir modelių) lyginamąja analize, konstatuota, kad visos nagrinėtos priemonės informacijos saugumo objektu taip pat įvardija informaciją, sutampa ir jų deklaruojami informacijos saugumo valdymo tikslai. Dimensijų lygmenyje šios priemonės taip pat turi daug

bendrumų, tačiau iki galo neatspindi suformuoto informacijos saugumo valdymo turinio.

Disertacijos pirmoje dalyje taip pat aprašytas 2010–2011 m. atliktas žvalgomasis tyrimas – Lietuvos valstybės institucijoms galiojančių informacijos saugumo reikalavimų turinio analizė ir dokumentinis atvejo tyrimas. Šio žvalgomojo tyrimo rezultatai leidžia teigti, kad Lietuvos valstybės institucijose neužtikrinamas informacijos saugumo valdymas. Pagrindinės to priežastys: 1) galiojantys informacijos saugumo valdymo reikalavimai remiasi tik rekomenduojamu informacijos saugumo įgyvendinimo priemonių taikymu; 2) informacijos saugumo valdymo reikalavimai patvirtinti subjekto, kuris neturi įgaliojimų teikti privalomų nurodymų visam Lietuvos viešajam sektoriui; 3) galiojančių informacijos saugumo valdymo reikalavimų objektas – informacinės sistemos – neapima visos organizacijose tvarkomos informacijos. Taigi, siekiant efektyvaus ir visapusiško informacijos saugumo valdymo Lietuvos valstybės institucijose, būtina koreguoti informacijos saugumo valdymo reikalavimus.

Apibendrinant pirmosios disertacijos dalies rezultatus galima daryti šias esmines išvadas ir pagrįsti tolesnių tyrimų poreikį:

1. Informacijos saugumo incidentų augimo mastai iliustruoja sisteminių informacijos saugumo valdymo problemų praktiniame lygmenyje egzistavimą.

2. Mokslinių tyrimų kontekste šalia technologinių sprendinių taikymo problematikos ryškėja aktualūs žmogiškieji, ekonominiai ir kiti aspektai, kyla platesnio vadybinio požiūrio poreikis bei tampa akivaizdu, kad esamos informacijos saugumo valdymo priemonės nebėra pakankamos informacijos saugumui valdyti.

3. Informacijos saugumo valdymo objektu išgryninus informaciją, stiprėja disertacijoje keliama esminė mokslinė prielaida, kad informacijos saugumas turėtų būti nagrinėjamas kaip informacijos vadybos sudedamoji dalis

ir naujų informacijos saugumo valdymo sprendinių reikėtų ieškoti informacijos vadybos moksluose.

4. Žvalgomasis tyrimas parodė, kad Lietuvos valstybės institucijose informacijos saugumas nėra tinkamai valdomas, todėl efektyvių ir moksliškai pagrįstų informacijos saugumo valdymo sprendimų paieška aktuali ir Lietuvos kontekste.

II DALIS. INTEGRALUS INFORMACIJOS SAUGUMO VALDYMO MODELIS

Disertacijos pirmoje dalyje išnagrinėjus teorines mokslininkų įžvalgas ryškėja, kad informacijos saugumo mokslinių tyrimų laukas nuolat plečiasi. Ilgą laiką vyravę techniniai informacijos saugumo klausimai tebėra aktualūs, tačiau pastebima ryški informacijos saugumo mokslinių tyrimų problematikos slinktis platesnio, apimančio vis daugiau aspektų, vadybinio požiūrio link. Atlikta šiuo metu plačiausiai taikomų informacijos saugumo valdymo priemonių (metodikų, standartų, modelių) lyginamoji analizė leidžia konstatuoti augančią taikomų priemonių turinio asimiliaciją, tačiau stebint nuolat kylančias informacijos saugumo problemas (pavyzdžiui, informacijos saugumo incidentų skaičiaus augimą), ryškėja, kad esamos priemonės nėra pakankamos informacijos saugumui valdyti.

Aptartos tendencijos formuoja mokslinių tyrimų poreikį ieškoti naujų informacijos saugumo valdymo priemonių. Išskirtas informacijos saugumo valdymo objektas (informacija) stiprina mokslinę prielaidą, kad informacijos saugumo valdymas turėtų būti nagrinėjamas kaip sudėtinė informacijos vadybos dalis, o informacijos saugumui valdyti galėtų būti pasitelkiami informacijos vadybos įrankiai.

Šioje disertacijos dalyje, nagrinėjant pagrindinių informacijos vadybos tyrėjų įžvalgas, ieškoma sąsajų su disertacijos pirmoje dalyje suformuluotu informacijos saugumo valdymo turiniu, siekiama identifikuoto saugumo vieta informacijos vadybos mokslų kontekste. Taip pat aktualu išnagrinėti informacijos vadybos įrankių taikymo informacijos saugumo valdymui galimybes, ypač esamų informacijos saugumo valdymo priemonių trūkumų kontekste.

Identifikavus šių diskursų sąsajumą, siekiama suformuoti teorinį integralų informacijos saugumo valdymo modelį, jungiantį informacijos vadybos įrankius ir informacijos saugumo valdymo turinį.

2.1. Saugumas informacijos vadybos moksluose

Siekiant pagrįsti disertacijoje suformuotą esminę mokslinę prielaidą, kad informacijos saugumas turėtų būti tiriamas kaip informacijos vadybos sudėtinė dalis, šiame disertacijos skyriuje siekiama atskleisti saugumo teorinį ištirtumą aprėpiant informacijos vadybos ir kitas gretutines informacines vadybos koncepcijas. Disertacijoje suformuluotų informacijos saugumo valdymo turinio dedamųjų ieškoma informacijos vadybos, informacijos išteklių vadybos, informacijos įrašų, žinių vadybos mokslų tyrėjų įžvalgose.

2.1.1. Saugumas informacijos vadybos kontekste

Informacijos vadybos apibrėžtis ir reikšmę nagrinėjo daug informacijos vadybos teoretikų: T. Davenport, T. Wilson, D. Chaffey, G. White, D. Marchand, E. Orna, Ch. Schlögl, S. Wood, Ch. Choo, Z. Atkočiūnienė, E. Macevičiūtė, A. Augustinaitis, R. Gudauskas, L. Markevičiūtė ir kiti.

Remiantis šių tyrėjų darbais, informacijos vadybos sąvokos raidą galima skirti į tris etapus: 1) šeštojo dešimtmečio antroje pusėje pradėta naudoti informacijos vadybos sąvoka dažniausia buvo taikoma duomenų apdorojimo kontekste; 2) aštuntojo dešimtmečio antroje pusėje sąvoka pradėta glaudžiai sieti su informatika, informacinių sistemų naudojimu; 3) nuo 1990 metų sąvoka vis daugiau įgavo vadybos bruožų, pabrėžiamas dėmesys pažangiems vadybos sprendimams, efektyviam informacijos apdorojimui, naudojant informacines technologijas, atsiranda organizaciniai, kultūriniai, strateginiai aspektai. Šiuo metu informacijos vadyboje skiriamos dvi problematikos nagrinėjimo kryptys – informacijos vadyba, orientuota į informacijos technologijas, ir informacijos vadyba, orientuota į turinį (Atkočiūnienė, 2009a; Vodacek 1998; Schlögl, 2005).

Išanalizavus informacijos vadybos tyrėjų formuluojamas informacijos vadybos sąvokas, tyrimų objektą bei tikslus, informacijos saugumas, kaip informacijos vadybos dedamoji, pradeda ryškėti apibrėžiant informacijos vadybos tyrimo objektą, t. y. informacijos vadyba nagrinėja informacijos

vertės, kokybės, nuosavybės, naudojimo aktualumo, prieinamumo, legalumo ir *saugumo* problematiką organizacijos kontekste (Wilson, 1997; Macevičiūtė ir Wilson, 2002; Chaffey ir White, 2011).

Informacijos vadybos srityje pabrėžiama informacijos kokybės svarba, kokybės vertinimo kategorijose taip pat galima rasti informacijos saugumo dedamąją. Informacijos kokybei vertinti išskiriami požymiai skirstomi į keturias kategorijas: *esminė kokybės kategorija,* susijusi su tikslumu, objektyvumu, patikimumu ir reputacija; *prieinamumo kokybės kategorija*, apimanti prieinamumo ir saugumo požymius; *kompleksinė kokybės kategorija*, jungianti relevantumą, pridėtinę vertę, savalaikiškumą ir išsamumą; *reprezentatyvumo kokybės kategorija,* pabrėžianti interpretavimo, nuoseklumo, suprantamumo ir glaustumo požymius (Wang ir Strong, 1996). Taigi vertinant saugumą informacijos kokybės kontekste, jis išskiriamas kaip prieinamumo kokybės kategorijos sudedamoji dalis.

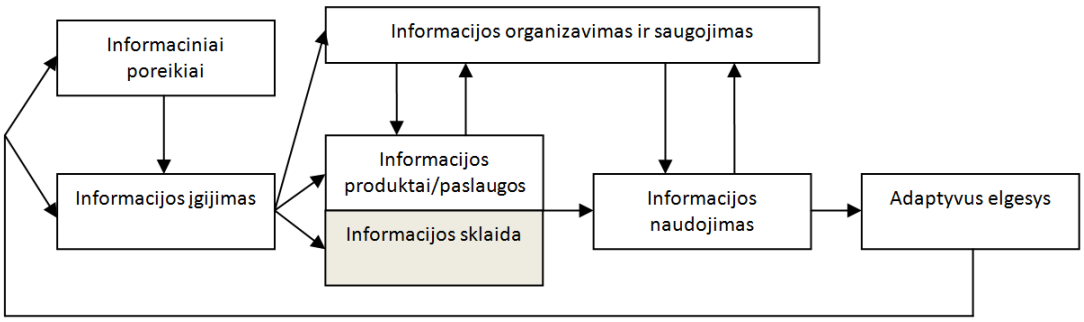
Informacijos saugumas taip pat išskiriamas kaip viena iš informacinės veiklos profesinių kompetencijų šalia tokių svarbių informacinės veiklos kompetencijų kaip organizacijos vadybos kompetencija, informacijos vadybos kompetencija, informacinių paslaugų vadybos kompetencija ar informacinių technologijų taikymo kompetencija (Abels et al, 2003).

Vertinant informacijos saugumą per rizikų mažinimo prizmę, saugumas atsispindi strateginiame požiūryje į informacijos vadybos svarbą – strateginis požiūris į informacijos vadybą organizacijoms leidžia sumažinti išlaidas, rizikų neapibrėžtumą, sukurti pridėtinę vertę esamiems produktams ar paslaugoms bei kurti naujus, informacija grįstus produktus ir paslaugas (Choo, 2008; Debowski, 2006). Sėkmingai informacijos vadybai visą informacijos gyvavimo ciklą prielaidas leidžia sukurti organizacijos informacijos vadybos programa, kurios sudėtinė dalis turėtų būti ir informacijos saugumas (Detlor, 2010).

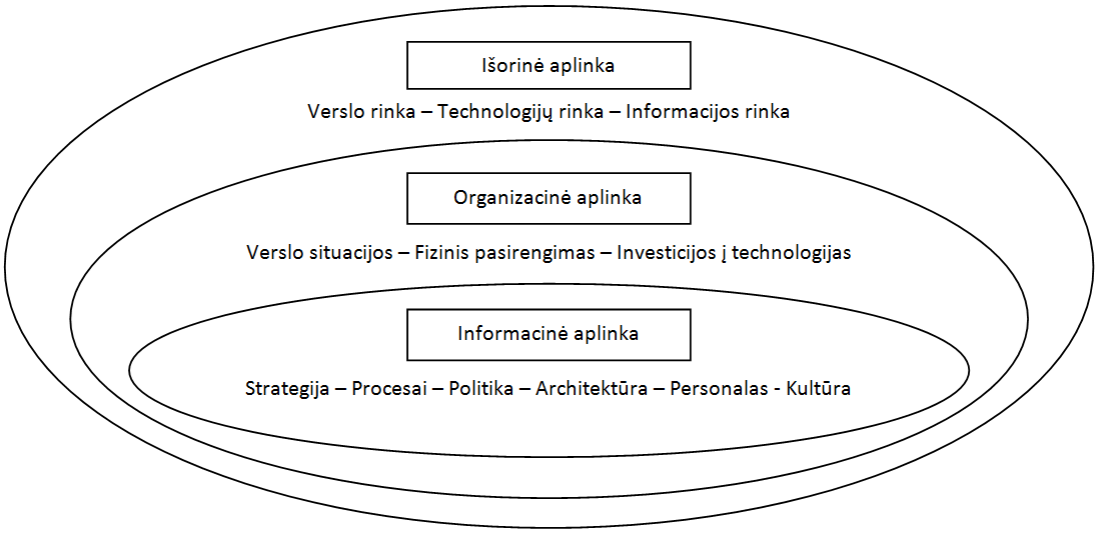
Informacijos saugumo dedamųjų galima aptikti ir analizuojant informacijos vadybos modelius. Pagrindiniais informacijos vadybos modeliais išskirtini – Ch. Choo (2002) sudarytas informacijos vadybos procesinis modelis (11 paveikslas) ir T. Davenport ir L. Prusak (1997) ekologinis

informacijos vadybos modelis (12 paveikslas). Šių modelių kūrėjai tiesiogiai nepažymi informacijos saugumo kaip informacijos vadybos proceso ar dedamosios, tačiau gretinant Ch. Choo modelio aprašo teorinį konceptą su T. D. Wilson išsakytu požiūriu, galima išskirti informacijos vadybos procesinio modelio informacijos sklaidos procesą (pilka spalva pažymėta 11 paveiksle). Šio proceso turinio apibrėžčiai Ch. Choo ir T. D. Wilson ryškina informacijos pristatymo reikiamam asmeniui, reikiama forma, reikiamu laiku svarbą; tai suponuoja būtinybę nustatyti tinkamus informacijos saugumo lygius konkrečiai informacijai bei užtikrinti atitinkamų prieigos teisių nustatymą ir valdymą (Choo 2002; Wilson 1997). Ši įžvalga siejasi ir su jau minėta informacijos kokybės prieinamumo kategorija, kurioje R. Wang ir D. Strong (1996) taip pat išskyrė saugumo dedamąją. Iš esmės prieigos valdymas priskiriamas prie pagrindinių informacijos saugumo užtikrinimo priemonių, o informacijos saugumo tikslų (konfidencialumo, vientisumo ir prieinamumo) kontekste prieigos valdymas aktualiausias užtikrinant informacijos konfidencialumą, taip pat iš dalies ir vientisumą. Konfidencialumas itin svarbus, kad tik sankcionuoti (turintys leidimus) vartotojai galėtų prieiti prie informacijos. Vientisumas svarbus tiek, kiek tai susiję su informacijos vartotojų teisių (pvz., informacijos skaitymas, informacijos įrašymas, informacijos naikinimas) valdymu, t. y. apribojus prieigos teises, galima sumažinti riziką, kad tyčiniu ar netyčiniu būdu bus pakeista ar sunaikinta informacija ir taip paveikti informacijos vientisumo išsaugojimą.

Apibendrinant saugumo paieškas informacijos vadybos teorinėse įžvalgose, galima teigti, kad nors ir fragmentiškai, tačiau saugumas tyrinėjamas kaip sudėtinė informacijos vadybos dalis. Kai kurie informacijos vadybos teoretikai saugumą tiesiogiai įvardija kaip vieną iš informacijos vadybos tyrimo objektų; saugumas nagrinėjamas kaip sudėtinė informacijos kokybės, informacinės veiklos kompetencijos sudedamųjų dalių; labiausiai saugumas išryškinamas informacijos sklaidos procesuose tyrinėjant prieigos valdymo priemonių naudojimą.

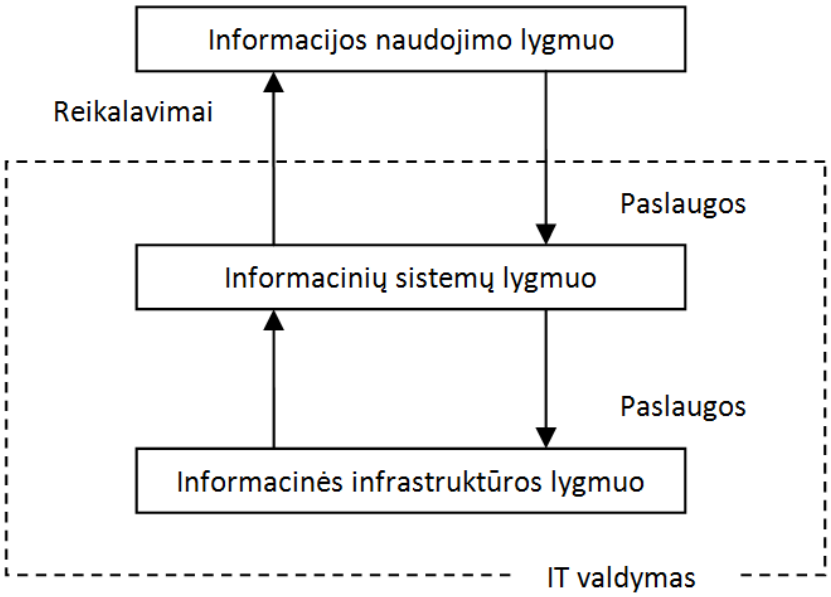


11 pav. Informacijos vadybos procesinis modelis (Choo, 2002).



12 pav. Informacijos vadybos ekologinis modelis (Davenport ir Prusak, 1997).

Vertinant mokslines diskusijas apie informacijos vadybos turinį, tikslinga išplėsti informacijos saugumo dedamosios paieškas į gimininga informacines vadybos koncepcijas – įrašų vadybą, informacinių išteklių vadybą, informacinių technologijų vadybą, duomenų vadybą, informacijos sistemų vadybą ir kt. Šiai tyrimo plėtotei vertinga pasiremti M. Wollnik sudarytu trijų lygių modeliu, susisteminusiu požiūrius į informacijos vadybą (13 paveikslas), kuriame išskiriamas aukščiausias – informacijos vadybos lygmuo, vidurinysis – informacinių sistemų valdymo lygmuo ir žemiausias – informacinės infrastruktūros valdymo lygmuo, sudarantis technologinį pagrindą (platformą), reikalingą aukštesniems lygmenims (Wollnik, 1988).



13 pav. Trijų lygių informacijos vadybos modelis (Wollnik, 1988).

Identifikavus saugumo ir informacijos vadybos tarpusavio ryšį bei išryškinus informacijos saugumo tyrimų tendencijas (kaip aptarta disertacijos 1 dalyje, didžiausias techninių informacijos saugumo aspektų ištirtumas), tikėtina žemesniuose (labiau techniniuose) informacijos vadybos lygiuose rasti dar glaudesnes saugumo ir informacijos vadybos sąsajas.

2.1.2. Saugumas informacijos išteklių vadybos kontekste

Informacijos išteklių vadybos apibrėžtis nagrinėjo ir modelius sukūrė C. Burk, D. Marchand, F. Horton, N. Willard, D. Skyrme, J. Hoven, Z. Atkočiūnienė, L. Markevičiūtė ir kiti.

Kaip teigia Z. Atkočiūnienė, tikslios ir vienareikšmiškos informacijos išteklių apibrėžties nėra, o išskiriant kokybinius informacijos apdorojimo lygmenis „duomenys–informacija–žinios“, išteklius kaip informacija gali būti bet kuriuo iš lygmenų (Atkočiūnienė, 2009a). D. Marchand ir F. Horton požiūriu, galima išskirti informacijos išteklių vadybos sąvokos genezę nuo popierinių laikmenų optimizavimo iki informacijos ir šiuolaikinių technologijų valdymo strategijų siekiant įgyvendinti organizacijos tikslus, taigi iš esmės

informacijos išteklių vadyba remiasi informacijos vadyba (Marchand ir Horton, 1986).

Analizuojant saugumo vietą informacijos išteklių vadybos srityje, tikslinga ištirti pagrindinius informacijos išteklių vadybos modelius, taip pat, atsižvelgiant į disertacijos kontekstą (temą), analizei pasitelkti ir Lietuvos tyrėjų suformuotą bendrąjį informacijos išteklių vadybos modelį.

Vieną pirmųjų nuoseklių informacijos išteklių vadybos modelių sukūrė C. Burk ir F. Horton. Šie autoriai aprašė keturis informacijos išteklių valdymo etapus (išteklių identifikavimą, išteklių paskirstymą, išteklių vertės nustatymą, išteklių žemėlapio sudarymą (Burk ir Horton, 1988), tačiau nė vieno etapo aprašyme saugumo dedamosios neišskyrė.

N. Willard informacijos išteklių valdymo modelyje išskyrė penkis pagrindinius elementus: identifikavimas ir aprašymas, nuosavybės ir atsakomybės nustatymas, vertės ir naudos nustatymas, vystymas ir didesnės pridėtinės vertės kūrimas, naudojimas organizacijos veikloje. Vėliau prie šių elementų buvo pridėtas rizikos elementas, kuris apima rizikas, kylančias organizacijai praradus, sunaikinus ar trečioms šalims nesankcionuotai pasinaudojus organizacijos informaciniais ištekliais (Willard, 1993, 2003). Paskutinysis, rizikos elementas, gali būti siejamas su saugumu ir yra aktualiausias informacijos saugumo kontekste.

Siekiant efektyviai valdyti informacijos išteklius, platų spektrą principų suformulavo D. Skyrme. Šio informacijos vadybos teoretiko teigimu, svarbiausia – suvokti informacijos reikšmę organizacijos veiklai; aiškiai paskirstyti atsakomybes už informacijos išteklių vadybos veiklas; sukurti aiškią informacijos išteklių valdymo politiką, apimančią nuosavybės, informacijos vientisumo ir sklaidos aspektus; identifikuoti (audituoti) turimus informacijos ir žinių išteklius, vertinti jų naudingumą, vertę ir sąnaudas; užtikrinti sąsajas su vadybos procesais; nuolat vykdyti organizacijos išorės ir vidaus veiklos stebėseną, vertinti išteklius, kurie yra svarbūs organizacijos veiklai; pasirinkti tinkamas programines ir technines priemones, vidaus ir išorės informacijai sisteminti ir naudoti; skaičiuoti ir optimizuoti lėšas, skiriamas informacijos

ištekliams įsigyti; integruoti informacijos rinkimo ir analizės procesus aktualiai informacijai apdoroti; vystyti modernias technologines sistemas; išnaudoti technologijų konvergenciją; skatinti palankios informacijai dalintis kultūros kūrimąsi (Skyrme, 1999). Saugumo kontekste aktualiausias šio modelio informacijos valdymo politikos principas, apimantis informacijos vientisumo ir sklaidos aspektus.

J. Hoven savo darbuose pabrėžia, kad turi būti glaudus sąryšis tarp organizacijos tikslų ir informacijos išteklių vadybos tikslų, ir tai turėtų būti integruota organizacijos verslo plane. Sėkmingai informacijos išteklių vadybai autorius išskiria šias veiklos sritis: skatinti duomenų svarbos ir jų valdymo atsakomybės supratimą; siekti, kad visoje organizacijoje dalinantis duomenimis būtų naudojama bendra terminologija, apibrėžtys ir identifikatoriai; sukurti bendrą visai organizacijai duomenų architektūrą, aiškiai parodančią ryšius tarp duomenų, esančių įvairiuose organizacijos padaliniuose; užtikrinti duomenų vientisumą; užtikrinti saugumą taikant ekonomiškai efektyvias priemones, apsaugančias išteklius nuo atsitiktinio ar sąmoningo pakeitimo, sunaikinimo ir neteisėtos prieigos; užtikrinti prieinamumą prie aktualių duomenų; skatinti duomenų naudojimą, siekiant pateikti duomenis veiklai patogia forma; kurti ir išlaikyti sąsajas su organizacijos veikla (Hoven, 2001). Šiame modelyje galima įžvelgti ir su saugumu sieti duomenų vientisumą ir duomenų saugumo priemonių taikymą, netiesiogiai dar gali būti priskirta prieinamumo prie aktualių duomenų užtikrinimo sritis. Aktualus ir J. Hoven išryškintas ekonomiškumo aspektas taikant saugumo priemones: kaip buvo aptarta disertacijos antroje dalyje, lyginant informacijos saugumo valdymo priemones su informacijos saugumo valdymo turiniu, ekonominių aspektų plėtotės esamose informacijos saugumo valdymo priemonėse pasigesta.

Z. Atkočiūnienė ir L. Markevičiūtė, apibendrindamos informacijos išteklių teorinius tyrimus, pastebėjo, kad autoriai dažnai nesiekia apibrėžti viso informacijos išteklių komplekso, o akcentuoja ir analizuoja tik tam tikrus informacijos išteklių valdymo aspektus. Autorės, pasiremdamos N. Willard,

D. Skyrme, C. Burk ir F. Horton ir kitų darbais, suformulavo bendrąjį informacijos išteklių vadybos modelį, kuris susideda iš devynių veiklos sričių: rinkimo, formos optimizavimo, apskaitos, atsakomybės, paieškos, sklaidos, apsaugos, audito ir technologijų taikymo (Atkočiūnienė ir Markevičiūtė, 2005). Šiame modelyje aiškiai ir tiesiogiai įvardinamas informacijos išteklių apsaugos aspektas.

Apibendrinant aptartus informacijos išteklių vadybos modelius informacijos saugumo tikslų – prieinamumo, vientisumo ir konfidencialumo kontekste – galima konstatuoti, kad informacijos išteklių saugumui nėra skiriama daug dėmesio (3 lentelė). C. Burk ir F. Horton modelyje informacijos išteklių saugumas neminimas, D. Skyrme savo modelyje tik iš dalies paliečia informacijos vientisumo problematiką, Z. Atkočiūnienės ir L. Markevičiūtės ir papildytame N. Willard modelyje minimi konfidencialumo ir prieinamumo aspektai, galima išskirti J. Hoven informacijos išteklių valdymo modelį, kuris tiesiogiai pamini visus tris informacijos saugumo aspektus – vientisumą, prieinamumą ir konfidencialumą.

3 lentelė. Informacijos išteklių valdymo modelių sąsajos su informacijos saugumo tikslais (sudaryta autoriaus).

Informacijos išteklių vadybos modeliai \ Informacijos saugumo tikslai	Burk ir Horton modelis	Willard modelis	Skyrme modelis	Hoven modelis	Atkočiūnienės ir Markevičiūtės modelis
Prieinamumas	-	+	-	+	+
Vientisumas	-	-	+	+	-
Konfidencialumas	-	+	-	+	+

Vertinant informacijos išteklių vadybą, tikslinga pažymėti įrašų vadybos dedamąją. Nuo įrašų tvarkymo pradžios pasitaikydavo informacijos praradimo bei manipuliavimo duomenimis, tačiau gera organizacijos vadyba turi apimti visos organizacijos informacijos (taip pat ir visų įrašų) tinkamą apsaugą.

Organizacijos turi rūpintis, kad tokia funkcija būtų aiškiai priskirta atsakingiems žmonėms bei užtikrinta tinkama funkcijos vykdymo kontrolė. Organizacijos valdomos informacijos netinkamas atskleidimas gali pažeisti privatumo, konfidencialumo ar kitus teisinius reikalavimus, o informacijos praradimas gali lemti organizacijos sukauptų žinių, intelektinės nuosavybės ar konkurencinio pranašumo praradimą (Willis, 2005; Lomas, 2010).

Įrašų vadybos tikslas yra koordinuoti įrašų valdymą viso jų gyvavimo ciklo metu. Įrašų gyvavimo ciklas apima įrašų kūrimą, sklaidą, naudojimą, saugojimą, prieigą, archyvavimą ir naikinimą. Viso šio ciklo metu įrašai turi atitikti jiems keliamus naudingumo, tinkamumo ir pasiekiamumo reikalavimus (Schlögl, 2005; Markevičiūtė, 2008; Xiaomi, 2003).

Remiantis A. Willis įžvalgomis, galima pažymėti, kad įrašų vadyba yra vienas pagrindinių organizacijų vadybos komponentų, ypač svarbus organizacijos atskaitomybei ir kasdienei veiklai. Pagrįsdamas šiuos teiginius, jis išskyrė šešis įrašų ir informacijos vadybos komponentus, kurie svarbūs sėkmingai organizacijų vadybai, – tinkamas procesas, skaidrumas, atskaitomybė, atitikimas, teisėtumas, saugumas (Willis, 2005).

P. Emery, nagrinėdama įrašų vadybos turinį, pažymėjo, kad įrašų saugumui dažnai naudojamos rolėmis grįstos prieigos teisės, taip pat akcentavo saugų įrašų naikinimą jų gyvavimo ciklo pabaigoje (Emery, 2003).

Apibendrinant saugumo sąsajumą su informacijos išteklių vadyba, pastebėtas platesnis saugumo ryškinimas nei informacijos vadyboje. Beveik visuose pagrindiniuose informacijos išteklių valdymo modeliuose galima pastebėti tiesiogiai integruotus informacijos saugumo tikslus. Nagrinėjant įrašų vadybos tyrėjų įžvalgas sėkmingam įrašų vadybos ciklui, aiškiai galima identifikuoti pasiekiamumo, konfidencialumo, prieigos valdymo ir kitų saugumo priemonių akcentuotę.

2.1.3. Saugumas žinių vadybos kontekste

Žinių vadybos tyrėjai P. Drucker, G. Probst, K. Wiig, I. Nonaka, Y. Malhorta, L. Prusak, T. D. Wilson, Z. Atkočiūnienė, A. Augustinaitis,

R. Gudauskas ir kiti kūrė ir plėtojo žinių vadybos apibrėžtį, žinių valdymo procesų aprašą bei modelius. M. Nordin ir kiti, ieškodami žinių vadybos ištakų, apibendrino L. Prusak, J. M. Pemberton, C. Amistead, K. Wiig, R. L. Baskerville, D. Skyrme, E. Davenport ir kitų atliktus tyrimus ir išskyrė, kad žinių vadyba artimai yra susijusi su ekonomika, sociologija, filosofija, psichologija, bibliotekininkyste, informatika, informacijos mokslais, informacijos ir informacijos išteklių vadyba, kokybės vadyba, pokyčių vadyba, organizacine elgsena, žmogiškųjų išteklių vadyba, procesų inžinerija, organizacijų teorija, besimokančia organizacija ir kitais mokslais bei tyrimų sritimis (Nordin et al., 2009). Pažymėtina, kad mokslinėje diskusijoje žinių vadybos sąvoka tebėra svarstoma, kritinio požiūrio šalininkai teigia, jog žinių vadyba yra tik kitas informacijos vadybos pavadinimas, bandantis įvertinti ir formaliai neišreikštą informaciją (Wilson, 2002).

Žinių vadyba sulaukia daug Lietuvos ir užsienio autorių dėmesio, žinios priskiriamos prie kertinių organizacijos sėkmės išteklių, sėkminga žinių vadyba tampa esminiu konkurenciniu pranašumu, tačiau žinių saugumui dėmesio beveik neskiriama (Salisbury 2003; Randeree, 2006; Atkočiūnienė, 2009b; Gudauskas, 2004).

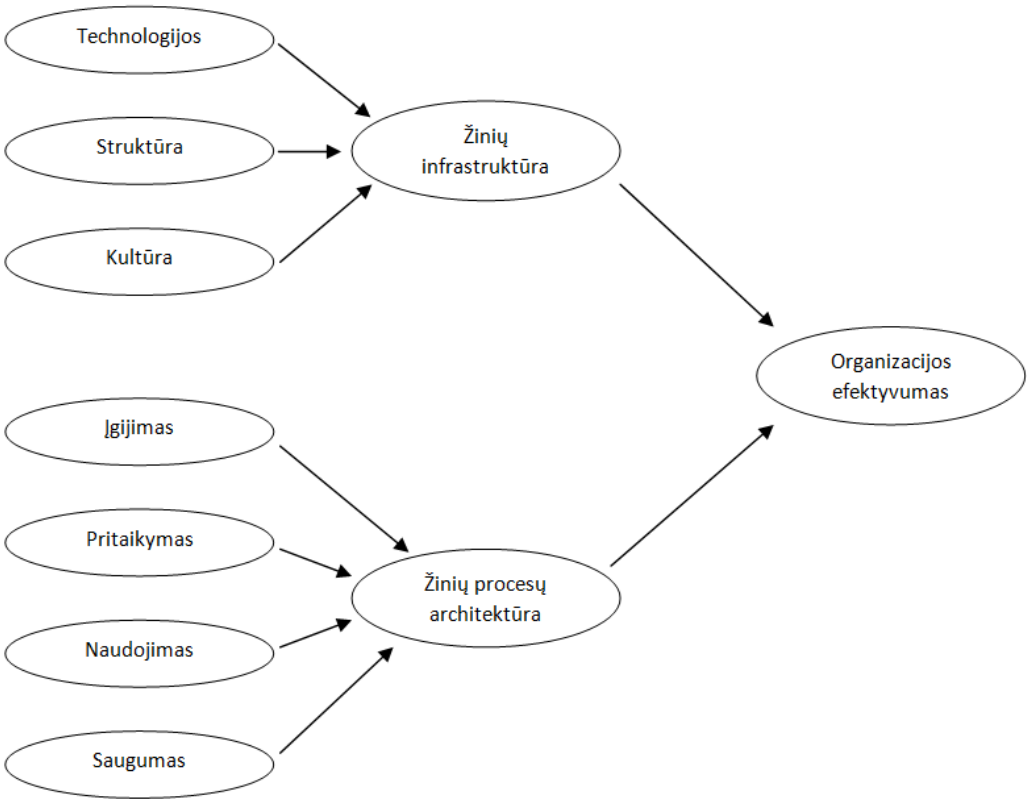
Viename pirmųjų mokslinių straipsnių apie organizacijos žinių saugumą J. Liebeskind nagrinėjo organizacijos strategijos ir žinių sąsajas bei akcentavo, kad organizacijoms būtina rūpintis žinių, kurios užtikrina organizacijos strateginį pranašumą, saugumu. Autorės nuomone, esamos žinių saugumo priemonės – patentus, autorines teises ir komercinių paslapčių apsaugą reglamentuojantys teisės aktai – apima tik labai mažą dalį organizacijos žinių, juos sudėtinga ir brangu įdiegti, taip pat jie turi daug kitų laiko, erdvės bei turinio apribojimų, todėl organizacijos, kurdamos savo veiklos strategijas, turi imtis platesnių priemonių tinkamam organizacijos žinių saugumui užtikrinti (Liebeskind, 1996).

Užuominų apie saugumą taip pat galima rasti ir kituose žinių vadybos moksliniuose tyrimuose. K. Wiig saugumą kaip vieną iš aspektų mini aptardamas žinių vadybą viešojo administravimo srityje. J. Bloodgood ir

D. Salisbury, aptardami sąsajas tarp informacinių technologijų, strateginių pokyčių ir žinių vadybos strategijų, pažymėjo, kad svarbu apsaugoti organizacijos žinias nuo konkurentų, kontroliuoti prieigą prie žinių bei taikyti kitas priemones žinių saugumui užtikrinti (Bloodgood ir Salisbury, 2001); Wiig, 2000).

A. Gold ir kiti išskyrė pagrindines efektyvios žinių vadybos prielaidas ir sudarė žinių vadybos įtakos organizacijos efektyvumui modelį (14 paveikslas). Šių tyrėjų požiūriu, svarbiausios prielaidos – *žinių infrastruktūra,* apimanti organizacijos technologijas, struktūrą bei kultūrą, ir *žinių procesų architektūra,* sujungianti žinių įgijimo, pritaikymo, naudojimo ir saugumo procesus. Šiame modelyje žinių saugumo procesai svarbūs kaip užtikrinantys organizacijos žinių apsaugą nuo neteisėto ar netinkamo naudojimo bei vagystės. Studijoje pastebima, kad žinių saugumui skiriama per mažai dėmesio, ir tai yra sudėtingesnis procesas nei vyraujantis požiūris, kad saugumas yra tik techninės infrastruktūros ar teisės aktais nustatytos nuosavybės teisių apsaugos dalis. Esama situacija kelia grėsmę, kad organizacijos veiklai svarbios žinios gali prarasti savo svarbias kokybines savybes, o tai darytų neigiamą įtaką organizacijos konkurenciniam pranašumui (Gold, Malhotra ir Segars, 2001).

Vėliau šį modelį panaudojo K. Lindsey, M. Jennex ir S. Zyngier ir kiti, taikydami jį žinių vadybos efektyvumui vertinti ir žinių vadybos vertinimo rodikliams sėkmingai nustatyti (Lindsey, 2002; Jennex ir Zyngier, 2007). Jennex ir Zyngier, analizuodami saugumo reikšmę žinių vadybos srityje, pažymėjo, kad dalyje žinių vadybos modelių galima numanyti, jog tyrėjai žinių saugumą laiko sudėtine žinių vadybos sistemų technine dalimi, todėl saugumo neišskiria nagrinėdami žinių vadybos problematiką. Šių autorių atliktas teorinis tyrimas ir atvejų analizė leido konstatuoti, kad žinių saugumas turi būti integrali žinių vadybos dalis, apimanti vadovybės palaikymą, rizikų vertinimą, sistemingą veiksmų planavimą, organizacijos kultūrą ir organizacijoje vykstančius procesus (Jennex ir Zyngier, 2007).



14 pav. Žinių vadybos įtaka organizacijos efektyvumui (Gold et al., 2001).

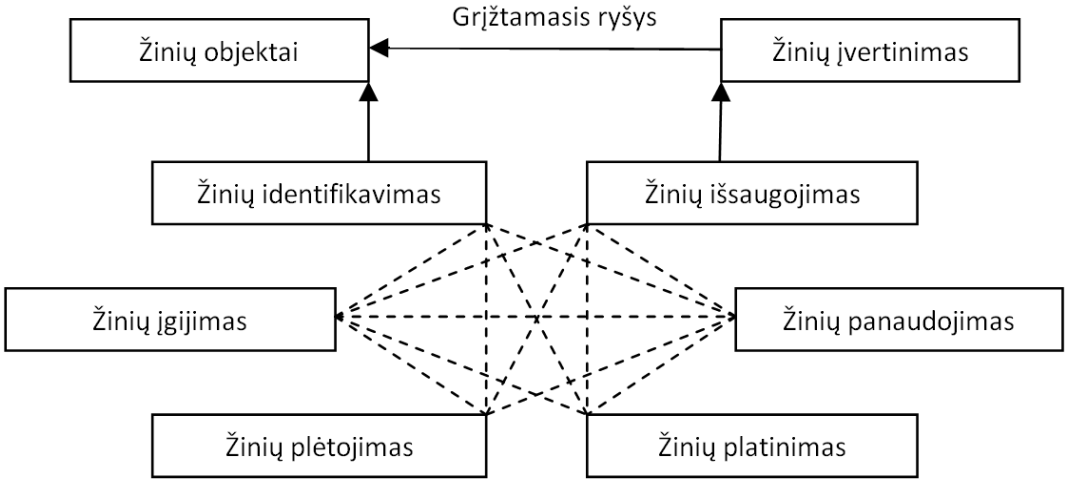
Žinių saugumas taip pat išskiriamas kaip vienas iš dvylikos kritinių žinių vadybos projektų sėkmės faktorių. Tokią išvadą padarė tyrimo autoriai, išstudijavę žinių vadybos efektyvumą ir apibendrinę daugiau kaip 30 studijų, vertinusių per 70 žinių vadybos projektų, rezultatus (Jennex ir Olfman, 2005; Jennex, Smolnik ir Croasdell, 2009).

Saugumo vietą žinių vadybos srityje iliustruoja ir pačių žinių vadybininkų požiūris į jų atsakomybę ir vykdomas funkcijas. A. Aslani ir F. Luthans atliko 307 žinių vadybininkų apklausą ir jos rezultatus palygino su 1980 metų analogiška studija. Ši lyginamoji analizė parodė, kad žinių vadybininkų veikloje sumažėjo rutininio komunikavimo funkcijų ir ypač padaugėjo darbo, sietino su žmogiškųjų išteklių vadyba, tačiau be kontrolės funkcijos nebuvo identifikuota jokia veikla, susijusi su žinių saugumo užtikrinimu. King ir kiti kokybiniu delfi metodu atliko 3 pakopų studiją, į kurią buvo įtraukta daugiau nei 2 tūkst. žinių vadybos praktikų ir vadybininkų. Šie

respondentai saugumą žinių vadybos srityje identifikavo kaip dešimtą pagal svarbą faktorių (Aslani ir Luthans, 2003; King et al., 2002).

G. Probst ir kiti, aptardami žinių proceso valdymo etapus (15 paveikslas), pažymėjo, jog būtina užtikrinti, kad organizacijai reikalingos žinios būtų išsaugotos. Autoriaus teigimu, organizacijos dažnai susiduria su problemomis, kada reikalingos žinios prarandamos, todėl organizacijos, siekdamos efektyviai valdyti žinias, turėtų įdiegti procesus, kurie užtikrintų nuolatinį reikalingų žinių saugojimą (Probst, Raub ir Romhardt, 1999).

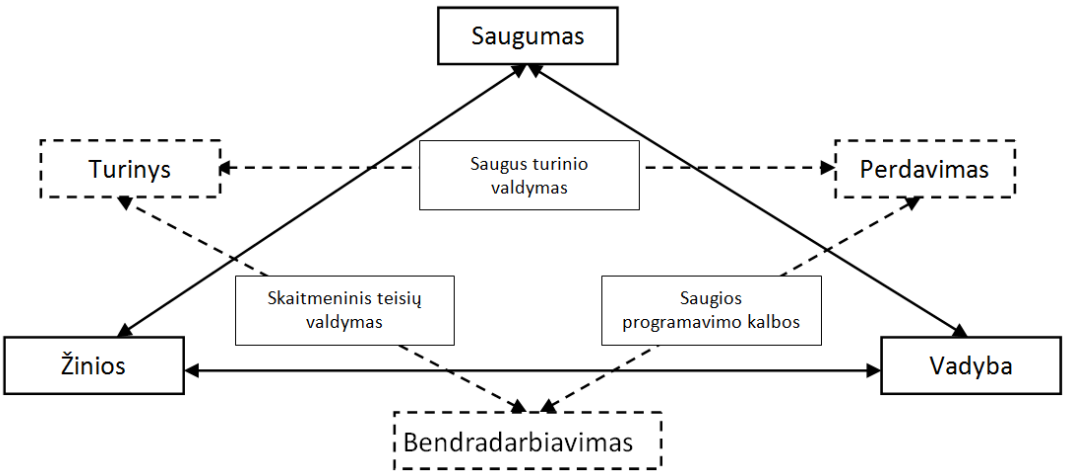
Analizuojant mokslinę literatūrą, nagrinėjančią žinių ir saugumo sąsajas, galima išskirti dvi tyrimų kryptis – žinių saugumą (dar sutinkamas terminas *saugi žinių vadyba*) ir žinių (kompetencijų) apie saugumą vadyba, t. y. kaip žinių vadyba gali padėti efektyviai rinkti, apdoroti, perduoti ir saugoti žinias apie saugumą (Bertino et al., 2006; Probst, Raub ir Romhardt, 1999; Upadhyaya, 2006).



15 pav. Žinių proceso valdymo etapai (Probst, Raub ir Romhardt, 1999).

S. Upadhyaya ir kiti sudarė ir aptarė saugios žinių valdymo sistemos modelį, sujungiantį *žinias*, *vadybą* ir *saugumą* bei žinių valdymo sistemos kritinius komponentus – *turinį*, *perdavimą* ir *bendradarbiavimą*. Kad būtų užtikrintas žinių *turinio*, jo *perdavimo* ir *bendradarbiavimo* saugumas,

remdamiesi sukauptomis žiniomis, tyrimo autoriai išskyrė tris pagrindinius aspektus – *saugias programavimo kalbas*, leidžiančias sukurti saugias žinių perdavimo ir bendradarbiavimo priemones, *skaitmeninį teisių valdymą,* reikalingą saugiai prieigai prie žinių turinio užtikrinti, ir *saugias turinio valdymo* priemones žinių bazei valdyti apjungiant turinio tvarkymą ir jo perdavimą (Upadhyaya et al., 2006, 16 paveikslas).



16 pav. Saugios žinių valdymo sistemos modelis (Upadhyaya, Rao ir Padmanabhan, 2006).

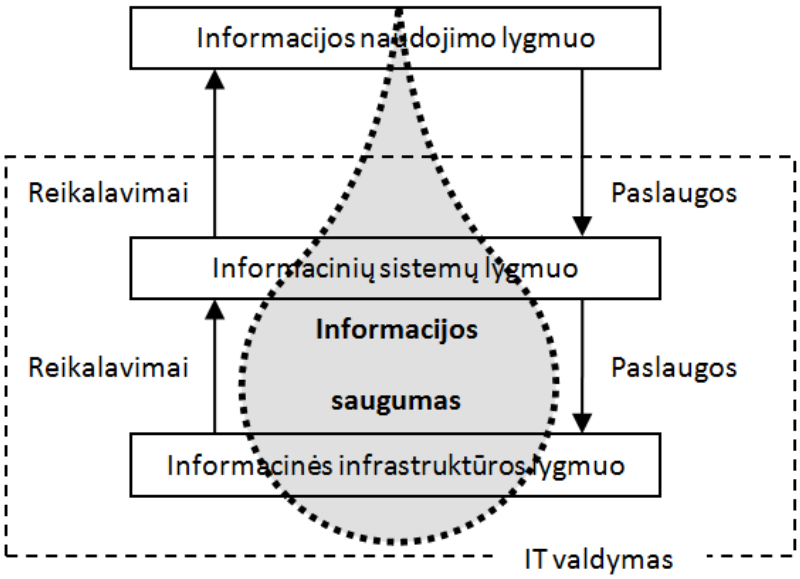
Apibendrinant saugumo vietą žinių vadybos kontekste, visų pirma pažymėtinos tyrėjų įžvalgos, jog žinios kaip konkurencinis pranašumas turi būti tinkamai saugomos, būtina rūpintis tinkama prieigos prie žinių kontrole. Pažymėtina, kad kai kurie žinių tyrėjai saugumą laiko sudėtine (technine) žinių sistemos apsaugos dalimi arba žinių vadybą sieja su žinių apie saugumą tinkamu valdymu.

2.1.4. Saugumas informacijos vadybos mokslų teorinių įžvalgų kontekste

Išanalizavus informacijos vadybos, informacijos išteklių vadybos ir gimininga informacijos vadybos mokslų koncepcijas galima teigti, kad šiuo metu daugiausia dėmesio saugumui skiriama informacijos vadybos

disciplinose ir atitinkamuose moksliniuose tyrimuose, kuriuose ryškinamas technologinis informacijos valdymo aspektas – įrašų vadybos ir informacijos išteklių vadybos srityse. Galima konstatuoti, kad į informacijos įrašų vadybą yra glaudžiai integruoti informacijos saugumo prieinamumo ir konfidencialumo tikslai, o informacijos išteklių vadybos moksliniuose tyrimuose ryškinami visi trys informacijos saugumo tikslai.

Įvertinus aptartas mokslines įžvalgas, galima daryti išvadą, kad saugumas nėra plačiai tirtas informacijos vadybos mokslų kontekste. Išanalizavus informacijos vadybos teoretikų tyrimus, nustatytos saugumo sąsajos su informacijos vadybos tyrimų objektu, informacijos vadybos procesais, naudojimu, informacinėmis technologijomis ir sistemomis bei informacijos vadybos kompetencijomis. Kokybiška informacija taip pat turi atitikti informacijos saugumo valdymo tikslus. 17 paveiksle pavaizduotos informacijos saugumo sąsajos su M. Wollnik (1988) trijų lygių informacijos vadybos modeliu. Šiame paveiksle pateikta schema grafiškai atspindi ištirtas saugumo problematikos lauko slinkties tendencijas nuo technologiškų informacinės infrastruktūros bei informacijos sistemų lygmenų į vadybinį – informacijos naudojimo lygmenį.



17 pav. Informacijos saugumo sąsajos su trijų lygių informacijos vadybos modeliu (sudaryta autoriaus).

Vertinant žinių vadybos ir informacijos saugumo sąsajumą, galima teigti, kad nors saugumas yra įvardijamas kaip viena iš žinių vadybininkų funkcijų bei vienas iš žinių vadybos sėkmės faktorių, žinių vadybos procesuose saugumas daugiausiai suprantamas kaip žinių išsaugojimas arba kaip informacinės (žinių) sistemos kūrimo technologinė dalis, tačiau vis daugiau žinių vadybos teoretikų pažymi, kad žinios yra kritinis organizacijos išteklius, suteikiantis konkurencinių pranašumų, todėl būtina pasirūpinti tinkamu žinių saugumu. Analizuojant ryškėjančią žinių saugumo problematikos svarbą, galima manyti, kad ši tematika ateityje gali tapti svarbia savarankiška saugumo studijų kryptimi, ypač vertinant neišreikštų žinių svarbos augimą bei žinių konversijos būdus kaip pagrindą naujoms žinioms formuoti (Polanyi, 1982; Nonaka ir Takeuchi, 1995), tačiau vertinant mokslines diskusijas dėl pačių informacijos vadybos ir žinių vadybos sąvokų, dėl jų sąsajumo bei, atsižvelgiant į šios disertacijos tikslus, disertacijoje plačiau nenagrinėjamas žinių kaip atskiro nuo informacijos objekto saugumas.

Išanalizavus informacijos vadybos teoretikų tyrimus ir konstatavus nepakankamą jų sąsajumą su informacijos saugumo turiniu, galima išryškinti rimtą spragą moksliniuose tyrimuose. Mokslinėse įžvalgose, akcentuojant informaciją kaip kritinį organizacijų resursą bei esminį konkurencinį pranašumą, menkas informacijos vadybos teoretikų dėmesys šio resurso saugumui užtikrinti tampa aktualia moksline problema, o moksliškai neįtvirtintas informacijos saugumo valdymas lemia problemas, kurios išryškėja ir praktiniame lygmenyje.

2.2. Informacijos vadybos įrankiai ir jų taikymas informacijos saugumo valdymui

Disertacijoje formuluojant esminę mokslinę prielaidą, kad informacijos saugumas turėtų būti sudėtinė informacijos vadybos dalis, informacijos saugumo valdymui turėtų būti pasitelkti ir informacijos vadybos įrankiai. Šioje

disertacijos dalyje siekiama išnagrinėti pagrindinius informacijos vadybos įrankius bei, gretinant jų apibrėžtis su informacijos saugumo valdymo turiniu, teoriniame lygmenyje patikrinti galimybę juos taikyti efektyviam informacijos saugumo valdymui užtikrinti.

2.2.1. Informacijos vadybos įrankiai

Informacijos vadybos įrankius, jų apibrėžtis ir svarbą nagrinėjo D. Chaffey, S. Wood, C. Schlögl, Ch. Choo, D. Skyrme, M. J. Earl, E. Orna, T. H. Davenport, T. D. Wilson ir kiti. Apibendrinant šių informacijos vadybos tyrėjų mokslines įžvalgas, pagrindiniais informacijos vadybos įrankiais įvardytina informacijos politika, informacijos strategija, informacijos 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 ir 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, atitinkančią organizacijos lūkesčius ir pridėtinę vertę kuriančią informaciją (English, 2004).

Ieškant gilesnių informacijos saugumo ir informacijos mokslų sąsajų ir bendrumų, vertinant pagrindinių informacijos vadybos įrankių tinkamumą valdyti informacijos saugumą, tikslinga detaliau atskleisti šių įrankių apibrėžtį, tikslus ir turinį.

2.2.1.1. Informacijos politika ir strategija

Pagrindinis informacijos politikos tikslas – pateikti pagrindinių principų sąrašą, kuris leistų įvertinti informacijos reikšmę ir vienareikšmiškai sieti ją su organizacijos tikslais ir prioritetais. Informacijos valdymas visų pirma priklauso nuo organizacijoje vyraujančios informacinės politikos. Mokslinėje literatūroje išskiriami tokie informacinės politikos modeliai (Davenport, Eccles ir Prusak, 1992, Davenport ir Prusak, 1997):

1. Technokratiškas utopizmas – pasižymi tuo, kad informacijos valdymui pasitelkiamos technologijos ir pagrindinis dėmesys teikiamas būtent joms;

2. Anarchija – būdingas absoliutus bet kokios bendros informacijos valdymo politikos nebuvimas, personalas pats tvarko savo informaciją individualiai remdamasis savo nuomone ir poreikiais;

3. Feodalizmas – informacija valdoma centralizuotai pagal padalinius ar atliekamas funkcijas, taip informacija nesidalinama visos organizacijos lygiu;

4. Monarchija – informacija tvarkoma ir informacinė veikla vykdoma pagal griežtai tik vadovo nustatytas taisykles;

5. Federalizmas – informacijos valdymas ir prieiga prie jos paremta bendru sutarimu ir jos svarbos supratimu.

Informacijos politika glaudžiai siejasi su informacijos strategija, kuri užtikrina kryptingą informacijos politikos įgyvendinimą. Remiantis teoriniais tyrimais organizacijos informacijos strategija, nustatanti organizacijos siekius ir veiklos kryptis, turi integruoti organizacijos informacinių sistemų, informacinių technologijų, informacijos išteklių bei informacijos vadybos strategijas (Schlögl, 2005; Earl, 1996), apimti organizacijos informacijos išteklių organizavimą, kontrolę, žmonių ir technologijų koordinavimą (Chaffey ir Wood, 2005; Chaffey ir White, 2011).

Vertinant informacijos politikos ir strategijos įrankių reikšmingumą informacijos saugumo valdymo kontekste, galima identifikuoti šių įrankių sąsajas su informacijos saugumo valdymo politikos dokumentu ir jame

nustatytais informacijos saugumo tikslais – konfidencialumu, vientisumu ir prieinamumu. Politika, remiantis bendrais organizacijos tikslais, turi nustatyti informacijos saugumo valdymo svarbą kitų organizacijos valdymo sričių kontekste, suformuoti pagrindinius informacijos saugumo prioritetus, identifikuoti, kurie informacijos saugumo tikslai organizacijos veiklai svarbiausi, kas turi būti atsakingas už jų įgyvendinimą. Strategijos įrankis įgalina koordinuoti organizacijoje vykdomas veiklas, nustatyti politikos įgyvendinimo kryptis, priemones ir atsakomybes.

2.2.1.2. Informacijos auditas

Informacijos audito problematiką nagrinėję autoriai (H. Botha, E. Orna, C. Burk, F. Horton, P. Drucker ir kiti) išryškino, kad informacijos auditas tampa įrankiu padedančiu valdyti informaciją, suderinti informacijos poreikius ir verslo uždavinius, išryškinti informacijos valdymo spragas, klaidas ir problemas, numatyti jų sprendimo būdus, įvertinti kokius išteklius valdo organizacija ir ar jie naudojami efektyviai.

Atliekant informacijos auditą, priklausomai nuo organizacijos poreikių ir audito tikslų, svarbu tinkamai pasirinkti konkretaus audito komandą – vidinius ar išorinius auditorius. Kiekvienas atvejis turi savų trūkumų ir privalumų, tačiau nors vidinių auditorių privalumas yra greitis, pigumas, organizacijos procesų ir prioritetų išmanymas, jų galimo subjektyvaus požiūrio padeda išvengti reguliarus išorinių auditorių pasitelkimas.

Nėra visuotinai pripažinto informacijos audito proceso modelio, tačiau, remiantis minėtų tyrėjų įžvalgomis, apibendrintai galima identifikuoti bendrus informacijos audito proceso etapus – audito planavimas, auditui reikalingų duomenų rinkimas, vertinimas ir analizė, audito ataskaitos (rastų trūkumų ir rekomendacijų) parengimas ir pateikimas vadovybei, dalyvavimas rengiant trūkumų šalinimo ir rekomendacijų įgyvendinimo planą, plano įgyvendinimo vertinimas.

Audito įrankis neabejotinai svarbus ir informacijos saugumo valdymo kontekste, ypač kada ieškoma problemų valdant informacijos saugumą. Šio

įrankio taikymas įgalina įvertinti, ar tinkamai funkcionuoja kontrolės sistema, turinti užtikrinti informacijos saugumo strategijoje numatytų priemonių įgyvendinimą, ar pasiekti numatyti rezultatai, ar šie rezultatai yra siekiami mažiausiomis sąnaudomis. Auditas taip pat leidžia įvertinti, ar teisingai pasirinkta ir pati informacijos saugumo politikos tikslų įgyvendinimo strategija.

2.2.1.3. Informacijos procesai ir aplinka

Siekiant sėkmingo informacinių procesų vykdymo bei informacijos valdymo, randasi vis daugiau informacijos valdymo sistemų. Tai nulemta sparčiai besivystančių informacinių technologijų bei jų teikiamų galimybių didėjimo. Vertinant C. Schlögl įžvalgas, į informacijos valdymą galima žiūrėti pagal tai, į ką, valdant informaciją, kreipiama daugiausiai dėmesio. Galima skirti tokias informacijos valdymo rūšis:

- į technologijas orientuotas informacijos valdymas;
- į turinį orientuotas informacijos valdymas (Schlögl, 2005).

Tačiau norint užtikrinti organizacijos prisitaikymą prie besikeičiančios aplinkos siektina taikyti Ch. Choo pasiūlytą procesinį informacijos modelį, kuriame pateikiamas nenutrūkstamas ir glaudžiai susijusių veiklų (informacijos poreikių identifikavimas, informacijos įsigijimas, informacijos organizavimas ir saugojimas, informacijos produktų ir paslaugų vystymas, informacijos sklaida ir informacijos naudojimas) ciklas, ir T. Davenport bei L. Prusak ekologinį informacijos vadybos modelį, kuris nusako, kad turėtų būti vertinami tiek išorinės (veiklos, technologijų ir informacijos rinkos), tiek organizacinės (verslo situacijos, fizinis pasirengimas, investicijos į technologijas), tiek ir informacinės (strategija, procesai, politika, architektūra, darbuotojai, kultūra ir elgsena) aplinkos komponentai (Choo, 2002; Davenport ir Prusak, 1997).

Informacijos vadybos teoretikai, nagrinėję informacijos vadybos procesus ir informacinę aplinką, neišryškino saugumo dedamosios, išskyrus jau aptartą informacijos sklaidos procesą, kuriame akcentuota prieigos valdymo svarba, t. y. užtikrinimas, kad informacija pasiektų tik tuos, kam ji skirta.

Gretinant informacijos vadybos procesinio modelio procesus ir ekologinio modelio aplinkas su informacijos saugumo valdymo priemonių turiniu ir išskirtomis informacijos saugumo valdymo dimensijomis, galima aiškiai identifikuoti sąsajas – siekiant tinkamai valdyti informacijos saugumą, jis turi būti integruotas į visus informacijos vadybos procesus bei informacijos aplinkų dedamąsias.

2.2.1.4. Informacijos kokybės valdymas

Sėkmingas organizacijos informacijos valdymas priklauso nuo informacijos kokybės. Informacijos kokybė gali būti pripažįstama pagrindine informacijos verte. Informacijos kokybei būdingos esmės, prieinamumo, konteksto ir reprezentatyvumo kategorijos, apimančios tikslumo, objektyvumo, patikimumo, reputacijos, prieinamumo, saugumo, relevantumo, pridėtinės vertės, savalaikiškumo, išsamumo, vienareikšmiškumo, suprantamumo, glaustumo bei nuoseklumo požymius (Wang ir Strong, 1996). Informacijos kokybė priklauso nuo organizacijos informacinės brandos, kuri išreiškia ir visų darbuotojų bei vadovybės požiūrį į informaciją. Informacinės brandos tyrėjai (English, 2004; Markevičiūtė, 2009; Griffin, 2006) išskiria informacinės brandos lygius, kurie nuo žemiausio iki aukščiausio gali būti įvardinami kaip neapibrėžtumo, pirminis, iniciatyvos, valdymo ir optimizavimo, bei kriterijus, kurių atžvilgiu šiuos lygius galima vertinti. Tokių kriterijų pavyzdžiai galėtų būti: požiūris į informaciją, informacijos organizavimas, informaciniai procesai ar informacinių technologijų integravimas procesams optimizuoti. Taigi galima teigti, kad vienas svarbiausių sėkmingo organizacijos tikslų įgyvendinimo veiksnių yra organizacijos informacinė branda, kuri tiesiogiai siejasi su organizacijos informacijos kokybės valdymu.

Lyginant minėtų informacijos brandos tyrėjų (English, 2004 ir kiti) išskirtų informacijos brandos lygių turinį su informacijos saugumo brandos lygių (COBIT metodikos autoriai) ir žinių vadybos brandos lygių (Ehms ir Langen, 2002) turinio apibrėžtimis galima identifikuoti akivaizdžias sąsajas. Tyrėjai, naudodami penkių pagrindinių lygių skalę (Cobit metodikoje

papildomai dar išskiriamas nulinis lygis), labai panašiai apibūdina šiuos lygius: nuo žemiausio (pradedant menku organizacijų supratimu apie poreikį ką nors (informaciją, žinias, informacijos saugumą) valdyti) iki aukščiausio (iki brandžių optimizuotų vadybinių procesų, glaudžiai integruotų į strateginius organizacijos tikslus ir kasdieninę veiklą (šių lygių turinys detaliai atskleistas disertacijos 7 priede).

Taigi organizacijos brandos lygis lemia tiek informacijos vadybos, tiek ir informacijos saugumo valdymo kokybę. Vertėtų išryškinti organizacijos brandos lygio ir taikomų vadybos priemonių priklausomybę, t. y. pagal organizacijos brandos lygį turėtų būti parenkami ir atitinkami vadybos metodai. Aukštesnės brandos organizacijos, kurios supranta ir turi patirties bei kompetencijos taikyti tiek informacijos vadybos, tiek ir informacijos saugumo valdymo metodus, gali taikyti vis sudėtingesnius vadybos metodus ir taip užtikrinti kokybės augimą ir priešingai – žemos brandos organizacijoms sudėtingi valdymo metodai iš karto laukiamos naudos neduos, jos turėtų nuosekliai kelti organizacijos kompetenciją ir brandą.

2.2.2. Informacijos vadybos įrankių taikymo informacijos saugumo valdymui analizės apibendrinimas

Išanalizavus pagrindinių informacijos vadybos įrankių turinį bei sąsajas tarp informacijos vadybos bei informacijos saugumo valdymo problematikų, galima apibendrintai įvertinti informacijos vadybos įrankių aktualumą 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 principus. Informacijos strategijos reikšmė yra svarbi informacijos saugumo valdymui ir leistų apibrėžti informacijos saugumo valdymo atsakomybes, koordinavimą, orientavimą į pagrindinius organizacijos procesus, audito bei informacinių technologijų taikymą.

Informacijos audito tikslai aktualūs vertinant informacijos saugumo kontekstą. Informacijos audito analogijas su informacijos saugumo auditu galima įžvelgti vertinant tiek audito tikslus, tiek informacijos audito komandos sudarymo (pasirinkimo tarp vidinių ir išorinių auditorių), tiek ir 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. Informacinė branda priklauso nuo visų darbuotojų bei vadovybės požiūrio į informacijos kokybę, taip pat ir į informacijos saugumą. Čia galima daryti sąsajas su disertacijoje aptarta įžvalga, kad tik saugi ir patikima informacija gali būti pavadinta kokybiška. Atlikus informacijos vadybos, žinių vadybos ir informacijos saugumo valdymo brandos lygių turinio analizę, identifikuotas jų sąsajumas. Organizacijos branda taip pat sietina su organizacijos sugebėjimu taikyti pažangias valdymo priemones, užtikrinti visų informacijos procesų saugumo valdymą bei savalaikį reagavimą į išorinės, organizacinės bei informacinės aplinkos komponentų pokyčius.

Jeigu organizacijoje yra aiški informacinė politika ir strategija, nuolat atliekamas auditas, valdomi visi informaciniai procesai, operatyviai prisitaikoma prie aplinkos pokyčių bei yra aukštas informacinės brandos lygis, galima pagrįstai tikėtis, kad bus užtikrintas ir informacijos saugumo valdymas.

Įvertinus disertacijos pirmoje dalyje išskirtą informacijos saugumo valdymo turinį (objektą, tikslus ir dimensijas), pagrindiniais įrankiais informacijos saugumo valdymui išskirtini – informacijos saugumo politika, informacijos saugumo strategija ir informacijos saugumo auditas. Informacijos saugumo procesų, aplinkos komponentų ir informacijos saugumo brandos vertinimas priskirtinas prie papildomų įrankių, kurių taikymas teoriniame ir praktiniame lygmenyse galėtų būti nagrinėjamas kaip pasiūlymai informacijos saugumo valdymo brandai ir kokybei gerinti.

2.3. Integralus informacijos saugumo valdymo modelis

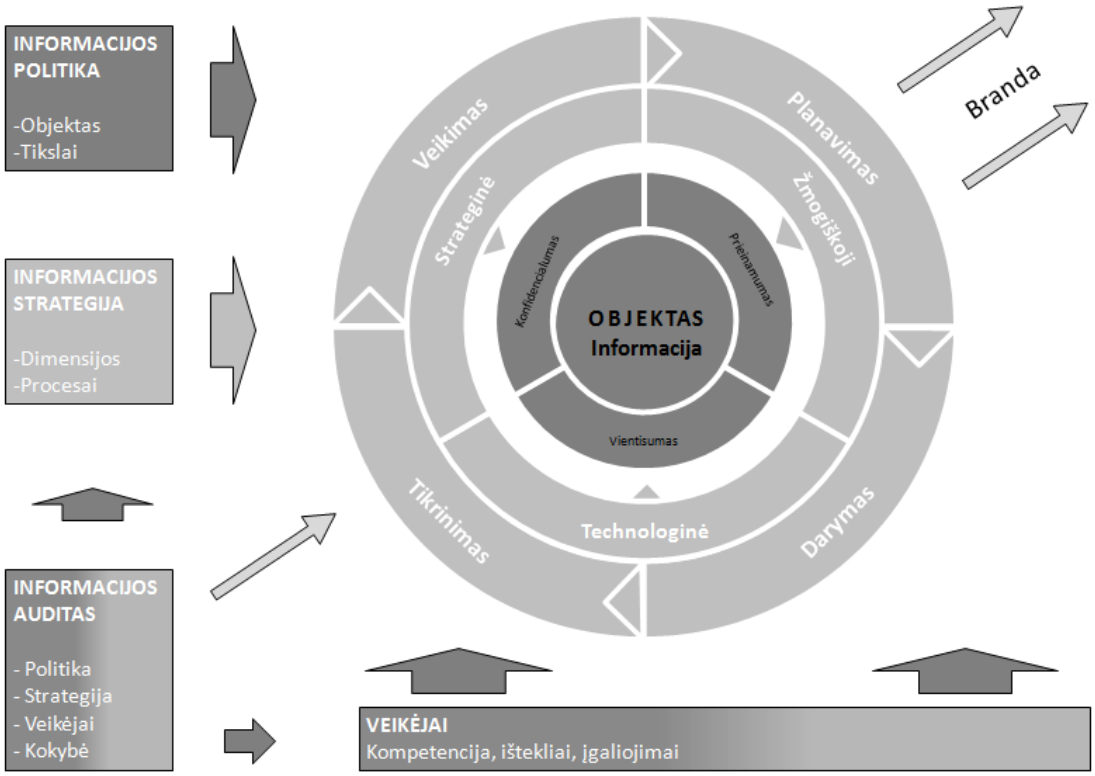
Atlikus informacijos saugumo ir informacijos vadybos diskursų tyrimą, disertacijos pirmoje dalyje suformuluoti informacijos saugumo valdymo turinio elementai – objektas, tikslai ir dimensijos, disertacijos antroje dalyje aptarti pagrindiniai informacijos vadybos įrankiai – informacijos politika, informacijos strategija ir informacijos auditas.

Ištyrus teorinius konceptus ir pagrindus informacijos saugumo valdymo ir informacijos vadybos sąsajumą, galima gretinti informacijos saugumo valdymo turinio elementus su informacijos vadybos įrankiais. Pasiremiant atskleista šių abiejų diskursų sudedamųjų dalių apibrėžtimi, galima jungti abiejų diskursų *politikos lygmenį*, kuriame nustatomi tikslai ir pagrindiniai principai, t. y. informacijos saugumo objektas (informacija) ir tikslai (konfidencialumas, vientisumas ir prieinamumas). *Strategijos lygmuo* sujungia 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. Remiantis disertacijoje pateiktais informacijos saugumo valdymo priemonių analizės rezultatais, galima konstatuoti, kad kaip plačiausiai aptartas ir universaliausias proceso valdymo įrankis gali būti naudojamas Demingo (2000) ciklas.

Audito lygmuo užtikrina efektyvaus valdymo kontrolę, padeda nustatyti valdymo spragas, įvertinti apibrėžtą informacijos politiką bei politikos įgyvendinimo strategiją. Bet kokiems procesams valdyti būtinas įgalinantis veiksnys – įgalioti veikėjai, t. y. pakankamų išteklių (kompetencijos) delegavimas. Kokybės (brandos) kėlimas įvardytinas kaip antrasis procesų tobulinimą įgalinantis veiksnys. *Audito lygmuo* leidžia įvertinti ir šiuos įgalinančius veiksnius.

Integralus teorinis informacijos saugumo valdymo modelis, sujungiantis aptartą informacijos vadybos mokslų ir informacijos saugumo valdymo sąsajumą pateikiamas 18 paveiksle.

Modelio centre pavaizduotas informacijos saugumo objektas – informacija. Pirmasis modelio žiedas iliustruoja informacijos saugumo tikslus. Šias modelio dedamąsias sujungia 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 sujungia informacijos strategijos įrankis ir nusako, *kaip* turėtų būti saugoma (modelyje išskirta šviesiai pilka spalva). Informacijos audito įrankis leidžia patikrinti politikos ir strategijos pilnumą bei įvertinti, *ar yra* kitos prielaidos informacijos saugumo valdymui, t. y. ar paskirti veikėjai (deleguoti ištekliai ir kompetencijos), ar užtikrinama veiklos kokybė.



18 pav. Integralus informacijos saugumo valdymo modelis (sudaryta autoriaus).

Šis modelis formuoja visuminį požiūrį į informacijos saugumo valdymą, apibrėžia, kas ir kaip turėtų būti valdoma. Integralaus informacijos saugumo valdymo modelio kompleksiškumą išreiškia ir tai, kad modelyje integruoti

informacijos vadybos įrankiai – politika, strategija, auditas, kokybė (branda), veikėjai (kompetencijos) yra sietini su identifikuotu esamų informacijos saugumo valdymo priemonių trūkumu strateginės ir žmogiškosios dimensijų kontekste. Tinkamas informacijos vadybos įrankių įdiegimas informacijos saugumo valdymui galėtų padėti įvertinti bei sustiprinti esamas silpnas vietas ir taip užtikrinti efektyvų ir kompleksišką informacijos saugumo valdymą.

Šioje disertacijos dalyje, išanalizavus informacijos vadybos tyrėjų įžvalgas, konstatuota, kad saugumo dedamoji informacijos vadybos srityje nėra išplėtota. Mokslinėse įžvalgose, akcentuojant informaciją kaip kritinį organizacijų resursą, menkas informacijos vadybos teoretikų dėmesys šio resurso saugumui užtikrinti tampa aktualia moksline problema, o moksliškai neįtvirtintas informacijos saugumo valdymas lemia problemas, kurios išryškėja ir praktiniame lygmenyje.

Įvertinus disertacijos pirmoje dalyje išskirtą informacijos saugumo valdymo turinį (objektą, tikslus ir dimensijas) bei išanalizavus pagrindinių informacijos vadybos įrankių turinį bei sąsajas tarp informacijos vadybos bei informacijos saugumo valdymo problematikų, pagrindiniais įrankiais informacijos saugumo valdymui išskirti – informacijos saugumo politika, informacijos saugumo strategija ir informacijos saugumo auditas, taip pat svarbūs aplinkos procesai bei informacijos saugumo branda. Šie įrankiai atspindi identifikuotus trūkumus esamose informacijos saugumo valdymo priemonėse. Identifikavus šių įrankių vertę informacijos saugumo valdymui, konstatuota, kad jeigu organizacijoje yra aiški informacinė politika ir strategija, nuolat atliekamas auditas, valdomi visi informaciniai procesai, operatyviai prisitaikoma prie aplinkos pokyčių bei yra aukštas informacinės brandos lygis, galima pagrįstai tikėtis, kad bus užtikrintas ir informacijos saugumo valdymas.

Analizės rezultatai leido sumažinti spragą moksliniuose tyrimuose ir parodyti teorinį mokslinės problemos sprendimą žvelgiant į informacijos saugumo valdymo problemą informacijos vadybos kontekste. Aptartų tyrimų

rezultatai sukūrė teorinį pagrindą suformuoti integralų informacijos saugumo valdymo modelį. Suformuotas teorinis modelis integruota ir išplėtota saugumo dedamąja praplėtė informacijos vadybos ribas.

Teorinis integralus informacijos saugumo valdymo modelis suformuoja visuminį požiūrį į informacijos saugumo valdymo turinį, nusakantį, kas ir kaip turėtų būti valdoma, ir apibrėžia informacijos vadybos įrankius, kurie sudaro sąlygas įvertinti ir užtikrinti informacijos saugumo valdymo kompleksiškumą.

Tikėtina, kad suformuotas teorinis integralus informacijos saugumo valdymo modelis gali būti taikomas tiek teoriniame, tiek ir praktiniame lygmenyse. Modelio praktiniam pritaikymui informacijos saugumui valdyti tikslinga atlikti tolesnius tyrimus.

III DALIS. EMPIRINIS TYRIMAS: INTEGRALAUS INFORMACIJOS SAUGUMO VALDYMO MODELIO TAIKYMAS LIETUVOS VALSTYBĖS INSTITUCIJOMS

Atlikus informacijos saugumo ir informacijos vadybos diskursų tyrimą, disertacijos pirmoje dalyje suformuluoti informacijos saugumo valdymo turinio elementai – objektas, tikslai ir dimensijos, disertacijos antroje dalyje aptarti pagrindiniai informacijos vadybos įrankiai – informacijos politika, informacijos strategija, informacijos auditas, informacijos kokybė (branda) bei veikėjai. Sujungus šiuos elementus sudarytas teorinis integralus informacijos saugumo valdymo modelis. Šis modelis suformuoja visuminį požiūrį į informacijos saugumo valdymo turinį, nusakantį, kas ir kaip turėtų būti valdoma, ir apibrėžia informacijos vadybos įrankius, kurie sudaro sąlygas įvertinti ir užtikrinti informacijos saugumo valdymo kompleksiškumą.

Teoriniame lygmenyje suformuotas integralus informacijos saugumo valdymo modelis, tikėtina, gali būti taikomas ne tik mokslinių tyrimų plėtotei, bet ir praktinio lygmens problemoms spręsti. Šiai prielaidai patikrinti atliktas integralaus informacijose saugumo valdymo modelio taikymo Lietuvos valstybės institucijoms empirinis tyrimas.

3.1. Empirinio tyrimo metodologinis pagrindimas

Empirinio tyrimo tikslas

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

Empirinio tyrimo objektas

Empirinio tyrimo objektas – integralaus informacijos saugumo valdymo modelio praktinis taikymas informacijos saugumo valdymui Lietuvos valstybės institucijose.

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 remiantis suformuotos informacijos saugumo valdymo prieigos įrankiais ir vertinimo kriterijais.
4. Įvertinti, kaip Lietuvos valstybės institucijos įgyvendina galiojančius informacijos saugumo reikalavimus.

Empirinio tyrimo hipotezės:

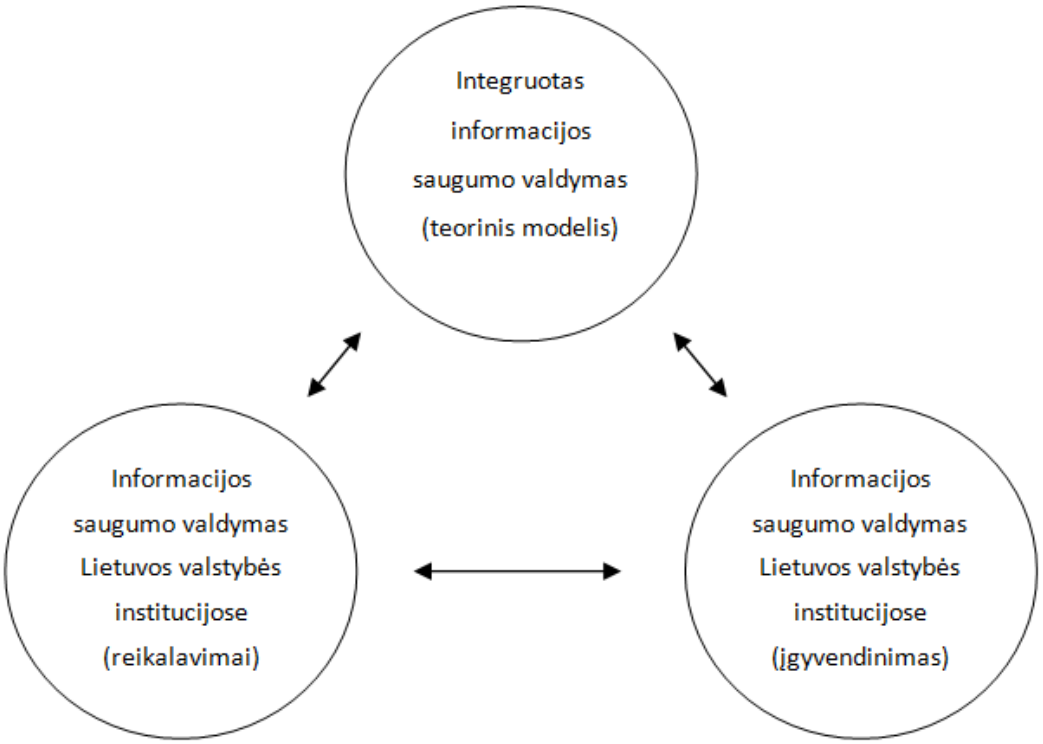
1. Informacijos saugumo valdymui pasitelkiant informacijos vadybos įrankius gali būti užtikrintas efektyvus informacijos saugumo valdymas.
2. Informacijos saugumas Lietuvos valstybės institucijose nėra tinkamai valdomas, dėl informacijos saugumo reikalavimų fragmentiškumo ir vyraujančio formalaus techninio požiūrio.
3. Integralus 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 modelis

Empirinio tyrimo modelis sudarytas iš šių elementų: 1) teorinio integralaus informacijos saugumo valdymo modelio; 2) galiojančių informacijos saugumo valdymo reikalavimų Lietuvos valstybės institucijoms (formalioji aplinka); 3) realios informacijos saugumo valdymo reikalavimų įgyvendinimo Lietuvos valstybės institucijose situacijos (realioji aplinka). Šių modelio elementų sąsajas (tikėtiną neatitikimą) turėtų atskleisti empirinio tyrimo rezultatai. Remiantis tyrimų rezultatais, formuluojami siūlymai, kaip

užtikrinti integralaus informacijos saugumo valdymo modelio, informacijos saugumo valdymo reikalavimų Lietuvos valstybės institucijoms ir šių reikalavimų įgyvendinimo atitikimą, t. y. kaip teorinį integralų informacijos saugumo valdymo modelį perkelti į formalią informacijos saugumo valdymo reikalavimų Lietuvos valstybės institucijoms aplinką ir užtikrinti šių reikalavimų įgyvendinimą realioje Lietuvos valstybės institucijų aplinkoje. Šių siūlymų įgyvendinimo galimybės rodo teorinio integralaus informacijos saugumo valdymo modelio praktinio įgyvendinimo galimybes.

Empirinio tyrimo modelis pavaizduotas 19 paveiksle.



19 pav. Empirinio tyrimų modelis.

Empirinio tyrimo metodai

Empiriniam tyrimui atlikti taikyta mišrių metodų prieiga derinant kokybinių ir kiekybinių tyrimų metodus – dokumentų turinio analizę, ekspertų interviu ir anketinę institucijų apklausą. Pagrindiniai mišrių metodų prieigos taikymo motyvai: siekis surinkti įvairesnę, turtingesnę empirinę medžiagą bei pagrįsti tyrimo rezultatus skirtingais duomenų šaltiniais ir formomis (Creswell

ir Clark, 2006). Mišrių metodų strategijoje skirtingų metodų derinimas leidžia vienu metodu surinktus ir išanalizuotus duomenis papildyti bei patikrinti kitu metodu surinktais ar išanalizuotais duomenimis. Taigi derinant šiuos metodus galima užtikrinti visapusiškai argumentuotus ir patikimus tyrimo rezultatus teorinio integralaus informacijos saugumo valdymo modelio praktinei realizacijai ir pagrindimui.

Empirinio tyrimo duomenims analizuoti taikyta nuoseklių procedūrų tyrimo strategija. Kokybiniai ir kiekybiniai duomenys renkami nuosekliai vieni po kitų, renkamais duomenimis detalizuoti, praplėsti bei papildyti anksčiau surinktų duomenų pagrindu gauti rezultatai. Remiantis teoriniu integraliu informacijos saugumo valdymo modeliu buvo suformuota informacijos saugumo vertinimo prieiga, išskirti informacijos saugumo valdymo įrankiai ir apibrėžti vertinimo kriterijai. Ši prieiga taikyta identifikuotų šaltinių, formuojančių informacijos saugumo valdymo reikalavimus Lietuvos valstybės institucijoms, turiniui analizuoti. Analizės rezultatai panaudoti formuluojant klausimus ekspertams, o kartu su ekspertų interviu įžvalgomis (iškeltais probleminiais klausimais) – sudarant kiekybinio tyrimo (institucijų apklausos) anketas. Taigi nuoseklių procedūrų tyrimo strategijos taikymas leido dokumentų turinio analizės rezultatus patikrinti kitu kokybiniu metodu – ekspertų interviu ir, pritaikius kiekybinius metodus (anketine apklausą), surinktais statistiniais duomenimis, reprezentuojančiais empirinio tyrimo populiaciją, – Lietuvos valstybės institucijas.

Aptarta mišrių metodų prieiga ir nuoseklių procedūrų tyrimo strategija sudaro prielaidas empirinio tyrimo tikslui pasiekti ir iškeltiems uždaviniams įgyvendinti.

Dokumentų turinio analizė

Pagrindinis informacijos saugumo valdymo Lietuvos valstybės institucijose tyrimo metodas – dokumentų turinio analizė. Šis metodas taikytinas pirminiams duomenims rinkti, kai pagrindiniu informacijos šaltiniu naudojami dokumentai. Metodo patikimumą užtikrina oficialių dokumentų

naudojimas (Tidikis, 2003). Dokumentų turinio analizės metodu įvairiais pjūviais išanalizuoti Lietuvos valstybės institucijoms galiojantys informacijos saugumo valdymo reikalavimai, institucijų nuostatai ir kiti identifikuoti, su informacijos saugumo valdymu susiję norminiai dokumentai.

Dokumentų turinio analizė. Tyrimo strategija ir etapai. Dokumentų turiniui analizuoti taikyti trys etapai: 1) remiantis teoriniu integraliu informacijos saugumo valdymo modeliu suformuoti vertinimo prieigą ir vertinimo kriterijus, 2) atlikti aktualių šaltinių, formuojančių informacijos saugumo valdymo reikalavimus Lietuvos valstybės institucijoms, atranką, 3) remiantis suformuota vertinimo prieiga ir vertinimo kriterijais, dokumentų turinio analizės metodu ištirti atrinktus šaltinius.

Dokumentų turinio analizė. Informacijos saugumo valdymo vertinimo prieiga. Integralaus informacijos saugumo valdymo modeliui taikyti informacijos saugumo valdymui Lietuvos valstybės institucijose vertinti suformuota informacijos saugumo valdymo vertinimo prieiga. Šiai prieigai suformuoti dekomponuotas integralus informacijos saugumo valdymo modelis išskleidžiant informacijos vadybos įrankius bei šių įrankių turinį susiejant su informacijos saugumo valdymo turinio dedamosiomis (objektu, tikslais, dimensijomis) ir taip suformuojant vertinimo kriterijus.

Informacijos saugumo valdymo vertinimo prieiga taikyta dokumentų turinio analizei – identifikuoti šaltiniai nagrinėjami vertinant ar (ir kaip) juose apibrėžtas įvardintų įrankių taikymas, šiam vertinimui taikomi iškirti kriterijai, kurie suformuluoti kaip klausimai, į kuriuos turėtų būti atsakyta atliekant dokumentų turinio analizę.

Informacijos saugumo valdymo vertinimo prieiga taip pat naudota ir kitais tyrimų metodais gautų rezultatų aptarimui struktūrizuoti, tai leido dokumentų turinio analizės rezultatus nuosekliai papildyti ir praplėsti kitais tyrimo metodais gautais rezultatais.

Informacijos saugumo valdymo vertinimo prieiga pateikta 4 lentelėje.

4 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, atsakomybės, 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?

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

Dokumentų turinio analizė. Šaltinių analizė. Dokumentų turiniui analizuoti reikalingi norminiai dokumentai atrinkti pasinaudojant viešai prieinama Lietuvos Respublikos Seimo teisės aktų baze[10]. Šioje bazėje buvo ieškoma teisės aktų, reglamentuojančių informacijos saugumą, paieškos

[10] Lietuvos Respublikos Seimas. Dokumentų paieška // http://www3.lrs.lt/dokpaieska/forma_l.htm (žiūrėta 2012 m. kovo 8 d.)

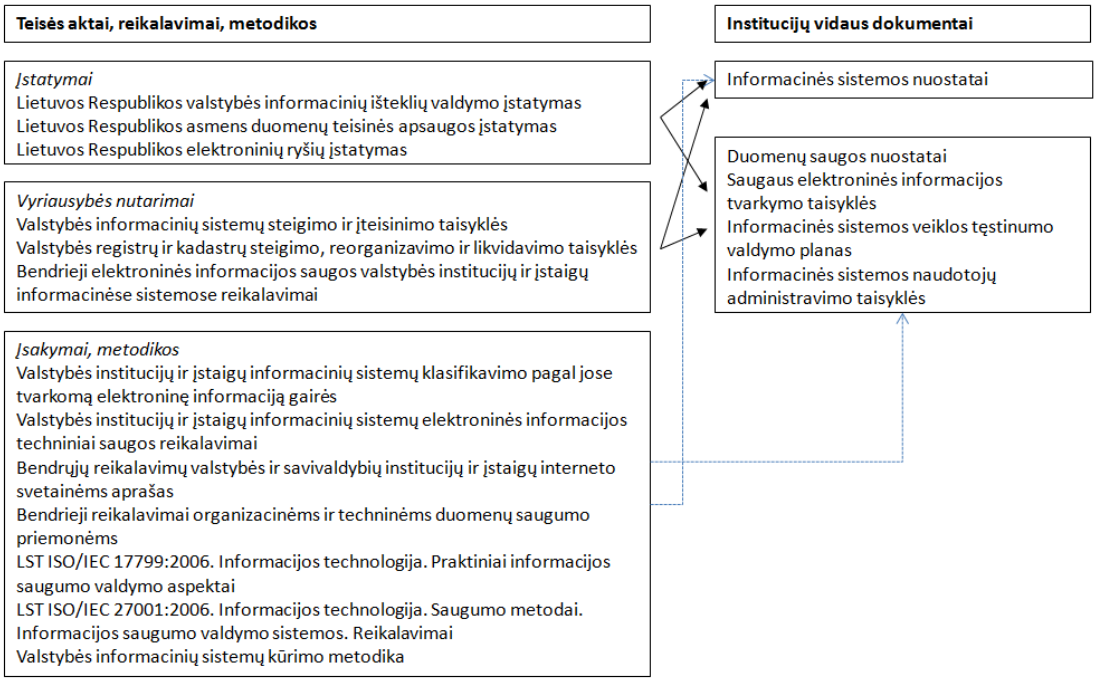
kriterijumi pasirenkant reikšminius žodžius „sauga“, „saugumas“, „apsauga“, „informacijos sauga“ „informacijos saugumas“, „informacijos apsauga“, taip pat pagal analogiją kombinacijas su reikšminiais žodžiais „elektroninis“, „informacinės sistemos“, „informacinės technologijos“ ir „duomenys“. Atrinkus aktualius šaltinius, gilesnė paieška buvo vykdoma pasiremiant teisės aktų bazės nuorodomis į susijusius teisės aktus bei teisės aktuose rastomis nuorodomis. Papildomos šaltinių paieškos atliktos atrinktuose teisės aktuose, nurodytuose juos įgyvendinančių institucijų interneto svetainėse. Buvo analizuojami šių institucijų parengti teisės aktai, metodiniai dokumentai, ataskaitos, nuostatai, struktūra, etatų sąrašai ir pareigybių aprašymai.

Atlikta tyrimui reikalingų šaltinių paieška leido sudaryti informacijos saugumą reglamentuojančių teisės aktų sąrašą (chronologinis teisės aktų sąrašas pateiktas disertacijos 3 priede). Analizuojant šių teisės aktų turinį konstatuotina, kad Lietuvoje nėra specialaus įstatymo, nuosekliai reglamentuojančio su informacijos saugumu susijusius santykius. Pažymėtina, kad nors jau kelios paskutinės Lietuvos Respublikos Vyriausybės savo programose numatė parengti Elektroninių ryšių tinklų ir informacijos saugumo įstatymą, kuriuo būtų siekiama kompleksiškai reglamentuoti informacijos saugumo valdymą, tačiau toks įstatymas iki šiol nepriimtas.

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 2012 m. galiojusi *Lietuvos Respublikos valstybės registrų įstatymą*. Informacijos saugumas taip pat reglamentuotas 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 pateikti 20 paveiksle. Kairėje šio paveikslo pusėje išdėstyti

aktualūs įstatymai, Lietuvos Respublikos Vyriausybės nutarimai, atsakingų institucijų įsakymai ir metodiniai dokumentai (valstybės lygmuo), dešinėje – vidiniai dokumentai, kuriuos privalo parengti Lietuvos valstybės institucijos (institucijų lygmuo). Šiame paveiksle rodyklės nurodo prievolę nustatančius ryšius, punktyrinės rodyklės – metodinius dokumentus, padedančius parengti privalomus dokumentus.



20 pav. Informacijos saugumo valdymo reikalavimų sąryšiai (sudaryta autoriaus).

Ekspertų interviu

Socialiniams reiškiniams geriau pažinti dažnai taikomas ekspertų interviu metodas. Ekspertų interviu 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, taikant ekspertų interviu metodą, siekiama pagrįsti ir papildyti dokumentų turinio analizės rezultatus. Šio metodo taikymas leidžia

susieti teorinį lygmenį su praktinio įgyvendinimo realybe, įvertinti teorinių išvadų pritaikomumo galimybes.

Ekspertų interviu. Ekspertų parinkimas. Tinkamas ekspertų parinkimas yra esminis šio metodo patikimumo kriterijus, todėl respondentams atrinkti vykdyta tikslinė atranka, kuriai taikyti šie kvalifikaciniai kriterijai:

1. Ne mažesnė nei 5 metų darbo patirtis informacijos saugumo srityje dalyvaujant informacijos saugumo politikos formavimo procese ir (arba) ją įgyvendinant, kada valdomi ypatingos svarbos valstybės informaciniai ištekliai;
2. Atstovavimas skirtingoms organizacijoms.

Šie kriterijai pasirinkti norint tyrimui pasitelkti ekspertus, kurie turi pakankamą patirtį informacijos saugumo srityje, tiesiogiai dalyvauja formuojant informacijos saugumo politiką ar yra atsakingi už šios politikos įgyvendinimą valdant ypatingos svarbos valstybės informacinius išteklius, taip pat išmano valstybės institucijų veiklos specifiką ir nėra tiesiogiai tarpusavyje susiję pavaldumo ar kitais ryšiais. Šie kriterijai leidžia užtikrinti kompetentingų bei visapusiškų nuomonių įtraukimą, kartu užtikrina, kad ekspertai vykdė funkcijas ilgiau nei vieną Lietuvos Respublikos Vyriausybės kadenciją, kas leidžia sumažinti galimą „politinį“ kontekstą (tai aktualu, nes ekspertai aukštas pareigas užimantys valstybės tarnautojai). Atsižvelgiant į šiuos kriterijus ekspertais buvo pasirinkti atstovai iš:

1. Institucijų dalyvavusių rengiant *Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programą*;
2. Institucijų paskirtų atsakingomis už *Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos* įgyvendinimą;
3. Priežiūros ir kontrolės institucijų;
4. Institucijų valdančių ypatingos svarbos valstybės informacinius išteklius.

Remiantis šiais kriterijais kokybiniam tyrimui buvo atrinkti 6 ekspertai. Visi šie ekspertai turi daugiau nei 5 metus profesinės darbo patirties valstybės

institucijose ir dalyvaujant informacijos saugumo politikos formavimo procese ir (arba) ją įgyvendinant. Atrinktų ekspertų tiesioginės funkcijos yra susijusios su informacijos saugumo politikos formavimu; teisės aktų rengimo organizavimu; dalyvavimu darbo grupėse, rengusiose informacijos saugumo strateginius dokumentus ir (ar) reikalavimus bei koordinuojančiose šių dokumentų įgyvendinimą; ypatingos svarbos valstybės informacinių išteklių valdymu ir jų saugumo užtikrinimo koordinavimu; institucijų veiklos kontrole bei reguliavimu informacijos saugumo srityje.

Siekiant surinkti kuo objektyvesnius duomenis bei sudaryti sąlygas ekspertams atvirai ir kritiškai įvertinti informacijos saugumo valdymo Lietuvos valstybės institucijose situaciją, nebūtinai sutampančią su oficialia jų atstovaujamų institucijų pozicija, ekspertams buvo garantuotas anonimiškumas, todėl detalesnė informacija apie ekspertus ir jų atstovaujamų institucijų pavadinimus neatskleidžiama.

Ekspertų interviu. Tyrimo projektavimas ir eiga. Informaciją iš ekspertų geriausia rinkti giluminio ekspertų interviu būdu, leidžiančiu visapusiškai suprasti analizuojamą situaciją. Giluminis interviu yra apibrėžiamas kaip tyrėjo ir informanto dialogas, siekiant gauti detalios informacijos nagrinėjamu klausimu. Kokybiniams tyrimams vykdyti priimtiniausiu laikomas iš dalies struktūruotas (kryptingas) interviu. Tokio interviu metu tyrėjas iš anksto numato pokalbio temas, bet pats interviu nėra griežtai įspraudžiamas į temų eiliškumą. Toks tyrimo būdas padeda surinkti išsamius duomenis svarbiais tyrimui klausimais (Kardelis, 2002; Tidikis, 2003).

Dėl aptartų pranašumų kokybiniam tyrimui atlikti pasirinktas kryptingas interviu: ekspertams suformuluoti iš dalies struktūruoti klausimai sieti su informacijos saugumo valdymo turinio (objekto, tikslų, dimensijų) ir jo sąsajų su informacijos vadybos įrankiais (politikos, strategijos, audito, veikėjų ir kokybės) kontekstu. Apibendrintos klausimų grupės buvo suformuotos atsižvelgiant į dokumentu turinio analizės metu iškeltus probleminius klausimus.

Ekspertams formuluotos šios penkios pagrindinės klausimų temos:

1. Informacijos saugumo valdymo objektas ir tikslai.
2. Informacijos saugumo valdymo organizavimas, kompetencijos ir atsakomybės.
3. Informacijos saugumo brandos vertinimo kriterijai ir poreikis. Institucijų situacija.
4. Informacijos saugumo funkcijų centralizavimo poreikis ir apimtys.
5. Informacijos saugumo stebėsenos ir kontrolės sistemos kūrimas ir vertinimo kriterijai.

Bendraujant su ekspertais, kaip pagrindinis komunikavimo metodas, buvo naudojamas interviu akis-į-akį, su keliais ekspertais buvo bendrauta telefonu. Interviu vidutiniškai truko devyniasdešimt minučių, kai kurie klausimai bei papildomi aspektai su ekspertais buvo tikslinami elektroniniu paštu.

Ekspertų interviu. Tyrimo rezultatų analizės metodas. Kokybinio tyrimo rezultatų analizei atlikti taikytas surinktos medžiagos turinio analizės metodas, grįstas fenomenologijos paradigma. Taikant šį metodą rekomenduojama analizuojant surinktą tyrimo medžiagą sudaryti ekspertų interviu išrašus (pateikta disertacijos 8 priede), išskirti pagrindines temas ir parengti apibendrinamąją lentelę (pateikta disertacijos 9 priede) bei formuluoti išsamius temų apibendrinimus.

Pabrėžtina, kad ekspertų nuomonės analizuotais klausimais iš esmės nesiskyrė, išsakyti požiūriai diskutuotomis temomis papildė vienas kitą. Tokia unitarinio pobūdžio interviu medžiaga leido suformuoti išsamų ir, manoma, objektyviai atitinkantį realybę informacijos saugumo valdymo Lietuvos valstybės institucijose padėties vaizdą.

Anketinė institucijų apklausa

Šis kiekybinio tyrimo metodas leidžia aiškinti ir prognozuoti socialinius objektus, priežastinius ryšius bei funkcionavimo veiksnius, išmatuoti ir statistiškai apibūdinti tiriamus požymius, taikant matematinius analizės

metodus įvertinti tiriamų požymių ryšį (Kardelis, 2002). Empirinio tyrimo kiekybiniams duomenims surinkti taikytas anketinės apklausos metodas. Šis metodas leidžia išmatuoti tiriamų objektų požymius ir identifikuoti jų ryšius.

Kiekybinis tyrimas taikytas statistiniams duomenims surinkti, šie duomenys reikalingi kokybinių tyrimų rezultatams pagrįsti bei atsakyti į kokybinių tyrimų metu iškeltus probleminius klausimus.

Institucijų apklausos anketą sudarė 3 dalys:

1. Pirmoji anketos dalis skirta išsiaiškinti tiriamos valstybės institucijos pilną pavadinimą, dydį (darbuotojų skaičių), informacinių technologijų bei informacijos saugumo padalinių egzistavimą.

Institucijos pilnas pavadinimas leidžia nustatyti jos statusą (centrinės ar regioninės valdžios) bei pavaldumą Lietuvos Respublikos Vyriausybei. Ši informaciją aktuali siekiant ištirti, kiek institucijos pavaldumas veikia nustatytų reikalavimų laikymąsi, ypač atsižvelgiant į tai, kad dauguma informacijos saugumo reikalavimų yra patvirtinti Lietuvos Respublikos Vyriausybės ir jai tiesiogiai nepavaldžioms institucijoms buvo tik rekomendacinio pobūdžio. Informacinių technologijų ir informacijos saugumo padalinio (atsakomybių) identifikavimas leido nustatyti valstybės institucijos požiūrį į informacijos saugumą, t. y. ar tiriama institucija turi informacinių technologijų padalinį bei kam pavesta atsakomybė už informacijos saugumo užtikrinimą – specialiam darbuotojui (padaliniui) ar tam pačiam, už informacijos technologijų priežiūrą atsakingam padaliniui.

2. Antroji anketos dalis skirta išsiaiškinti, kiek ir kokių valstybės informacinių išteklių valdo tiriama valstybės institucija.

Ši informacija aktuli atsižvelgiant į tai, jog dokumentų turinio analizės metu buvo nustatyta, kad informaciniai ištekliai yra Lietuvos valstybės institucijoms galiojantis informacijos saugumo valdymo objektas, bei į tai, kad tik trims iš keturių informacinių išteklių rūšių yra tiesiogiai taikomi informacijos saugumo valdymo reikalavimai. Taigi surinkta informacija leistų įvertinti, ar visos tiriamos institucijos valdo informacinius išteklius, kokia

informacijos saugumo valdymo situacija valstybės institucijose, kurios nevaldo informacinių išteklių ar valdo kelis.

3. Trečioji – skirta išsiaiškinti valstybės institucijos požiūrį į informacijos saugumo tikslus (kiek šie tikslai aktualūs tiriamai institucijai, kuriam tikslui skiriamas prioritetas); informacijos saugumo valdymui taikomus reikalavimus ir metodikas; saugos įgaliotinio egzistavimą bei jo vietą institucijoje (pareigas, pavaldumą); informacijos saugumo audito ir kitų vertinimo bei kontrolės priemonių taikymą; institucijos turimus informacijos saugumą reglamentuojančius dokumentus ir jų aktualumą; informacijos saugumo mokymų vykdymą institucijoje; pagrindines problemas ir iššūkius, su kuriais susiduria valstybės institucija, siekdama užtikrinti informacijos saugumą, bei institucijos nuomonę, kokias informacijos saugumo funkcijas reikėtų organizuoti centralizuotai, kokias palikti vykdyti pačiai institucijai.

Ši informacija aktuali analizuojant, kaip valstybės institucijos laikosi galiojančių informacijos saugumo valdymo reikalavimų, bei formuluojant siūlymus dėl šių reikalavimų tobulinimo.

Apklausos anketos priedas buvo skirtas duomenims apie kiekvieną valstybės institucijos valdoma informacinį išteklių surinkti.

Anketoje pateiktiems klausimams įvertinti naudota nominalinė (siekiant nustatyti, kokiai kategorijai priklauso požymis, pavyzdžiui, valdomų išteklių rūšis), ranginė (siekiant nustatyti požymio vertes, jų didėjimo tvarką, pavyzdžiui, identifikuoti informacijos saugumo tikslų svarbą konkrečiai valstybės institucijai) ir intervalinė (siekiant nustatyti ir įvertinti požymio dydį, pavyzdžiui, identifikuoti institucijos dydį) skalės.

Anketos ir jos priedo klausimynas pateiktas disertacijos 10 priede.

Anketinė institucijų apklausa. Imties dydis ir parinkimas. Vienas iš pagrindinių kiekybinių tyrimų patikimumo kriterijų – imties dydis. Norint rezultatus taikyti platesnei populiacijai, būtina formuoti imtį tikimybiniu būdu, parenkant tokį atvejų skaičių, kuris leistų reprezentuoti tiriamąją populiaciją. Visi potencialūs empirinio tyrimo stebiniai vadinami generaline aibe. Šio

empirinio tyrimo generalinė aibė yra Lietuvos valstybės institucijos. Iš viso buvo identifikuota 140 valstybės institucijų (11 priedas).

Ruošiantis atlikti empirinį tyrimą apskaičiuotas reprezentatyvus imties dydis, kuris leistų daryti išvadas apie visą tiriamą populiaciją (Yamane, 1967):

$$n = \frac{1}{\Delta^2 + \frac{1}{N}}$$

Kur n – atvejų skaičius atrankinėje grupėje (imties dydis);

N – generalinės aibės dydis (šiuo atveju 140);

Δ – leidžiamas paklaidos dydis (0,05); skaičiuojant 95 proc. patikimumu, įprastu socialiniuose moksluose.

Pagal pateiktą formulę reikėtų apklausti 104 institucijas; įvertinta kiek daugiau – 106 institucijos.

Baigtinių populiacijų imties dydžio reprezentatyvumą gali parodyti ir koeficientas K, kuris skaičiuojamas pagal formulę (Yamane, 1967):

$$\mathrm{K} = \frac{n}{N} \times 100\ \%$$

Kur n – imties dydis (šiuo atveju 106),

N – populiacijos dydis (šiuo atveju 140).

Šio tyrimo imties reprezentatyvumo koeficientas – 75,71 proc., tai yra daugiau nei pakankamai. Tyrimų rezultatų reprezentatyvumą užtikrina ir tai, kad tyrime dalyvavo tiek centrinės valdžios Lietuvos valstybės institucijos, (ministerijos ir kitos (departamentai, Seimo, Prezidento kanceliarijos)), tiek ir regioninio lygmens valstybės institucijos (savivaldybių administracijos). Kiekybinio tyrimo reprezentatyvumo duomenys pateikti 5 lentelėje. Galima identifikuoti didžiausią reprezentatyvumą *ministerijų* ir *kitų* institucijų grupėje, kuriai priskirtos Lietuvos Respublikos Vyriausybei ir ministerijoms pavaldžios tarnybos, departamentai, inspekcijos ir kitos institucijos bei Seimo ir

Prezidento kanceliarijos). Mažiausias reprezentatyvumas savivaldos grupėje, tačiau, vertinant tai, kad tyrime dalyvavo du trečdaliai savivaldybių, o analizuojant tyrimo rezultatus pastebėtas statistiškai nedidelis skirtumas tarp savivaldybių administracijų pateiktų atsakymų, galima vertinti, kad visose grupėse respondentų tyrimo reprezentatyvumas yra pakankamas.

5 lentelė. Kiekybinio tyrimo reprezentatyvumas.

	Iš viso	Ministerijos	Savivalda	Kitos
Institucijų imtis	140	14	60	66
Gauta atsakymų	106	12	40	54
Procentas	75,71	85,71	66,67	81,82

Siekiant užtikrinti didesnį grįžtamąjį ryšį Lietuvos valstybės institucijoms apklausos anketa buvo išplatinta bendradarbiaujant su Lietuvos Respublikos vidaus reikalų ministerija. Vidaus reikalų ministerija parengtą anketą išsiuntė centrinės valdžios institucijoms – ministerijoms, tiesiogiai Lietuvos Respublikos Vyriausybei pavaldžioms institucijoms, Lietuvos Respublikos Prezidento, Ministro Pirmininko ir Seimo kanceliarijoms bei Lietuvos savivaldybių asociacijai, prašydama užtikrinti joms pavaldžių institucijų įtraukimą į anketinę apklausą. Vertinant aptartus 5 lentelėje pateiktus sugretintus valstybės institucijų ir gautų atsakymų duomenis, galima teigti, kad anketų platinimo būdas leido užtikrinti tyrimo reprezentatyvumą.

Empirinio tyrimo vykdymo laikotarpis

Dokumentų turinio analizė vykdyta 2012 m. sausio–rugpjūčio mėnesiais, rezultatų apdorojimas ir analizė – 2012 m. kovo–rugsėjo mėnesiais.

Kokybinis tyrimas (ekspertu interviu) vykdytas 2012 m. gegužės–liepos mėnesiais. Kokybinio tyrimo rezultatų apdorojimas – 2012 m. liepos–rugsėjo mėnesiais.

Kiekybinis tyrimas (anketinė apklausa) vykdytas 2012 m. liepos–rugpjūčio mėnesiais, rezultatų apdorojimas ir analizė – 2012 m. rugpjūčio ir rugsėjo mėnesiais.

3.2. Dokumentų turinio analizės rezultatai

Identifikuoti tyrimo šaltiniai analizuoti pagal suformuotą informacijos saugumo valdymo tyrimo prieigą, remiantis išskirtais informacijos saugumo politikos, strategijos, audito, brandos ir veikėjų įrankiais bei suformuotais vertinimo kriterijais.

3.2.1. Informacijos saugumo valdymo politika Lietuvos valstybės institucijose

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

Informacijos saugumo valdymo objektas

Remiantis atrinktų tyrimui šaltinių turinio analize, konstatuota, kad Lietuvoje nėra specialaus įstatymo, nuosekliai reglamentuojančio su informacijos saugumu susijusių santykių. 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 *Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas*. Analizuojant šių įstatymų turinį bei atsižvelgiant į jų reglamentuojamą sritį, galima išskirti juose apibrėžtus informacijos saugumo valdymo objektus. Šie informacijos saugumo valdymo objektai pateikti 6 lentelėje. Atsižvelgiant į empirinio tyrimo objektą, aktualiausias Lietuvos valstybės institucijoms galiojantis informacijos saugumo valdymo objektas yra informaciniai ištekliai.

6 lentelė. Teisės aktais įtvirtinti informacijos saugumo valdymo objektai (sudaryta autoriaus).

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

Informacinių išteklių funkcionavimo aplinkos analizei iki 2011 m. gruodžio 31 d. svarbiausi galiojantys teisės aktai – *Lietuvos Respublikos valstybės registrų įstatymas* ir Lietuvos Respublikos Vyriausybės nutarimai, kuriais patvirtinta: *Valstybės registrų ir kadastrų steigimo, reorganizavimo ir likvidavimo taisyklės (2005)*; *Valstybės informacinių sistemų steigimo ir įteisinimo taisyklės (2004)*; *Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai (2007)*.

Remiantis šių teisės aktų turinio analize (teisės aktų turinys detaliai atskleistas 4 disertacijos priede), Lietuvos Respublikos valstybės institucijos valdo 4 rūšių informacinius išteklius – valstybės registrus, žinybinius registrus, valstybės informacines sistemas ir vidaus administravimo informacines sistemas.

Tikslinga aptarti kiekvienos informacinių išteklių rūšies specifiką, išskiriant tyrimui aktualius gyvavimo ciklo ir informacijos saugumo užtikrinimo reikalavimus:

1. *Valstybės registrų* (kadastrų) veikla reglamentuota *Lietuvos Respublikos valstybės registrų įstatymu*, jų steigimas, reorganizavimas ir

likvidavimas nustatytas Lietuvos Respublikos Vyriausybės patvirtintomis valstybės registrų veiklą reglamentuojančiomis taisyklėmis. Valstybės registruose tvarkomos informacijos saugumas, remiantis galiojančiais teisės aktais, turi būti užtikrinamas vadovaujantis Lietuvos Respublikos Vyriausybės patvirtintuose *Bendruosiuose elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimuose* nustatyta tvarka. Galima teigti, kad šiai informacinių išteklių grupei tiek gyvavimo ciklo, tiek ir saugumo reikalavimai nustatyti aiškiai ir nedviprasmiškai.

2. *Žinybinių registrų* veiklą, kai žinybinį registrą valdo valstybės institucijos, pavaldžios Lietuvos Respublikos Vyriausybei, pavesta organizuoti vadovaujantis Lietuvos Respublikos Vyriausybės patvirtintomis valstybės registrų veiklą reglamentuojančiomis taisyklėmis tiek, kiek tai atitinka žinybinių registrų specifiką, kitoms įstaigoms šiomis taisyklėmis vadovautis tik rekomenduojama. Remiantis minėtomis taisyklėmis, žinybiniuose registruose tvarkomos informacijos saugumas turi būti užtikrinamas vadovaujantis Lietuvos Respublikos Vyriausybės patvirtintais *Bendraisiais elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimais*. Taigi žinybinių registrų atveju situacija yra dichotomiška – Lietuvos Respublikos Vyriausybei pavaldžioms institucijoms galioja privalomi žinybinių registrų gyvavimo ciklo ir saugumo reikalavimai, o nepavaldžios gali rinktis ar taikyti gyvavimo ciklo reikalavimus (informacijos saugumo valdymo reikalavimai be gyvavimo ciklo reikalavimų netenka prasmės).

3. *Valstybės informacinių sistemų* veikla reglamentuota Lietuvos Respublikos Vyriausybės patvirtintomis *Informacinių sistemų steigimo ir įteisinimo taisyklėmis*. Įstaigoms nepavaldžioms Lietuvos Respublikos Vyriausybei šios taisyklės yra rekomendacinio pobūdžio. Remiantis minėtomis taisyklėmis, valstybės informacinėse sistemose tvarkomos informacijos saugumas turi būti užtikrinamas vadovaujantis Lietuvos Respublikos Vyriausybės patvirtintais *Bendraisiais elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimais*. Vertinant

šios išteklių rūšies teisinį reglamentavimą, galima pastebėti reikalavimų taikymo analogiją žinybinių registrų atvejui.

4. *Vidaus administravimo informacinių sistemų* veiklos tiesiogiai nereglamentuoja jokie teisės aktai. Šiose sistemose tvarkomos informacijos saugumui užtikrinti taikytini Lietuvos Respublikos Vyriausybės patvirtinti *Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai*, tačiau, kaip ir žinybinių registrų atveju, informacijos saugumo reikalavimai, be informacinės sistemos gyvavimo ciklo reikalavimų, „pakimba ore“. Taigi galima konstatuoti, kad šios informacinių išteklių rūšies veikla yra silpniausiai reglamentuota, realiai nei gyvavimo ciklo, nei informacijos saugumo valdymo reikalavimai šiai informacinių išteklių rūšiai tinkamai netaikomi, jų funkcionavimas paliktas išteklių valdytojų valiai.

Apibendrinti informacinių išteklių gyvavimo ciklo ir saugumo valdymo reikalavimai pateikti 7 lentelėje. Pažymėtina, kad iki 2011 m. gruodžio 31 d. tik valstybės registrų funkcionavimas (tarp jų ir saugumo valdymas), buvo apibrėžtas įstatyminiu lygiu, o visų kitų informacinių išteklių funkcionavimą nustatė Lietuvos Respublikos Vyriausybė. Atsižvelgiant į tai, žinybinių registrų, valstybės informacinių sistemų ir vidaus administravimo sistemų valdytojams, kurie tiesiogiai nepavaldūs Lietuvos Respublikos Vyriausybei (Lietuvos Respublikos Seimas, Lietuvos Respublikos Prezidentūra, savivaldybių administracijos, teismai, prokuratūra ir pan.), gyvavimo ciklo ir saugumo reikalavimai buvo tik rekomendacinio pobūdžio arba iš viso neapibrėžti (7 lentelėje pažymėta žvaigždute).

Nuo 2012 metų sausio 1 dienos, 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 visuma“,* valstybės informacinių išteklių *„kūrimą, tvarkymą, valdymą, naudojimą, priežiūrą, sąveiką, planavimą, finansavimą ir saugą“* apibrėžė būtent šis įstatymas.

7 lentelė. Informacijos išteklių gyvavimo ciklo ir saugumo reikalavimų taikymas iki 2011 gruodžio 31 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
		Rekomenduojamas*	Rekomenduojamas*	
Saugumas	Privalomas	Privalomas	Privalomas	Privalomas
		Rekomenduojamas*	Rekomenduojamas*	Rekomenduojamas*

Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme taip buvo apibrėžtos šios naujos valstybės informacinių išteklių rūšys:

„1) ypatingos svarbos valstybės informaciniai ištekliai. Juos sudaro visai valstybei svarbi informacija, apdorojama valstybės informacinėse sistemose ir pagrindiniuose valstybės registruose, ir ją apdorojančios valstybės informacinės sistemos ir pagrindiniai valstybės registrai;

2) svarbūs valstybės informaciniai ištekliai. Juos sudaro kelioms institucijoms svarbi informacija, apdorojama valstybės informacinėse sistemose ir valstybės registruose, ir ją apdorojančios valstybės informacinės sistemos ir valstybės registrai;

3) žinybinės svarbos valstybės informaciniai ištekliai. Juos sudaro vienai institucijai svarbi informacija, apdorojama valstybės informacinėse sistemose ir žinybiniuose registruose, ir ją apdorojančios valstybės informacinės sistemos ir žinybiniai registrai;

4) kiti valstybės informaciniai ištekliai. Juos sudaro informacija, kurią valdo institucija, atlikdama vidaus administravimo funkcijas, apdorojama

kitomis informacinėse sistemose ir šią informaciją apdorojančios informacinės sistemos. Šiame punkte minimų informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarką nustato Lietuvos Respublikos Vyriausybės įgaliotos institucijos“.

Apibrėžus valstybės informacinių išteklių gyvavimo ciklą ir jų saugumo užtikrinimą įstatyminiu lygiu, šie reikalavimai tapo privalomi visam Lietuvos viešajam sektoriui, tačiau vidaus administravimo informacinėms sistemoms (*Lietuvos Respublikos valstybės informacinių išteklių įstatyme* dar įvardinamoms kaip *„kiti valstybės informaciniai ištekliai“*) gyvavimo ciklo reikalavimai vis dar nėra apibrėžti, o įstatymo straipsnis, nustatantis valstybės informacinių išteklių saugą, vidaus administravimo informacinėms sistemoms netaikomas. Pažymėtina, kad *Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme*, naudojant informacijos, sudarančios valstybės informacinius išteklius, svarbos sąvoką, įvestos naujos informacinių išteklių rūšys. Remiantis šia klasifikacija, minėtame įstatyme nustatyti specialūs reikalavimai valstybės institucijoms, valdančioms ypatingos svarbos valstybės informacinius išteklius (rengti *„informacinių technologijų plėtros plano projektą“*, tokioms sistemoms *„ne rečiau kaip kartą per trejus metus atliekamas informacinių technologijų auditas“*), taip pat išskirti specialūs gyvavimo ciklo reikalavimai informacinėms sistemoms, kuriose valdoma informacija svarbi visai valstybei arba kelioms institucijoms, tačiau, remiantis informacijos svarbos kriterijumi, jokie specialūs informacijos saugumo valdymo reikalavimai šiame įstatyme nenustatomi. Taip pat galima pastebėti, kad aptartoms įstatymo nuostatoms įgyvendinti reikalingi teisės aktai, pavyzdžiui, informacijos svarbos įvertinimo tvarka, kriterijai ir kita, vis dar nepatvirtinti.

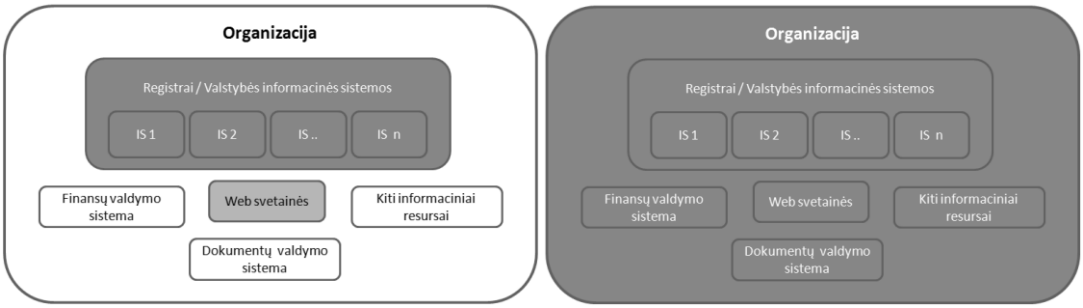
Taigi nuo 2012 m. sausio 1 d. informacijos saugumo reikalavimai privalomai taikomi platesniam Lietuvos viešojo sektoriaus subjektų ratui, tačiau vidaus administravimo sistemų valdytojams, kurie nėra tiesiogiai pavaldūs Lietuvos Respublikos Vyriausybei, informacijos saugumo valdymo reikalavimai nėra privalomi (8 lentelė).

8 lentelė. Informacijos išteklių gyvavimo ciklo ir saugumo reikalavimų taikymas nuo 2012 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*

Apibendrinant galima pastebėti, kad nors nuo 2012 m. sausio 1 d. informacijos saugumo reikalavimai privalomai taikomi platesniam Lietuvos viešojo sektoriaus subjektų, valdančių informacinius išteklius, ratui, tačiau tebėra aktualus tikslas – sukurti sąlygas, kad visiems viešojo sektoriaus informacijos ištekliams būtų taikomi informacijos saugumo reikalavimai (21 paveikslas).

Atsižvelgiant į tai, kad vidaus administravimo informacinių sistemų veikla nėra reglamentuota, sunku numatyti, ar tai yra spraga užtikrinant informacijos saugumą Lietuvos valstybės institucijose ir (jei taip) koks šios potencialios spragos mastas. Tiksliausias šaltinis problemai identifikuoti – kiekybinių tyrimų metodų pasitelkimas. Atliekant empirinio tyrimo sudedamąja dalimi numatytą institucijų anketinę apklausą, į apklausos anketą įtrauktini atitinkami klausimai, kurie leistų nustatyti vidaus administravimo sistemų naudojimo mastus bei ar valstybės institucijos, valdančios šiuos informacinius išteklius, taiko rekomenduojamus informacijos saugumo valdymo reikalavimus.



21 pav. Esama situacija (kairėje) ir siekiama situacija (tamsi spalva vaizduoja informacijos saugumo reikalavimų taikymo objektą, sudaryta autoriaus).

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 juos <...> nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, sugadinimo, atskleidimo, neteisėto pasisavinimo, paskelbimo, pateikimo ar kitokio panaudojimo, taip pat nuo bet kokio kito neteisėto tvarkymo“*.

Lyginant šią įstatymo nuostatą su disertacijoje aptartų informacijos saugumo valdymo tikslų (konfidencialumo, vientisumo ir prieinamumo) turiniu, galima daryti išvadą, kad galiojantys reikalavimai apima tik du iš trijų informacijos saugumo valdymo tikslų, t. y. Lietuvos valstybės institucijoms, valdančioms valstybės informacinius išteklius, įstatyminiu lygiu reikalavimas užtikrinti informacijos prieinamumą neįtvirtintas (9 lentelė). Išanalizavus žemesnės teisinės galios informacijos saugumo valdymo norminių dokumentų turinį (Vyriausybės patvirtintus *Bendruosius elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimus,* vidaus reikalų ministro nustatytus *Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techninius saugos reikalavimus* (disertacijos 4 priedo 2 ir 3 lentelės)), informacijos prieinamumo užtikrinimo reikalavimas aptiktas

tik techniniuose, Lietuvos Respublikos vidaus reikalų ministro patvirtintuose saugos reikalavimuose.

9 lentelė. Informacijos saugumo valdymo tikslai, galiojantys Lietuvos valstybės institucijoms (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.

Aptarti šaltiniai, formuojantys informacijos saugumo politiką valstybės lygmenyje, nustato ir atitinkamus informacijos saugumo politikos reikalavimus instituciniam lygmeniui. Apibendrintai vertinant informacijos saugumo valdymo politiką institucijų lygmenyje, remiantis *Bendrųjų elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimų* nuostatomis, Lietuvos valstybės institucijos informacijos saugumo politiką turi išdėstyti 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.

Siekiant įvertinti, ar (ir kaip) Lietuvos valstybės institucijos laikosi šių reikalavimų, į kiekybinio tyrimo anketa įtrauktini atitinkami klausimai.

3.2.2. Informacijos saugumo valdymo strategija Lietuvos valstybės institucijose

Analizuojant Lietuvos valstybės institucijoms galiojančią informacijos saugumo valdymo strategiją išskirti 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 (2002)*. Remiantis šia metodika ir dokumentų turinio analizei išskirtais šaltiniais (disertacijos 3 priedas), identifikuoti aktualūs informacijos saugumo valdymo strateginiai dokumentai.

Aukščiausio lygmens Lietuvos Respublikos strateginio dokumento, numatančio šalies vystymosi prioritetus ir perspektyvas iki 2030 m., – *Valstybės pažangos strategijos (2012)* projekte, nors yra nuoroda į Nacionalinio saugumo strategiją, – informacijos saugumas tiesiogiai neišskirtas. Paminėtina, kad šis dokumentas tebėra svarstymo stadijoje.

Analizuojant kitų strateginių šalies dokumentų turinį ir tiriant sąsajas su informacijos saugumu, paminėtina 2012 metais Lietuvos Respublikos Seimo patvirtinta *Nacionalinio saugumo strategija (2012)*. Šioje strategijoje informacijos ir kibernetinis saugumas minimi tarp pirmaeilių Lietuvos nacionalinio saugumo interesų. Strategijoje koncentruotai ir aiškiai išdėstyti tikslai – „*visapusiškai stiprinti nacionalinės kibernetinės erdvės saugumą, užtikrinti elektroninės informacijos konfidencialumą, vientisumą ir prieinamumą*“. Šiems tikslams įgyvendinti numatoma kurti „*nacionalinę koordinavimo sistemą kibernetinio saugumo srityje*“, tobulinti „*nacionalinį elektroninės informacijos saugos (kibernetinio saugumo) srities teisinį reglamentavimą*“, dalyvauti „*tarptautinėse teisinio reglamentavimo tobulinimo iniciatyvose*“, stiprinti „*nacionalinius gebėjimus reaguoti į elektroninės informacijos saugos incidentus (įskaitant kibernetines atakas) nacionalinėje kibernetinėje erdvėje ir likviduoti jų padarinius*“, „*užtikrinti nacionaliniam*

saugumui strategiškai svarbios informacinės infrastruktūros saugą“ bei „*elektroninės informacijos saugos (kibernetinio saugumo) kultūrą*“, plėtojant „*bendradarbiavimą tarp viešojo, privataus, nevyriausybinio ir mokslo sektorių bei su tarptautiniais partneriais*“. Galima pastebėti, kad šioje strategijoje aiškiai identifikuoti svarbiausi strateginio lygmens trūkumai, valdant informacijos saugumą, ir nustatyti prioritetiniai tikslai jiems šalinti. Šių tikslų įgyvendinimas deleguotas Lietuvos Respublikos Vyriausybei, taigi sėkmingas iškeltų tikslų įgyvendinimas tiesiogiai priklauso nuo Vyriausybės sugebėjimo įtvirtinti atitinkamas priemones savo ir pavaldžių valstybės institucijų priemonių planuose bei užtikrinti tinkamą šių planų įgyvendinimo kontrolę.

Analizuojant su informacijos saugumo valdymu susijusius Lietuvos Respublikos Vyriausybės patvirtintus kitus strateginius dokumentus, pažymėtinas siekis „*užtikrinti elektroninės erdvės saugumą ir patikimumą, didinti gyventojų ir įmonių pasitikėjimą elektronine erdve*“, įtvirtintas tarp *Lietuvos informacinės visuomenės plėtros 2011–2019 metų programos (2011)* prioritetų, tačiau analizuojant šios programos įgyvendinimo priemones, akcentuojamos tik siauros *elektroninės tapatybės patikimumo* ir *elektroninių dokumentų autentiškumo, vientisumo ir išsaugojimo* problemos.

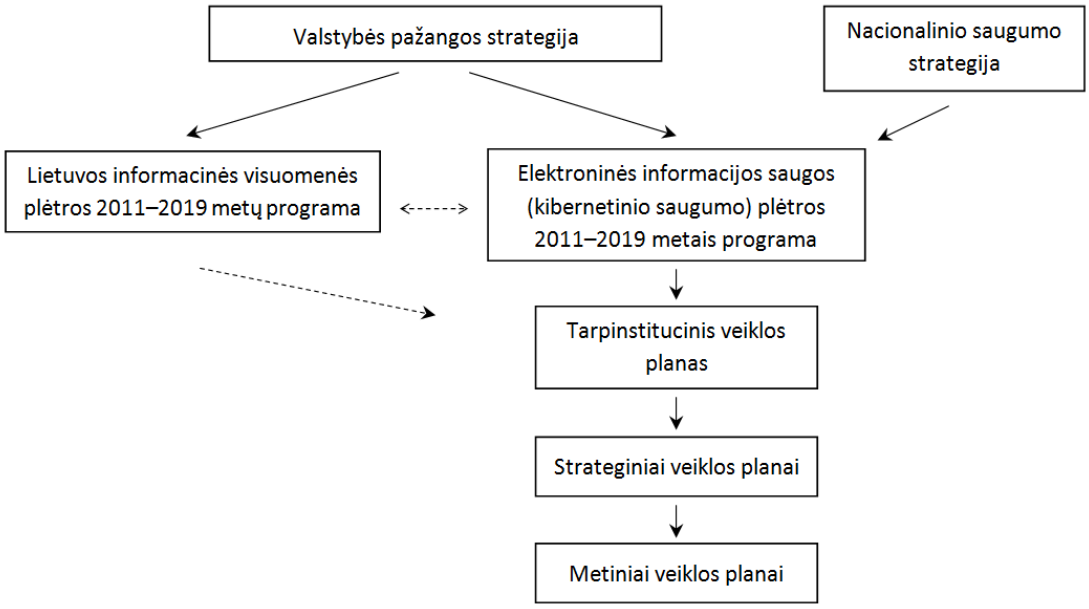
Detaliai informacijos saugumo tikslai, uždaviniai ir jų įgyvendinimo vertinimo kriterijai nustatyti 2011 metų birželio 29 d. Lietuvos Respublikos Vyriausybės patvirtintoje *Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programoje*, kurios tikslas – apimti ne tik viešąjį, bet ir visus kitus sektorius. Šios programos uždavinių įgyvendinimo vertinimo kriterijų reikšmės nustatytos 2015 ir 2019 metams, tarpinius uždavinius ir jų įgyvendinimo vertinimo kriterijus pavesta nustatyti atitinkamoms atsakingoms institucijoms savo planuose. 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[11]. Jokie kiti detalesni

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

tarpinstituciniai veiklos planai dar nepatvirtinti, todėl šiuo metu nėra galimybių atlikti detalesnės dokumento įgyvendinimo analizės ir vertinimo.

Vadovaujantis *Strateginio planavimo metodikoje* nustatyta planavimo dokumentų schema (disertacijos 6 priedas) ir išanalizuotais strateginiais informacijos saugumo valdymo dokumentais, galima sudaryti valstybės lygmens strateginių informacijos saugumo dokumentų schemą (22 paveikslas).

Apibendrinant informacijos saugumo valdymo strategiją formuojančių dokumentų turinio analizę, galima konstatuoti, kad svarbiausi valstybės lygmens strateginiai informacijos saugumo valdymo dokumentai yra *Nacionalinio saugumo strategija* ir *Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programa.* Šie dokumentai nustato strateginius informacijose saugumo valdymo tikslus ir uždavinius, nurodo pagrindines jų įgyvendinimo kryptis, tačiau pastebėtas detalių įgyvendinimo planų trūkumas.



22 pav. Strateginių informacijos saugumo valdymo dokumentų schema (sudaryta autoriaus).

Vertinant institucijų lygmenį, galiojantys teisės aktai nenustato pareigos valstybės institucijoms rengti specialius strateginius informacijos saugumo valdymo dokumentus.

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 šio įstatymo tik *rekomendacinė* nuostata, kad *„organizuojant valstybės informacinių išteklių saugą, rekomenduojama vadovautis pripažintų standartizacijos organizacijų ir standartizacijos institucijų priimtais ir paskelbtais standartais“*, neleidžia vienareikšmiškai teigti, ar Lietuvos viešajame sektoriuje privaloma taikyti priemones, visapusiškai 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, apibrėžtų informacijos saugumo valdymo dimensijų kontekste, turėtų remtis šių dimensijų turinį gretinant su Lietuvos Respublikos Vyriausybės patvirtintų *Bendrųjų elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimų* turinio nuostatomis.

Minėtų dokumentų turinio analizei pasitelktas disertacijos 1.1.4 poskyryje aptartas informacijos saugumo valdymo dimensijų turinys (informacijos saugumui aktualūs aspektai, kuriuos apjungia dimensijos) ir *Bendrųjų elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimų* turinio nuostatos. Atlikus turinio analizę galima teigti, kad *Bendrųjų elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimų* turinys turi daug bendrumų su informacijos saugumo valdymo dimensijų turiniu, tačiau galima identifikuoti šiuos pagrindinius reikalavimų turinio trūkumus: strateginės

dimensijos kontekste – neapimami ekonominiai aspektai, techninės dimensijos – neišryškinti kriptografijos aspektai (galima numanyti sąsajas su reikalavimu duomenų perdavimui tinklais), žmogiškosios dimensijos – pastebimas psichologinių ir etinių aspektų įtraukties trūkumas. Analizės rezultatai pateikti 10 lentelėje.

10 lentelė. Informacijos saugumo dimensijų lyginamoji lentelė (sudaryta autoriaus).

Informacijos saugumo valdymo priemonė	**Integralus informacijos saugumo valdymo modelis**	**Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai**
Saugumo dimensijos	Strateginė (administraciniai, organizaciniai, valdymo, ekonominiai, standartų, teisiniai, gerųjų praktikų ir kiti aspektai);	Saugumo tikslai, organizavimas, prioritetai, duomenų svarba ir pagrindiniai reikalavimai; teisės aktų sąrašas; informacijos kategorijų sąrašas; duomenų vientisumo pažeidimų fiksavimo ir pažeistų duomenų atkūrimo tvarka; veiklos tęstinumo valdymas; incidentų tyrimo tvarka; rizikos vertinimas; planų tikslinimas; prieigos ir kontrolės tvarka;
	technologinė (informacinių technologijų, techninių ir programinių priemonių, matematiniai, kriptografiniai ir kiti aspektai);	techninių ir fizinių saugos priemonių aprašymas; perdavimo tinklais reikalavimai;
	žmogiškoji (saugumo kultūros, etiniai, kompetencijų, mokymų, psichologiniai ir kiti aspektai).	personalo kvalifikaciniai reikalavimai; supažindinimo su saugos dokumentais principai; atsakomybė už pažeidimus; naudotojų mokymas.
Saugumo procesų ciklišKumo valdymas	Planuoti, daryti, tikrinti, veikti	Reikalavimai dokumentų peržiūrai, sistemos pokyčių valdymas, periodinis atitikties ir rizikos vertinimas.

Informacijos saugumo valdymo procesų ciklas, reagavimas į aplinkos pokyčius

Valstybės lygmeniu informacijos išteklių valdymo procesų ciklas analizuotas nagrinėjant informacijos saugumo valdymo objektą ir informacijos išteklių funkcionavimo (gyvavimo ciklo) aplinką (7 ir 8 lentelės), t. y. valdymo procesai nustatyti valstybės registrams, valstybės informacinėms sistemoms ir žinybiniams registrams, tačiau vis dar neapibrėžti vidaus administravimo informacinėms sistemoms. Institucijų lygmeniu Lietuvos valstybės institucijos įpareigotos atlikti rizikos analizę ir atitikties vertinimą, nuolat peržiūrėti informacijos saugumo valdymą reglamentuojančius dokumentus ir valdyti sistemos pokyčius (10 lentelė, eilutė „Saugumo procesų ciklišKumo valdymas“). Tačiau tiek vienu, tiek ir kitu atveju reikalavimo įgyvendinimo kontrolės tvarka neapibrėžta, todėl apibendrintoms išvadoms, kaip šių reikalavimų laikosi valstybės institucijos, formuluoti tikslinga atitinkamus klausimus įtraukti į tolesnius tyrimus.

3.2.3. Informacijos saugumo valdymo auditas Lietuvos valstybės institucijose

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

Lietuvos Respublikos aukščiausioji valstybinio audito institucija yra Valstybės kontrolė. Šios institucijos pagrindinė funkcija – prižiūrėti, ar teisėtai ir efektyviai valdomi ir naudojami valstybės finansai ir kitas turtas bei kaip vykdomas valstybės biudžetas.

Valstybės kontrolė, įgyvendindama savo funkcijas, atlieka valstybinį auditą, kuris yra dviejų rūšių – finansinis (teisėtumo) ir veiklos auditas. Finansinio (teisėtumo) audito tikslas – įvertinti, ar audituojamas subjektas teisingai tvarko savo finansus, ar pateikia teisingas finansines ir kitas

ataskaitas, taip pat ar valstybės lėšos ir kitas turtas valdomas ir naudojamas teisėtai, taip, kaip numatyta įstatymuose. Veiklos auditu siekiama įvertinti, ar audituojamas subjektas vadovaujasi ekonomiškumo, efektyvumo ir rezultatyvumo principais, ar valstybės lėšos ir turtas naudojamas taupiai ir racionaliai.

Valstybės kontrolė yra atlikusi ne vieną auditą, kurio metu buvo vertinamas ir informacijos saugumo valdymas Lietuvos valstybės institucijose. Paskutinis auditas tiesiogiai skirtas informacijos saugumo valdymo strateginiam vertinimui – *Išankstinio tyrimo ataskaita. Strateginės informacijos sauga (2009)*. Šio išankstinio tyrimo metu buvo nustatytos dvi pagrindinės informacijos saugumo valdymo 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)“. (Išankstinio tyrimo ataskaita. Strateginės informacijos sauga, 2009).

Nors Valstybės kontrolė šį auditą vykdė 2009 metais, dar iki patvirtinant aptartą *Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programą*, po kurios priėmimo planuotas pakartotinis auditas vis dar neatliktas, vertinant Valstybės kontrolės išvadas empirinio tyrimo kontekste, jos tebėra aktualios. Taip pat pažymėtina, kad Valstybės kontrolė nėra įtraukta tarp institucijų, atsakingų už *Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos* įgyvendinimą.

Informacijos saugumo auditas iš dalies apibrėžiamas *Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo* nuostatomis, kad

Vidaus reikalų ministerija *„organizuoja informacinių technologijų priemonių valdymo ir saugos vertinimą“* ir *„atlieka saugos reikalavimų laikymosi priežiūrą“* bei, remiantis įstatymo 14 straipsnio nuostatomis, 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 tvarka šioms įstatymo nuostatoms įgyvendinti ir kontroliuoti nepatvirtinta, informacijos saugumo valdymo audito priemonių nenumatyta ir *Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos* įgyvendinimo priemonių plane.

Vertinant institucinį lygmenį, pažymėtina *Bendrųjų elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimų* nuostata, kad saugos politikos dokumentus valstybės institucijos su Vidaus reikalų ministerija privalo derinti prieš juos patvirtindamos. Taip pat *„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 instituciniame lygmenyje, tačiau atkreiptinas dėmesys, kad procedūra, kaip turėtų būti kontroliuojamas nuolatinis šių reikalavimų įgyvendinimas, nenumatyta.

Šių įžvalgų aktualumą galima pagrįsti nagrinėjant Valstybės kontrolės auditų, kuriuose vertintas ir informacijos saugumo valdymas Lietuvos valstybės institucijose (auditų sąrašas pateiktas disertacijos 1 priede), išvadas. Visuose audituose Valstybės kontrolė atkreipia dėmesį ne tik į formalius

galiojančių informacijos saugumo reikalavimų neatitikimus, pavyzdžiui, turinio spragas perkeliant galiojančius informacijos saugumo reikalavimus į vidines institucijų informacijos saugumo valdymo tvarkas, bet ir į esmines problemas realiai įgyvendinant tvarkose nustatytas procedūras. Dauguma vertintų valstybės institucijų nesilaiko formalizuotų informacijos saugumo reikalavimų, nėra užtikrinama šių reikalavimo įgyvendinimo kontrolė.

Atsižvelgiant į išdėstytas aplinkybes, galima teigti, kad institucijų lygmenyje periodinis informacijos saugumo audito privalomumas nustatytas, valstybės lygmenyje nuostata dėl periodinio informacijos saugumo audito yra įtvirtinta įstatymu, tačiau šių reikalavimų įgyvendinimo ir kontrolės tvarka nėra užtikrinta. Taigi aktualu ištirti, kaip laikomasi privalomų reikalavimų, kurių įgyvendinimas nėra kontroliuojamas, ir į tolesnius tyrimus įtraukti atitinkamus klausimus.

3.2.4. Informacijos saugumo valdymo veikėjai Lietuvos valstybės institucijose

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

Išanalizavus Lietuvos Respublikos ministerijų[12] ir kitų institucijų nuostatus ir vykdomas funkcijas, vertinant informacijos saugumo valdymo organizavimą ir koordinavimą galima išskirti šiuo metu didžiausią įtaką užtikrinant informacijos saugumą turinčias institucijas: Lietuvos Respublikos vidaus reikalų ministeriją (pagrindinės funkcijos informacijos saugumo kontekste – valstybės institucijų informacijos saugumo politikos formavimas), Lietuvos Respublikos susisiekimo ministeriją (ryšių saugumo politikos formavimas), Lietuvos Respublikos teisingumo ministeriją (asmens duomenų apsaugos politikos formavimas), Ryšių reguliavimo tarnybą (ryšių operatorių

[12] Lietuvos Respublikos ministerijos // http://www.lrv.lt/lt/vyriausybe/apie-vyriausybe/ministerijos/, (žiūrėta 2012 m. kovo 2 d.)

priežiūra, saugumo incidentų stebėsena), Policijos departamentą prie Lietuvos Respublikos vidaus reikalų ministerijos (elektroninių nusikaltimų tyrimas). Valstybės institucijų veiklai koordinuoti dar 2006 m. Lietuvos Respublikos Vyriausybė iš minėtų atsakingų valstybės institucijų atstovų sudarė nuolatinę Elektroninės informacijos saugos koordinavimo komisiją[13], kurios veiklai vadovauja Vidaus reikalų ministerijos atstovas. Į šios komisijos sudėtį taip pat buvo įtraukti Ministro Pirmininko tarnybos atstovas, Asmens duomenų apsaugos inspekcijos atstovas ir Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos susisiekimo ministerijos atstovas, kurį vėliau pakeitė Lietuvos Respublikos krašto apsaugo ministerijos atstovas. Sudarytai komisijai pavesta koordinuoti institucijų veiklą įgyvendinant informacijos saugumo užtikrinimo darbus ir vykdomus projektus, skatinti informacijos saugumo kultūros kėlimą, analizuoti informacijos saugumo tendencijas ir pavojus, bendradarbiauti su privačiu sektoriumi, teikti rekomendacijas ir sprendimų projektus Lietuvos Respublikos Vyriausybei. Vertinant Elektroninės informacijos saugos koordinavimo komisijai pavestas funkcijas galima teigti, kad komisija vykdė koordinacines, rekomendacines ir stebėsenos funkcijas, tačiau neturėjo įgaliojimų tiesiogiai duoti nurodymų ar priimti sprendimų, privalomų kokiems nors ūkio subjektams. Vertinant komisijos veiklą, pažymėtina, kad ši komisija atliko plačią esamos situacijos analizę ir padėjo pamatus naujai informacijos saugumo strategijai parengti. Vėliau buvo sudarytos net kelios specialios darbo grupės[14], įtraukiant ir kitų institucijų, pavyzdžiui, Valstybės saugumo departamento atstovus, kurios parengė naują strateginį dokumentą – *Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programą*. Ši programa buvo patvirtinta Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. sprendimu. Už atskirų *Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–*

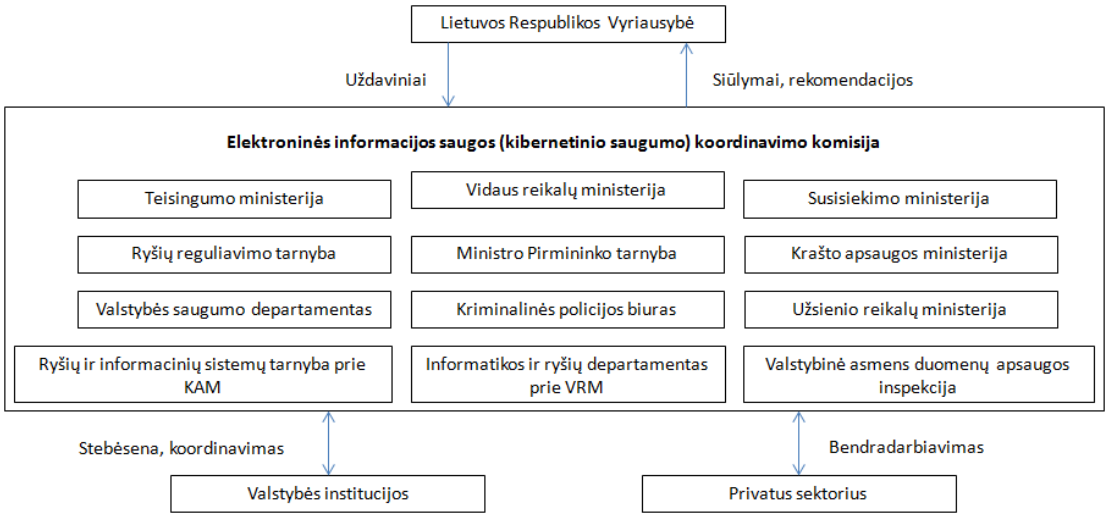
[13] Lietuvos Respublikos Vyriausybės nutarimas // http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=288880&p_query=&p_tr2=, (žiūrėta 2012 m. kovo 2 d.)
[14] Ministro Pirmininko sprendimai dėl Darbo grupės sudarymo // http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=322412&p_query=kibernetinio&p_tr2=2; http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=358836&p_query=informacijos%20saugos&p_tr2=2, (žiūrėta 2012 m. kovo 2 d.)

2019 metais programos uždavinių įgyvendinimą paskirtos atsakingomis – Vidaus reikalų, Krašto apsaugos, Susisiekimo, Švietimo ir mokslo, Ūkio, Energetikos bei Finansų ministerijos, Valstybinė duomenų apsaugos inspekcija, Ryšių reguliavimo tarnyba, Policijos departamentas prie Vidaus reikalų ministerijos, Ministro Pirmininko tarnyba, Lietuvos mokslo ir studijų institucijų kompiuterinio tinklo LITNET taryba, Valstybės saugumo departamentas.

Šios Programos koordinatore paskirta Lietuvos Respublikos vidaus reikalų ministerija. Tarpinstituciniam bendradarbiavimui stiprinti 2012 metų balandžio 25 d. Lietuvos Respublikos Vyriausybė savo sprendimu[15] dar kartą atnaujino minėtos Elektroninės informacijos saugos koordinavimo komisijos sudėtį, ją pavadino Elektroninės informacijos saugos (kibernetinio saugumo) koordinavimo komisija ir į jos sudėtį papildomai įtraukė Užsienio reikalų ministerijos bei Valstybės saugumo departamento atstovus (23 paveikslas).

Vertinant institucijoms pavestas informacijos saugumo valdymo koordinavimo funkcijas, galima konstatuoti, kad Lietuvoje šios funkcijos decentralizuotos ir atsakomybė už pavienes sritis formaliai išdalinta tarp kelių institucijų. Pagrindine informacijos saugumo valdymo koordinatore paskirta Vidaus reikalų ministerija, tarpinstituciniam darbui organizuoti ir koordinuoti taip pat įkurta Elektroninės informacijos saugos (kibernetinio saugumo) koordinavimo komisija. Taigi už tam tikras informacijos saugumo valdymo funkcijas atsakingų institucijų kompetencijos nėra persidengiančios, tačiau teisės aktais nėra aiškiai apibrėžti šių institucijų tarpusavio ryšiai, pavyzdžiui, kieno atsakomybės sritis – kritinės informacinės infrastruktūros saugumas, apimantis ir informacines sistemas, ir ryšių tinklus, priklausančius tiek valstybei, tiek ir privačiam sektoriui. Informacijos saugumo priežiūros, reguliavimo ir teisėkūros procesuose taip pat dalyvauja ir kitos valstybės institucijos (jų funkcijų, vykdomos veiklos, tarpusavio santykių bei pavaldumo klausimai nėra išspręsti).

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



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

Siekiant įvertinti institucijų galimybes vykdyti pavestas informacijos saugumo valdymo koordinacines funkcijas, atlikta šių institucijų žmogiškųjų išteklių analizė. Analizės metu išnagrinėti Elektroninės informacijos saugos (kibernetinio saugumo) komisijos sudėtyje esančių institucijų ir jų padalinių, tiesiogiai atsakingų už informacijos saugumo koordinavimo funkcijų vykdymą, nuostatai ir struktūra bei šiuose padaliniuose dirbančių darbuotojų pareigybių aprašymai. Ši analizė leido identifikuoti žmogiškuosius išteklius, dedikuotus informacijos saugumo valdymo koordinavimui.

Išanalizavus Lietuvos Respublikos vidaus reikalų ministerijos (VRM) administracijos padalinių[16] nuostatus ir jais patvirtintas šių padalinių funkcijas, išskirtas Elektroninės valdžios politikos skyrius, kurio nuostatuose tiesiogiai įrašytos atsakomybės už informacijos saugumą: *„formuoti valstybės politiką informacinių technologijų saugos srityje, organizuoti, koordinuoti ir kontroliuoti jos įgyvendinimą*“. Pažymėtina, kad Lietuvos Respublikos vidaus reikalų ministras 2012 m. lapkričio 5 d., patvirtino šio skyriaus nuostatų naują redakciją. Vertinant šių nuostatų turinį pastebėta, kad naujoje redakcijoje didžioji dalis skyriaus funkcijų sietinos su tiesiogiai informacijos saugumo

[16] Lietuvos Respublikos vidaus reikalų ministerija: Ministerijos administracijos padaliniai // http://www.vrm.lt/go.php/lit/Struktura-ir-kontaktai/12/5, (žiūrėta 2012 m. rugsėjo 21 d.)

valdymu (Lietuvos Respublikos vidaus reikalų ministerijos Elektroninės valdžios politikos skyriaus nuostatai, 2011, 2012). Iš viso šiame skyriuje dirba 9 darbuotojai, tačiau išnagrinėjus šio skyriaus valstybės tarnautojų funkcijas[17], rastas tik vienas valstybės tarnautojas, kurio funkcijos tiesiogiai susijusios su informacijos saugumo valdymu, bei vienas valstybės tarnautojas, kuriam saugumo koordinavimo funkcijos priskirtos kartu su kitomis (skyriaus vadovas).

Informatikos ir ryšių departamente prie Lietuvos Respublikos vidaus reikalų misterijos (IRD prie VRM) identifikuotas Saugos skyrius[18], 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 valdymo koordinavimu.

Nagrinėjant atitinkamas Lietuvos Respublikos susisiekimo ministerijos (SM) funkcijas, pastebėtas Informacinės visuomenės politikos departamento Elektroninių ryšių skyrius[19]. Šiame skyriuje išskirti du valstybės tarnautojai; vieno iš jų vykdomos funkcijos siejasi su dalyvavimu koordinuojant informacijos saugumo užtikrinimą bendrąja prasme, kito susijusios su informacijos saugumu el. ryšių srityje.

Nagrinėjant Lietuvos Respublikos teisingumo ministerijos (TM) administracijos padalinių nuostatus ir valstybės tarnautojams pavestas vykdyti funkcijas, išskirtas Registrų departamento Registrų teisinio reguliavimo skyrius[20]. Šiame skyriuje dirba 6 valstybės tarnautojai, iš kurių penkiems viena iš pavestų funkcijų yra susijusi su asmens duomenų apsauga, ir vienas valstybės tarnautojas, kurio funkcijos tiesiogiai siejasi su asmens duomenų apsauga.

[17] Lietuvos Respublikos vidaus reikalų ministerijos Elektroninės valdžios politikos skyrius // http://www.vrm.lt/go.php/lit/ELEKTRONINES-VALDZIOS-POLITIKOS-SKYRIUS/15, (žiūrėta 2012 m. rugsėjo 21 d.)
[18] Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos // http://www.ird.lt/viewpage.php?page_id=12, (žiūrėta 2012 m. rugsėjo 5 d.)
[19] Lietuvos Respublikos susisiekimo ministerija // http://www.transp.lt/lt/struktura_ir_kontaktai/kontaktai/ministerijos_kontaktai, (žiūrėta 2012 m. birželio 10 d.)
[20] Lietuvos Respublikos teisingumo ministerija // http://www.tm.lt/struktura/kontaktineinfo/12, (žiūrėta 2012 m. birželio 10 d.)

Ryšių reguliavimo tarnyboje (RRT), pagal interneto svetainėje skelbiamą informaciją[21], įkurtas specialus struktūrinis padalinys – Tinklų ir informacijos saugumo departamentas, kuriame dirba septyni darbuotojai; trijų iš jų funkcijos priskirtinos tiesiogiai informacijos saugumo problemoms spręsti; dar dviejų tik iš dalies.

Valstybinėje asmens duomenų apsaugos inspekcijoje (VDAI) pagal etatų sąrašą ir paskelbtus pareigybių aprašymus[22] buvo rasti trys valstybės tarnautojai, kurių viena iš funkcijų – asmens duomenų, apdorojamų informacinėmis technologijomis, apsauga.

Policijos departamento Kriminalinės policijos biure galima išskirti specialią Nusikaltimų elektroninėje erdvėje tyrimo valdybą[23], tačiau jos etatų sąrašas ir konkrečios funkcijos internete neskelbiamos.

Lietuvos Respublikos Ministro Pirmininko tarnybos etatų sąrašuose[24] nepavyko atskleisti padalinio ar valstybės tarnautojo, atsakingo už informacijos saugumo valdymo koordinavimą. 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.

Susisteminti žmogiškųjų išteklių, atsakingų už informacijos saugumą, skaičiai pateikti 11 lentelėje. Žmogiškieji ištekliai išskirti 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 valdymo organizavimo ir koordinavimo funkcijas, galima teigti, kad formaliai funkcijos yra padalintos tarp kelių pagrindinių

[21] 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.)
[22] Valstybinė duomenų apsaugos inspekcija // http://www.ada.lt/index.php?lng=lt&action=page&id=57 , (žiūrėta 2012 m. birželio 10 d.)
[23] Policijos departamentas prie VRM » Kriminalinės policijos biuras // http://www.policija.lt/index.php?id=7441&ou=3053, (žiūrėta 2012 m. birželio 10 d.)
[24] LR Vyriausybė - Ministro Pirmininko tarnybos kontaktai // http://www.lrv.lt/lt/kontaktai/ministro-pirmininko-tarnyba/ , (žiūrėta 2012 m. birželio 10 d.)

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 valdymą Lietuvos valstybės institucijose. Šią išvadą pagrįsti, empirinio tyrimo sudėtine dalimi numatyto ekspertu interviu metu, tikslinga pateikti atitinkamus klausimus ekspertams.

11 lentelė. Žmogiškųjų išteklių, atsakingų už informacijos saugumo valdymo funkcijų vykdymo koordinavimą Lietuvos valstybės institucijose, skaičius (sudaryta autoriaus).

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

Vadovaujantis *Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu* ir kitais aptartais teisės aktais, instituciniame lygmenyje pagrindinis informacijos saugumo valdymo veikėjas – saugos 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. Ištirti, kaip valstybės institucijos laikosi šio reikalavimo, t. y. ar valstybės institucijų vadovai yra paskyrę saugos įgaliotinius, į kiekybinio tyrimo anketą įtrauktinas atitinkamas klausimas.

3.2.5. Informacijos saugumo valdymo branda Lietuvos valstybės institucijose

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

Išanalizavus atrinktų šaltinių turinį, galima išskirti *Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programą,* kurioje 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. Šios spragos reikšmę tikslinga aptarti numatyto ekspertų interviu metu.

3.3. Dokumentų turinio analizės rezultatų aptarimas

Remiantis suformuota informacijos saugumo valdymo vertinimo prieiga, dokumentų turinio analizės metodu detaliai išanalizavus informacijos saugumo valdymo reikalavimus Lietuvos valstybės institucijoms ir kitus galiojančius su informacijos saugumo valdymu susijusius formalius dokumentus organizacijų ir valstybės lygmenyse, galima teigti:

1. Informacijos saugumo valdymo objektas Lietuvos valstybės institucijose – valstybės institucijų valdoma informacija, apdorojama valstybės ir žinybiniuose registruose, valstybės ir vidaus administravimo informacinėse sistemose (valstybės informaciniuose ištekliuose). Valstybės informacinių išteklių kūrimą, tvarkymą, valdymą, naudojimą, priežiūrą, sąveiką, planavimą, finansavimą ir saugą reglamentuoja *Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas* ir kiti poįstatyminiai aktai.

2. Lietuvos valstybės institucijų informacijos saugumo valdymo politika nustatyta *Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme* ir specializuotuose, Lietuvos Respublikos Vyriausybės patvirtintuose,

informacijos saugumo valdymo reikalavimuose. Reikalavimai šiuo metu tiesiogiai netaikomi vienai iš keturių valstybės informacinių išteklių rūšiai – vidaus administravimo informacinėms sistemoms. Aptarti reikalavimai remiasi rekomenduojamu tarptautinių informacijos saugumo valdymo standartų ir metodikų taikymu, tačiau tiesiogiai taikomi tik dviem iš trijų pagrindinių informacijos saugumo tikslų – informacijos konfidencialumui ir vientisumui, tačiau neapima informacijos prieinamumo (šis tikslas išryškintas tik techniniuose informacijos saugumo reikalavimuose).

3. Informacijos saugumo valdymo įgyvendinimą Lietuvos valstybės institucijose koordinuojančia institucija paskirta Lietuvos Respublikos vidaus reikalų ministerija, taip pat sudaryta nuolatinė Elektroninės informacijos saugos (kibernetinio saugumo) koordinavimo komisija. Pastebėtas su informacijos saugumo valdymo organizavimu ir koordinavimu sietinos atsakomybės decentralizavimas bei formalus paskyrimas kelioms valstybės institucijoms. Tačiau ištyrus valstybės institucijų, atsakingų už informacijos saugumo valdymo organizavimą ir koordinavimą, žmogiškuosius išteklius, paskirtus institucijai deleguotoms funkcijoms vykdyti, galima vienareikšmiškai konstatuoti, kad šie ištekliai nėra pakankami.

4. Lietuvos valstybės institucijų ilgalaikė informacijos saugumo strategija nustatyta dviejuose strateginiuose dokumentuose – *Nacionalinio saugumo strategijoje* ir *Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programoje*. Šie dokumentai nustato ilgojo ir vidutinio laikotarpio tikslus ir vertinimo kriterijus (pavyzdžiui, *Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programoje* numatyti siekiniai ir jų vertinimo kriterijai 2015 ir 2019 metams), tačiau artimojo laikotarpio veiksmai ir priemones detalizuojantys dokumentai šioms strategijoms įgyvendinti nepatvirtinti.

5. *Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programoje* numatyta, kad bus vertinamas informacinių sistemų valdytojų informacijos saugumo valdymo brandos lygis, tačiau

Lietuvos valstybės institucijoms informacijos saugumo brandos lygiai neapibrėžti, vertinimo sistema nenumatyta.

6. Ypatingos svarbos valstybės informacinių išteklių periodinis informacijos saugumo auditas yra įtvirtintas įstatymu, tačiau šios nuostatos įgyvendinimo tvarka ir kontrolė nėra užtikrinta.

7. Pagal teisės aktais įtvirtintus principus, Lietuvos viešajame sektoriuje, rengiant valstybinius strateginius dokumentus, vykdoma aplinkos analizė (rizikų vertinimas), tačiau nuolatinio pokyčių vertinimo ir reagavimo į juos proceso kontrolė neapibrėžta. Lietuvos valstybės institucijos įpareigotos nuolat peržiūrėti informacijos saugumo politikos dokumentus, tačiau kaip (ar) institucijos tai atlieka, kontrolės sistemoje taip pat nenumatyta.

Apibendrinti teorinio dokumentinio tyrimo rezultatai pateikti 12 lentelėje.

12 lentelė. Informacijos saugumo valdymo įrankių taikymas pagal vertinimo prieigą (sudaryta autoriaus).

Įrankis	**Valstybės lygmuo**	**Institucinis lygmuo**
Informacijos saugumo politika:	Informacijos saugumo politika apibrėžta Valstybės informacinių išteklių valdymo įstatyme ir Vyriausybės patvirtintuose reikalavimuose.	Informacijos saugumo politika apibrėžta Institucijos informacijos saugumo politikos dokumentuose (duomenų saugos nuostatuose).
Ar nustatytas informacijos saugumo valdymo objektas?	Informacijos saugumo valdymo objektas – Valstybės informaciniai ištekliai.	Institucijos valdomi valstybės informaciniai ištekliai.
Ar nustatyti informacijos saugumo tikslai?	Aiškiai nustatyti tikslai – informacijos konfidencialumo ir vientisumo užtikrinimas.	Aiškiai nustatyti tikslai – informacijos konfidencialumo ir vientisumo užtikrinimas, techniniuose reikalavimuose įtvirtintas ir prieinamumo tikslas.

Įrankis	Valstybės lygmuo	Institucinis lygmuo
Informacijos saugumo strategija:	Patvirtinta Nacionalinio saugumo strategija ir Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programa.	Institucijos neįpareigotos rengti specialios informacijos saugumo strategijos.
Ar nustatytos strateginės informacijos saugumo politikos įgyvendinimo kryptys, prioritetai ir uždaviniai?	Nustatytos įgyvendinimo kryptys, prioritetai ir uždaviniai su vertinimo kriterijais 2015 ir 2019 metams.	Kryptys ir prioritetai nustatomi Duomenų saugos nuostatuose ir kituose saugumo politiką įgyvendinančiuose dokumentuose.
Ar nustatytos strategijos įgyvendinimo priemonės, ar šios priemonės apima strateginę, žmogiškąją ir technologinę dimensijas?	Detalių priemonių planų ir jų vertinimo kriterijų nėra, tačiau Bendrųjų elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimų turinys iš esmės atitinka informacijos saugumo valdymo dimensijų turinį.	Institucijos, rengdamos vidinius dokumentus, turi vadovautis Bendraisiais elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimais, kurių turinys iš esmės atitinka informacijos saugumo valdymo dimensijų turinį.
Ar apibrėžtas informacijos saugumo procesų ciklas, užtikrinamas reagavimas į aplinkos pokyčius?	Rengiant strateginius informacijos saugumo dokumentus atliekama aplinkos analizė, tačiau informacijos saugumo procesų ciklas ir nuolatinis aplinkos pokyčių vertinimas nenumatytas.	Teisės aktais nustatyta, kad saugos politikos dokumentai valstybės institucijoje turi būti peržiūrimi ne rečiau kaip kartą per metus, atlikus rizikos analizę ar saugos atitikties vertinimą arba valstybės institucijoje įvykus esminiams organizaciniams, sisteminiams ar kitiems pokyčiams. Detali tvarka ir jos įgyvendinimo kontrolė nenumatyta.

Įrankis	Valstybės lygmuo	Institucinis lygmuo
Informacijos saugumo auditas: Ar apibrėžtas audito procesas, atsakomybės, periodiškumas ir vykdymo kontrolė?	Svarbiausių informacinių išteklių auditas nustatytas Valstybės informacinių išteklių įstatyme, įgyvendinimo tvarka ir atsakomybės nenustatytos.	Institucijos privalo vykdyti periodinius auditus ir nustatyti atsakingus asmenis. Nėra apibrėžtas kontrolės procesas, ar institucijos vykdo auditą.
Informacijos saugumo veikėjai: Ar apibrėžtas informacijos saugumo organizavimas ir nustatytos atsakomybės? Ar paskirtos informacijos saugumo valdymo atsakomybės (kompetencijos)?	Informacijos saugumo įgyvendinimą koordinuojančia institucija paskirta Lietuvos Respublikos vidaus reikalų ministerija, sudaryta nuolatinė Elektroninės informacijos saugos (kibernetinio saugumo) koordinavimo komisija tarpinstituciniam koordinavimui. Atsakingos institucijos neturi pakankamai žmogiškųjų išteklių funkcijoms vykdyti.	Institucijos informacijos saugumo organizavimas ir atsakomybės nustatomos Duomenų saugos nuostatuose ir kituose saugumo politiką įgyvendinančiuose dokumentuose. Teisės aktais nustatyta, kad įstaigos vadovas privalo paskirti saugos įgaliotinį informacijos saugumui valdyti organizacijoje.
Informacijos saugumo branda: Ar nustatyti informacijos saugumo brandos lygiai? Ar vertinama informacijos saugumo branda?	*Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programoje* numatyta, kad bus vertinamas informacijos saugumo valdymo brandos lygis, tačiau tokio vertinimo sistema nenumatyta, brandos lygiai neapibrėžti.	Brandos lygiai neapibrėžti, vertinimo sistema nenumatyta.

Dokumentų turinio analizė leido identifikuoti šaltinius formuojančius informacijos saugumo valdymo reikalavimus Lietuvos valstybės institucijoms, išryškinti jų trūkumus bei iškelti probleminius klausimus. Empirinio tyrimo metodologijoje pažymėta, kad dokumentų turinio analizės rezultatams pagrįsti, tikslinga juos patikrinti ekspertų interviu metodu.

3.4. Ekspertų interviu rezultatų analizė

Ekspertams buvo formuluojamos penkios pagrindinės klausimų grupės:

1. Informacijos saugumo valdymo objektas ir tikslai.

Aptardami informacijos saugumo valdymo objektą ir tikslus ekspertai aptarė tarptautinę situaciją, istorinę raidą Lietuvoje, įvardijo esamos situacijos privalumus ir trūkumus bei išsakė savo nuomones dėl ateities perspektyvų.

Ekspertai pažymėjo, kad Lietuvoje ir tarptautinėje erdvėje vyksta diskusijos apie tai, kas turėtų būti informacijos saugumo objektas (*„tarp saugos specialistų nuolat kyla diskusijų dėl informacijos saugumo objekto – sistemos ar tinklai“*; *„Europos Sąjungoje nėra bendros nuomonės, kas turėtų būti informacijos saugumo objektu“;* Lietuvoje *„informacijos saugumo objektu valstybės institucijose susiklostė informacinės sistemos“* , tačiau pastebėta, kad *„iškyla opus klausimas – kaip apsaugoti informaciją, kai ji perduodama iš sistemos į sistemą“*). Ši diskusija ir tyrime dalyvavusius ekspertus paskatino kelti prielaidas dėl informacijos saugumo objekto, taikytino Lietuvos valstybės institucijoms, keitimo (*„informacijos saugumo objektas turėtų būti informacija, kaip vienetas, tiesiogiai nesiejant nei su informacinėmis sistemomis ar ištekliais, nei su ryšių tinklais“*; *„derėtų apmąstyti saugumo objekto plėtimą, galbūt sujungiant informacines sistemas ir ryšių tinklus <...> svarstytinas klausimas dėl informacijos kaip bendrinio saugos objekto apibrėžimo“*; *„pagrindas yra informacija ir duomenys, juos ir reikėtų saugoti“*; *„galbūt vertėtų mažinti objektų skaičių, informacijos saugumo reglamentavimą galima būti sieti su organizacija“*; pažymėta, kad *„tai aktualu daugiau išteklių valdančioms institucijoms“*).

Vertinant istorinį kontekstą ekspertų teigta, kad *„nuo seno Lietuvoje susiklostė informacinės sistemos, kaip saugumo objektas“*, tačiau *„buvo didelė spraga vertinant bendrą institucijose valdomos informacijos kiekį, kuriam saugumo reikalavimai nebuvo taikomi“*. Ekspertai pažymėjo, kad nuo šių metų pradžios įsigaliojęs *„naujasis Valstybės informacinių išteklių valdymo*

įstatymas apėmė daug didesnį išteklių skaičių ir praktiškai dengia visas informacijos valdymo formas institucijose“, o tai *„sudaro kaip niekad geras prielaidas informacijos saugai užtikrinti“*. Taigi jungiant ekspertų nuomones, konstatuotina, kad *„Lietuvoje informacijos saugumo objektu, priėmus naują įstatymą, tapo informacijos ištekliai“* ir, nors šis informacijos saugumo valdymo objektas turi minėtų trūkumų, *„istoriškai susiklosčiusią situaciją labai sudėtinga pakeisti, tam reikėtų labai daug resursų ir pastangų“*.

Kitas aspektas, kurį pabrėžė ekspertai, – *„šiuo metu yra tarpinis laikotarpis <...> Valstybės informacinių išteklių valdymo įstatymas jau galioja, <...> tačiau teisės aktai, kurių reikia šiam įstatymui įgyvendinti, dar tik planuojami“*, kartu atkreiptas dėmesys, kad *„šie metai yra rinkiminiai, todėl sunku prognozuoti, ar planuojami teisės aktai laiku ir tinkamai bus priimti“*.

Vertindami teisės aktais įtvirtintus informacijos saugumo tikslus Lietuvos valstybės institucijoms ekspertai minėjo, kad *„tikslai nėra tiesiogiai deklaruoti, tačiau vertinant <...> visumą, galima juos įžvelgti“*, (teisės aktais yra *„įtvirtinti saugumo tikslai, apimantys konfidencialumą“*, *„formalizuotas vientisumo užtikrinimo poreikis“*, *„prieinamumo klausimai taip pat svarbūs, <...> galbūt nėra aiškiai ir formaliai deklaruoti, tačiau galima įžvelgti šio tikslo siekimą“*).

Vertindami tai, kad visoms Lietuvos valstybės institucijoms galioja vienodi informacijos saugumo valdymo tikslai, neišskiriant prioritetų, ekspertai išsakė nuomones, kad tokia situacija yra ydinga (*„situacija, suvienodinusi visas institucijas prioritetu klausimu, tikrai nėra pati tinkamiausia. Brandžios institucijos turėtų turėti galimybę pačios pasirinkti“*, *„reikalavimai turėtų būti labiau detalizuojami pagal duomenų svarbumą“*, *„saugumo tikslai, taikomos saugos priemonės turėtų remtis informacijos klasifikavimu“*, *„saugant informaciją, tikslais pagal prioritetus galėtų būti įvardinti – CIA*[25]*, tinklus – AIC“*).

[25] pagal angliškus terminus *Confidentiality, Integrity, Availability* (*atitinkamai konfidencialumas, vientisumas, prieinamumas*).

Kartu buvo iškeltos aktualios problemos – šiuo metu *„galioja kiek komplikuotas informacijos klasifikavimas, anksčiau buvo keturios kategorijos, įsigaliojęs įstatymas numato kiek kitokią klasifikaciją“*, taip pat teisės aktais yra išskirta asmens duomenų kategorija, kuriai taikomi kiti reikalavimai, įneša papildomų neaiškumų (*„asmens duomenų apsaugai taikomi specializuoti reikalavimai. Galėtų būti ieškoma bendrumų tarp šių kategorijų ir tik esant išskirtiems ypatumams taikomi specializuoti reikalavimai“*).

Kaip netinkamą pavyzdį ekspertai paminėjo tai, kad *„pirmos kategorijos (svarbiausioms) sistemoms neproporcingai sureikšmintas informacijos prieinamumo reikalavimas – sistemos atstatymas per 15 min. nepasiekiamas net ir institucijoms, valdančioms kritinės svarbos sistemas“*, bei teigė, kad toks nekorektiškas *„reikalavimas įgyvendinamas tik formaliai, tinkamas jo realizavimas pareikalautų labai daug finansinių resursų“*.

Galima konstatuoti, kad ši išsakyta mintis apibendrina ekspertų nuomones: *„institucijoms turėtų būti labiau leidžiama pasirinkti joms aktualius saugumo tikslus ir atitinkamai jų siekimo priemones, tačiau procesas turi būti gerai apgalvotas, nepamatuoti keitimai gali sukurti daug bereikalingo biurokratinio darbo ir neatnešti jokios papildomos naudos saugumui“*.

Kartu pažymėta, kad *„institucijų požiūris į saugumo prioritetus <...> nėra tirtas, būtų įdomu išsiaiškinti jų požiūrį“*.

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 atstovai, taigi *„galima tikėtis, komisija pradės koordinuoti darbus“*. Komisijai vadovauti ir pagrindine informacijos saugumo koordinatore paskirta Vidaus reikalų ministerija. Sudarytas sąrašas teisės aktų, kuriuos būtina parengti naujam *Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymui* įgyvendinti, tarp jų yra ir susijusių su saugumu.

Vertindami informacijos saugumo valdymo organizavimą ekspertai beveik vienbalsiai sutaria: formaliai ši sritis reglamentuota (*„saugumo valdymo organizavimas tikrai neblogas formaliąja prasme“, „formaliai institucijoms išdalintos atsakomybės sritys“, „atsakomybe dalinasi visa eilė institucijų“, „Institucijų kompetencijos gana aiškios“, „koordinatore paskirta Vidaus reikalų ministerija“, „tarpinstitucinę koordinacinę funkciją Lietuvoje vykdo <...> koordinavimo komisija“*), tačiau pradėjus nagrinėti realią situaciją stebimi dideli formalios situacijos įgyvendinimo trūkumai (*„koordinatorių daug, o realius darbus dirbti nėra kam“*; *„koordinavimo klausimai deleguoti tarpinstitucinei komisijai, konsultavimo klausimai – konsultacinei tarybai, deja, šiuo metu ji dar nesudaryta“*; *„saugos atsakomybės išdalintos po truputį daugelyje institucijų“*; *„bendra tendencija – kompetencijos trūkumas ir žmonių stoka. Su esamu etatų skaičiumi iš atsakingų institucijų sunku tikėtis proveržio ar didelių darbų. Jau kurį laiką galima stebėti lėtą reikalingų teisės aktų rengimą, užtrunkantį nuostatų ir kitų saugos dokumentų derinimą“*; *„po kelis žmones institucijose, ypač vertinant biurokratinio darbo mastus, tikrai negali nuveikti didelių darbų“*, *„trūksta resursų saugos funkcijoms vykdyti <...> trūksta tiek etatų, tiek kompetencijos, tiek ir finansų“*; *„pastebima gana aiški valstybiniam sektoriui būdinga tendencija – kompetentingų specialistų, finansų ir kitų resursų trūkumas. Dažnai saugos prioritetai pasimeta tarp kitų institucijų funkcijų“*; *„paskutiniu metu atsakingų institucijų, gal išskyrus Ryšių reguliavimo tarnybą, kompetencija saugos srityje pastebimai sumenko“*; *„Vidaus reikalų ministerija, turėjusi dedikuotus padalinius saugos problemoms koordinuoti ir spręsti, krizės metu visai išbarstė kompetenciją“*).

Vertinant tokį unitarinį ekspertų požiūrį bei konstatavimą, kad *„su šia valdžia iki naujų rinkimų mažai tikėtinas koks nors proveržis“*, galima išskirti keletą svarbių ekspertų siūlymų situacijai optimizuoti – visų pirma ekspertai pastebėjo teigiamą Valstybės kontrolės įdirbį ir išsakė siūlymus jį išnaudoti (*„daugiau tvarkos padėtų įnešti ir Valstybės kontrolės aktyvesnė veikla analizuojant saugos įgyvendinimą institucijose“*). Kitas siūlymas – kompetencijos trūkumo klausimus spręsti bendradarbiaujant viešajam

privačiam ir mokslo sektoriams (*„kolegialią instituciją galėtų pastiprinti viešojo ir privataus sektorių bendradarbiavimo pagrindu veikiantis kompetencijos centras, kuris galėtų jungti ir akademinio sluoksnio specialistus“*; *„privalumas būtų veikianti idėjų generavimo, konsultacinė struktūra“*). Šis bendradarbiavimas galėtų remtis tarptautine gerąja praktika (*„galėtų būti pasisemta patirties, kaip tokie dariniai veikia užsienio šalyse, ir išnaudota galimybė pasitelkti akademinį bei privatų sektorius“*; *„būtų galima pasimokyti iš Estijos, kurioje labai sėkmingai veikia savanoriška organizacija – Saugumo lyga, pavyzdžio“*; *„šiuo pavyzdžiu ketina sekti ir kaimynai latviai, susidomėjimą išreiškė ir kitos šalys“*) bei sėkmingais pavyzdžiais Lietuvoje (*„geri papildomos kompetencijos pritraukimo pavyzdžiai – kai kurių ministerijų bendradarbiavimas su universitetais. Ar dalyvavimas tarptautinių organizacijų veikloje“*; *„buriasi kompetencijų centrai bendradarbiaujant didžiosioms savivaldybėms su universitetais ir pan.“*). Šiame kontekste svarbi ekspertų įžvalga, kad *„galima pastebėti tiek verslo, tiek ir akademinio sluoksnių pageidavimus dalyvauti platesnio pobūdžio konsultaciniame procese“*.

Ekspertai aiškiai išskiria ir kitą svarbią „spragą“ – dėmesio trūkumą kritinei informacinei infrastruktūrai *(„Lietuvoje vėliausiai susirūpinta kritinės infrastruktūros saugumo funkcijomis“*; *„kritinės infrastruktūros klausimai nėra tinkamai sprendžiami – neturime ne tik vienareikšmiškai atsakingos institucijos, bet net ir šios infrastruktūros apibrėžimo“*; *„neatsakytų klausimų išlieka dėl kritinės infrastruktūros identifikavimo ir apsaugos“*).

Vertinant informacijos saugumo valdymo Lietuvos valstybės institucijose organizavimo tolesnę plėtrą, pastebėta, kad *„išsiskiria institucijų nuomonės dėl tolesnio (platesnio) informacijos saugumo reglamentavimo <...> specialiu saugos įstatymu“* ar esamo *Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo* tobulinimo (*„galima modernizuoti saugumo reglamentavimą esamo <...> įstatymo bazėje“*).

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

Ekspertų pastebėjimu, pagal galiojančius teisės aktus (*Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programoje*) *„numatytas brandos stebėjimas, tačiau kol kas nėra bendros metodikos brandai vertinti, nebuvo vykdyti platūs tyrimai“* (*„neteko girdėti apie platesnius brandos vertinimus“*). Tokią metodiką, ekspertų teigimu, vertėtų kurti tarptautinių metodikų pagrindu (*„galėtų remtis COBIT, ITIL ar kitos tarptautinės metodikos principais“; „tikrai vertėtų sukurti brandos vertinimo sistemą valstybės institucijoms, kad ir COBIT ar panašios metodikos pagrindu“*). Ekspertai pažymi, kad *„institucijos paliktos savieigai, stipresnės juda, silpnesnės – labai sunkiai“* ir nors, jų teigimu, *„institucijų branda ir saugumo reikšmės supratimas tikrai įvairus“*, pakankamai panašiai vertina institucijų dabartinį brandos lygį (*„iš pavienių tyrimų galima numanyti, kad maždaug du trečdaliai Lietuvos institucijų atitinka maždaug pirmą, trečdalis – antrą brandos lygį (iš penkių), galbūt su labai retomis išimtimis“; „stipresnės jau dabar atitinka saugumo valdymo standartus“; „galima numanyti „mažąsias“ institucijas esant nuliniame ar pirmajame lygyje“; „net ir didelės institucijos, investavusios ženklias sumas į sistemas ir saugą, nesugeba išvengti incidentų, o taip neturėtų būti“; „institucijų branda yra labai įvairi, tikrai yra institucijų, smarkiai pažengusių, tačiau kas darosi, pavyzdžiui, savivaldybių lygmenyje, labai sunku pasakyti“*; *„nėra aiški institucijų brandos būklė, nors pastebima, kad institucijos pradeda po truputį suprasti pridėtinę jos vertę“*). Taigi akivaizdu, kad *„vertinimai labiau proginės veiklos nei sistema“,* o platesnio masto *„tyrimai šiame kontekste nedaryti ir tikrai būtų aktualūs“*.

Brandos lygis (ar jo siekimas) *„galėtų būti siejamas su institucijų valdomų informacinių išteklių svarba (kategorija). Kuo svarbesnius išteklius valdo institucija, tuo aukštesnio brandos lygio ji turėtų siekti“*, tačiau *„brandos lygiai turėtų sietis ir su taikymo apimtimi, nebūtina taikyti visų saugumo priemonių, išdėstytų standartuose šimtu procentų“*, nes *„tiesioginis standartų įgyvendinimas sietinas ir su nemažu lėšų poreikiu“*.

4. Informacijos saugumo funkcijų centralizavimo poreikis ir apimtys.

Aptariant šį klausimą ekspertai sutaria – *„centralizuoti funkcijas tikrai yra poreikis“* ir pažymi, kad *„tai leistų taupyti finansinius išteklius, lengviau palyginti institucijų situaciją“*.

Grupuojant ekspertų nuomones, galima išskirti dvi pagrindines siūlomas funkcijų centralizavimo kryptis:

1) infrastruktūra *(„Centralizavimas tikrai praverstų techninės infrastruktūros lygmenyje“*; *„Funkcijos galėtų būti centralizuojamos įvairiais lygmenimis, pavyzdžiui, „vyriausybės debesis“ (angl. Government Cloud), kolektyvinės ryšių gynybos sistemos ar kitos infrastruktūrinės priemonės“*; *„būtų sveikintinas dalykas – infrastruktūros centralizavimas <...> institucijoms tai leistų mažiau rūpintis su tiesiogine veikla nesusijusiomis funkcijomis, lengviau atitikti iškeltus saugos reikalavimus“*), tam pradžiai siūloma inventorizuoti valstybės institucijų valdomą turtą (*„Valstybė turėtų aiškiai suinventorizuoti turimą turtą ir tada būtų galima spręsti dėl valstybės institucijų valdomos infrastruktūros konsolidavimo, centralizuoto naudojimo“*) ir *„nebekurti dar kartą esamų funkcionalumų“*.

2) metodinė pagalba (*„esant tokiai kompetencijos situacijai valstybės sektoriuje, tikrai reikia galvoti apie kompetencijų centrus, institucijos nesugebės kiekviena sau išlaikyti profesionalių specialistų“*; *„brandžios institucijos galbūt gali „savimi pasirūpinti“, tačiau mažiau brandžioms tikrai praverstų centralizuota pagalba – kompetencijos kėlimo, audito, rizikos analizės klausimais“*; *„net ir brandžioms institucijoms vertinga gali būti išorės audito nuomonė „iš šalies“*; *„funkcijų centralizavimo sritis galėtų būti mokymų vykdymas ar bent organizavimas; informacijos saugumo kompetencijos trūkumas ir konsultacijų poreikis pastebimas visuose lygiuose“*; *„galėtų būti svarstomas centralizuotas rizikos analizės ir vertinimo, saugos ir valdymo audito vykdymas. Labai naudinga būtų vienoda metodika ir palyginami kriterijai“*; *„rengiamos vienodos metodikos, daromos rizikos analizės ar intervenciniai auditai“*; *„svarbus veiksnys – stipri koordinuojanti*

institucija, turinti pakankamai kompetencijos koordinuoti darbus, organizuoti centralizuotus saugos vertinimus, auditus, rizikos analizes, metodinius dokumentus, mokymus ir pan.“; *„galėtų būti apibrėžti taikytini informacijos saugumo sertifikatai auditoriams ir institucijoms, išorinio audito tvarka, galbūt jis irgi galėtų būti vykdomas (užsakomas) centralizuotai“*).

Kita tendencija ekspertų įžvalgose – funkciniai kompetencijų centrai (*„galėtų būti centralizuojamos funkcijos apimant valdomas sistemas pagal veiklos sritis. Ministerijos galėtų centralizuotai vykdyti mokymus, saugos vertinimą, tipinių teisės aktų rengimą visoms savo pavaldžioms institucijoms“*, *„kompetencijos centrai galėtų būti ir pagal funkcines sritis“*).

Analizuojant informacijos saugumo valdymo tobulinimą taip pat išsakyta nuomonė, kad „*verta būtų svarstyti <...> finansinių resursų paieškos klausimų centralizuotą paskyrimą kokiai nors institucijai“*.

5. Informacijos saugumo stebėsenos ir kontrolės sistemos kūrimas ir vertinimo kriterijai.

Anot ekspertų, *„tokios sistemos poreikis yra“*, ypač atsižvelgiant į informacijos saugumo valdymą koordinuojančių valstybės institucijų kompetenciją ir turimus žmogiškuosius išteklius (*„su esama kompetencija ir resursais sunkiai tikėtina reikšminga stebėsena ir kontrolė“*), taigi *„tokia sistema turėtų būti esminis koordinuojančios institucijos darbo įrankis“*.

Jau dabar *„egzistuoja rimta automatizuota incidentų ir anomalijų tinkluose stebėsenos sistema“*, tačiau platesnių *„stebėsenos <...> priemonių <...> trūksta“*, tokiai sistemai, ekspertų manymu, tikrai netruktų naudingų funkcijų (*„tokia sistema leistų stebėti institucijų atitiktį saugos reikalavimams, dokumentų savalaikį parengimą ir atnaujinimą“*; *„galėtų būti stebimas ir organizacijų brandos lygis ir jo kitimas“*; *„įrankis galėtų padėti apibrėžti ir stebėti tą pačią institucijų brandą, atitiktį teisės aktuose įtvirtintiems reikalavimams, auditų, rizikos analizių rezultatus, spręsti apie institucijų kompetenciją ir pagalbos joms poreikį“*).

3.5. Kokybinių tyrimų rezultatų aptarimas

Ekspertų apklausa leido pagrįsti ir praplėsti dokumentų turinio analizės rezultatus, išdėstytus 12 lentelėje. Apibendrintų kokybinių tyrimų rezultatų aptarimui struktūrizuoti panaudota suformuota informacijos saugumo valdymo vertinimo prieiga.

Informacijos saugumo politikos lygmenyje 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 informaciniais ištekliais. Taigi tyrimo rezultatai išryškino, kad informacijos saugumo valdymo objektas – pavieniai valstybės institucijų valdomi informaciniai ištekliai. Šis objektas turi trūkumų tiek dėl to, kad toks objektas vienareikšmiškai neapima visos valstybės institucijos valdomos informacijos, tiek dėl to, jog šiuo metu informacijos saugumo valdymo reikalavimai galioja ne visiems informaciniams ištekliams. Ekspertai pripažino šį trūkumą, tačiau išsakė nuomonę, kad esamo informacijos saugumo valdymo objekto keitimas kainuotų pernelyg daug finansinių ir administracinių išteklių. Apibendrintai vertinant ekspertų įžvalgas labiau tinkamas sprendimas – patvirtinti trūkstamus informacijos saugumo valdymo reikalavimus vidaus administravimo sistemoms ir informacijos saugumo valdymą reglamentuojančius dokumentus kompleksiškai taikyti visiems valstybės institucijos valdomiems informacijos ištekliams, t. y. siekti, kad nepriklausomai nuo to, kiek informacinių išteklių valdo valstybės institucija, joje būtų vienas informacijos saugumo valdymo politikos dokumentas (duomenų saugos nuostatai), kuriuo būtų bendrai apibrėžiami visi tos valstybės institucijos valdomi informaciniai ištekliai.

Dokumentų turinio analizė leido identifikuoti, kad informacijos saugumo valdymo politiką formuojantys reikalavimai tiesiogiai apima tik du iš trijų informacijos saugumo valdymo tikslų – konfidencialumą ir vientisumą, t. y. neapima prieinamumo, tačiau ekspertų interviu rezultatų analizė išryškino,

kad aukščiausio lygmens teisės aktais neapibrėžtas prieinamumo reikalavimas tėra formalus trūkumas. Pavyzdžiui, valstybės institucijos, valdančios pirmos kategorijos (svarbiausias) valstybės informacines sistemas, informacijos saugumo prieinamumo tikslą taiko atsižvelgdamos į Lietuvos Respublikos vidaus reikalų ministro patvirtintus techninius reikalavimus, kurie, ekspertų manymu, netgi neproporcingai per griežti. Taip pat buvo pažymėta, kad per griežti reikalavimai dažnai įgyvendinami tik formaliai. Ekspertai išsakė abejones ir dėl tapačiai taikomų informacijos saugumo tikslų visoms valstybės institucijoms. Jų manymu, institucijos turėtų turėti galimybę pačios nusistatyti prioritetus šiems tikslams taikyti atsižvelgdamos į institucijoje valdomos informacijos specifiką.

Informacijos saugumo strategijos lygmenyje dokumentų turinio analizės metu buvo identifikuota, kad valstybės institucijos neįpareigotos rengti specialios informacijos saugumo strategijos, o valstybės lygmenyje strateginiai dokumentai galioja, tačiau dar nėra patvirtintų detalių įgyvendinimo priemonių planų. Vertinant informacijos saugumo strategijos įgyvendinimo 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 privalomo taikymo (strateginės dimensijos sudedamoji dalis). Informacijos saugumo valdymo procesas apibrėžtas tiek įstatymu, tiek ir poįstatyminiais aktais, tačiau nėra užtikrinamas šio proceso nuolatinis taikymas.

Informacijos saugumo audito lygmenyje dokumentų turinio analizė 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 lygmenyse, tačiau šių reikalavimų įgyvendinimo tvarka nėra nustatyta. Kokybiniame tyrime dalyvavę ekspertai taip pat pabrėžė, kad tiek vidinio, tiek išorinio audito vykdymas būtų naudingas ir reikalingas, tačiau

nevykdomas. Ekspertai išsakė siūlymą parengti vienodą metodiką ir centralizuoti informacijos saugumo valdymo audito atlikimą (ar bent užsakymą), į valstybės institucijų informacijos saugumo valdymo auditavimą labiau įtraukti Valstybės kontrolę.

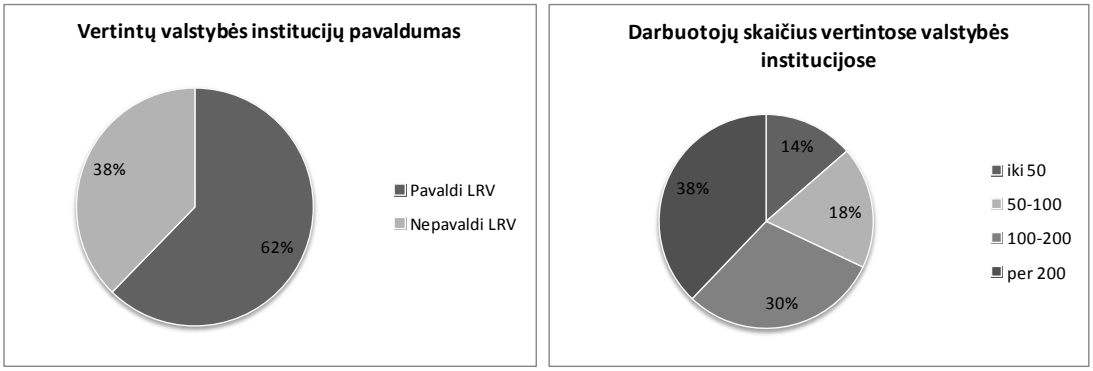
Informacijos saugumo veikėjų (kompetencijos) lygmenyje atlikta dokumentų turinio analizė atskleidė decentralizuotą informacijos saugumo valdymo organizavimo ir koordinavimo modelį – pavienės sritys formaliai išdalintos kelioms atsakingoms institucijoms (išskyrus kritinės infrastruktūros apsaugos funkciją, kuri vienareikšmiškai niekam nepriskirta), tačiau išanalizavus kompetentingų institucijų funkcijas ir etatų sąrašus akivaizdžiai matyti, kad koordinuojančios institucijos nėra pajėgios vykdyti iškeltų joms uždavinių. Ekspertų interviu rezultatai patvirtino šias įžvalgas: ekspertai pažymėjo, kad nors yra sudarytas kolegialus koordinavimo organas, paskirtos kompetentingos institucijos, tačiau informacijos saugumo organizavimas pasižymi žema institucijų kompetencija, specialistų trūkumu, lėtu paskirtų užduočių vykdymu bei viešojo ir privataus sektorių bendradarbiavimo neišnaudojimu. Ekspertų manymu, siekiant valstybės institucijų veiklos efektyvumo, reikėtų centralizuoti informacinės infrastruktūros naudojimą (prieš tai ją inventorizavus), stiprinti centralizuotą metodologinę pagalbą institucijoms (pasitelkiant viešojo, privataus ir mokslo sektorių bendradarbiavimą) bei užtikrinti nuolatinį informacijos saugumo valdymo vertinimą ir kontrolę pagal vienodą metodiką ir aiškius vertinimo kriterijus.

Informacijos saugumo brandos lygmenyje dokumentų turinio analizė parodė, kad informacijos saugumo brandos lygiai ir vertinimo sistema nėra nustatyti. Ekspertų interviu metu respondentai praktiškai vienbalsiai pabrėžė brandos lygių nustatymo ir vertinimo privalumus. Pagal institucijų brandos lygį galėtų būti parenkamos informacijos saugumo valdymo priemonės, svarbesnius išteklius valdančios institucijos turėtų siekti atitinkamai aukštesnio brandos lygmens. Ekspertų manymu, brandos lygiams apibrėžti galėtų būti taikytinos tarptautinės metodikos (COBIT ar pan.).

3.6. Kiekybinio tyrimo rezultatai ir jų interpretacija

Kaip pažymėta empirinio tyrimo metodologijoje, pirmoji kiekybinio tyrimo dalis skirta išsiaiškinti institucijos statusą (centrinės ar regioninės valdžios bei pavaldumą Lietuvos Respublikos Vyriausybei), dydį bei informacinių technologijų ir informacijos saugumo valdymo atsakomybes.

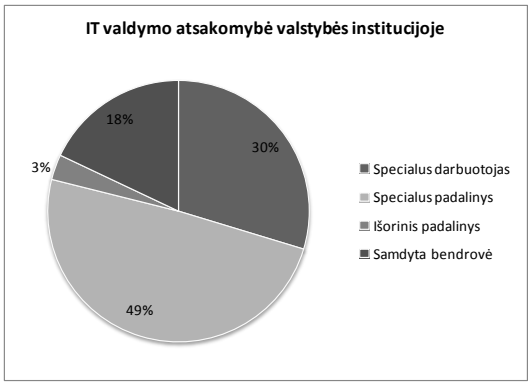
Anketa buvo išsiųsta 140 Lietuvos Respublikos valstybės institucijų, iš kurių gauti 106 atsakymai. Tyrime dalyvavusių institucijų pasiskirstymas pagal pavaldumą – 62 proc. institucijų pavaldžios Lietuvos Respublikos Vyriausybei, 38 proc. nepavaldžios. Taigi galima konstatuoti, kad apklausoje dalyvavusių respondentų imtis atitinka tyrimui keltą uždavinį įvertinti įvairaus pavaldumo institucijas. Skirtingo pavaldumo institucijos tyrimui svarbios, vertinant tai, kad iki 2012 m. sausio 1 d. visoms tiesiogiai nepavaldžioms Lietuvos Respublikos Vyriausybei valstybės institucijoms, informacijos saugumo valdymo reikalavimai buvo tik rekomendacinio pobūdžio, todėl šios institucijos yra svarbi tyrimui tikslinė grupė, kuri gali reikšmingai veikti bendrus tyrimų rezultatus. Vertinant aptartą kontekstą prasminga šios grupės respondentų rezultatus įvertinti ir atskirai nuo bendro rezultatų srauto (24 paveikslas).

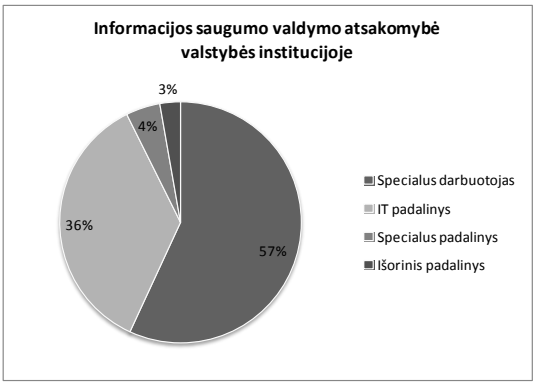


24 ir 25 pav. Lietuvos valstybės institucijų, dalyvavusių tyrime, pavaldumas ir dydis.

Atsižvelgiant į tyrime dalyvavusių institucijų dydį (pagal darbuotojų skaičių), galima teigti, kad tyrimo rezultatuose atspindėta įvairių institucijų specifika, taip pat galima pastebėti, kad beveik 70 proc. dalyvavusių tyrime valstybės institucijų dirba per 100 darbuotojų, o tai vertintina kaip pakankamai stambios organizacijos, kuriose apdorojamas reikšmingas informacijos kiekis (25 paveikslas).

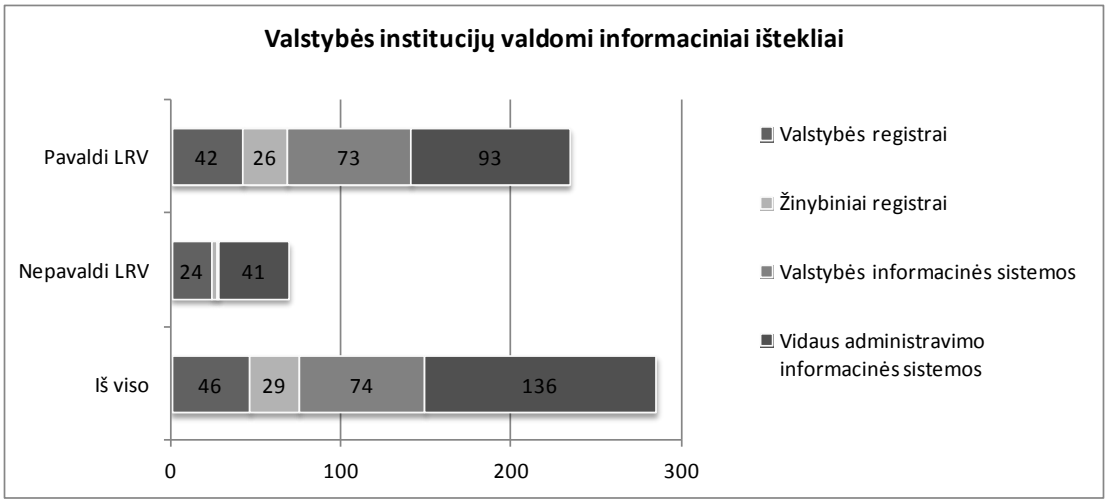
Vertinant Lietuvos valstybės institucijose vyraujančią atsakomybę už informacinių technologijų valdymą, galima pastebėti, kad beveik trečdalyje valstybės institucijų (daugumoje mažesnėse) tuo užsiima vienas konkretus darbuotojas, pusė jų turi dedikuotus padalinius (90 proc. iki 10 darbuotojų dydžio), taip pat pastebėtina, kad beveik penktadalis tyrime dalyvavusių valstybės institucijų informacinių technologijų atsakomybę delegavusios išorinėms bendrovėms (tarp jų absoliuti dauguma centrinės valdžios institucijos). Analizuojant informacijos saugumo valdymo atsakomybę – beveik du trečdaliai institucijų (61 proc.) turi paskirtą specialų už informacijos saugumo valdymo atsakingą darbuotoją ar netgi visą padalinį, tačiau beveik 40 proc. visų tyrime dalyvavusių valstybės institucijų informacijos saugumo valdymas yra informacinių technologijų padalinio atsakomybė (26 ir 27 paveikslai). Savivaldybių lygmenyje šis procentas viršija 50, vertinant situaciją ministerijose – tik ketvirtadalyje iš jų informacijos saugumo funkcijos patikėtos informacinių technologijų padaliniams.





26 ir 27 pav. Informacinių technologijų ir informacijos saugumo valdymo atsakomybė Lietuvos valstybės institucijose.

Antroji kiekybinio tyrimo dalis buvo skirta išsiaiškinti, kokius valstybės informacinius išteklius valdo institucija. Tyrime dalyvavusios valstybės institucijos deklaravo valdančios 285 įvairius informacijos išteklius, taigi statistiškai viena valstybės institucija valdo 2,7 informacijos išteklių (pažymėtina, kad vienai ministerijai vidutiniškai tenka 5,2, o savivaldybės administracijai tik 1,15 valdomo informacijos ištekliaus). Tarp Lietuvos valstybės institucijų valdomų informacinių išteklių vyrauja vidaus administravimo informacinės sistemos (47 proc. visų informacinių išteklių, savivaldybių administracijų atveju – 87 proc.). Ši įžvalga ypač aktuali tyrimui vertinant tai, kad vidaus administravimo informacinėms sistemoms vis dar nėra patvirtintų privalomų informacijos saugumo valdymo reikalavimų (28 paveikslas), o ir savivaldybių administracijoms ilgą laiką informacijos saugumo reikalavimai nebuvo tiesiogiai taikomi.



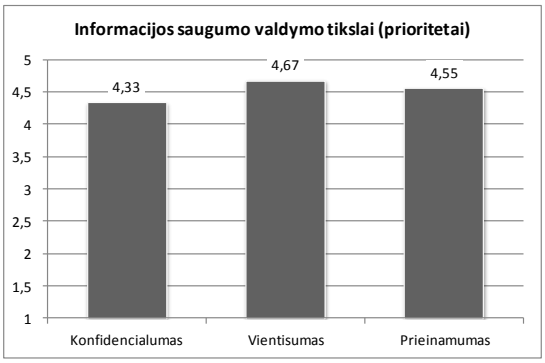
28 pav. Lietuvos valstybės institucijose valdomi informaciniai ištekliai (informacinių išteklių sąvoka ir rūšys naudojamos remiantis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu).

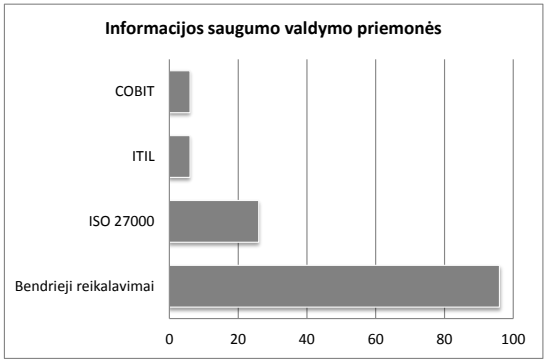
Trečioji kiekybinio tyrimo dalis skirta išsiaiškinti valstybės institucijos požiūrį į informacijos saugumo tikslus (kiek šie tikslai aktualūs tiriamai institucijai, kuriam tikslui skiriamas prioritetas); informacijos saugumo

valdymui taikomus reikalavimus ir metodikas; saugos įgaliotinio egzistavimą bei jo vietą institucijoje (pareigas, pavaldumą); informacijos saugumo audito ir kitų vertinimo bei kontrolės priemonių taikymą; institucijos turimus informacijos saugumą reglamentuojančius dokumentus ir jų aktualumą; informacijos saugumo mokymų vykdymą institucijoje; pagrindines problemas ir iššūkius, su kuriais susiduria valstybės institucija, siekdama užtikrinti informacijos saugumą, bei institucijos nuomonę, kokias informacijos saugumo funkcijas reikėtų organizuoti centralizuotai, kokias palikti vykdyti pačiai institucijai.

Dauguma tyrime dalyvavusių valstybės institucijų, vertindamos informacijos saugumo valdymo prioritetus, nors pirmenybę ir atidavė vientisumo prioritetui (vidurkis 4,67 balų iš 5 galimų), o mažiausiai vertino konfidencialumą (4,33 balų), tarp šių tikslų svarbos valstybės institucijoms, vertinant tiek bendrus rezultatus, tiek atskirai pagal institucijų statusą, nėra statistiškai reikšmingo skirtumo (29 paveikslas).

Nagrinėjant valstybės institucijų taikomas informacijos saugumo valdymo priemones, beveik visos institucijos paminėjo taikančios Lietuvos Respublikos Vyriausybės patvirtintus Bendruosius informacijos saugumo reikalavimus (96 proc., ministerijų atvejų – 100 proc.). Šalia šių reikalavimų 26 proc. institucijų nurodė taikančios ir tarptautinio informacijos saugumo valdymo standarto ISO 27000 reikalavimus, o beveik 6 proc. dar kartu taikė ir tarptautines metodikas COBIT ir ITIL (30 paveikslas). Institucijų pavaldumas ryškiai rezultatuose neatsispindėjo, tačiau svarbu paminėti, kad nors tiesiogiai Bendrieji saugumo reikalavimai savivaldybių administracijoms tiesiogiai netaikomi, net 93 proc. nurodė juos taikančios. Apklausus valstybės institucijas taip pat paaiškėjo, kad beveik 30 proc. valstybės institucijų turi aktualų informacijos saugumo strategijos dokumentą, nors tokio dokumento turėti galiojantys informacijos saugumo reikalavimai nereikalauja. Galima numatyti, kad šį dokumentą institucijos pasitvirtino besivadovaudamos „gerosiomis praktikomis“.

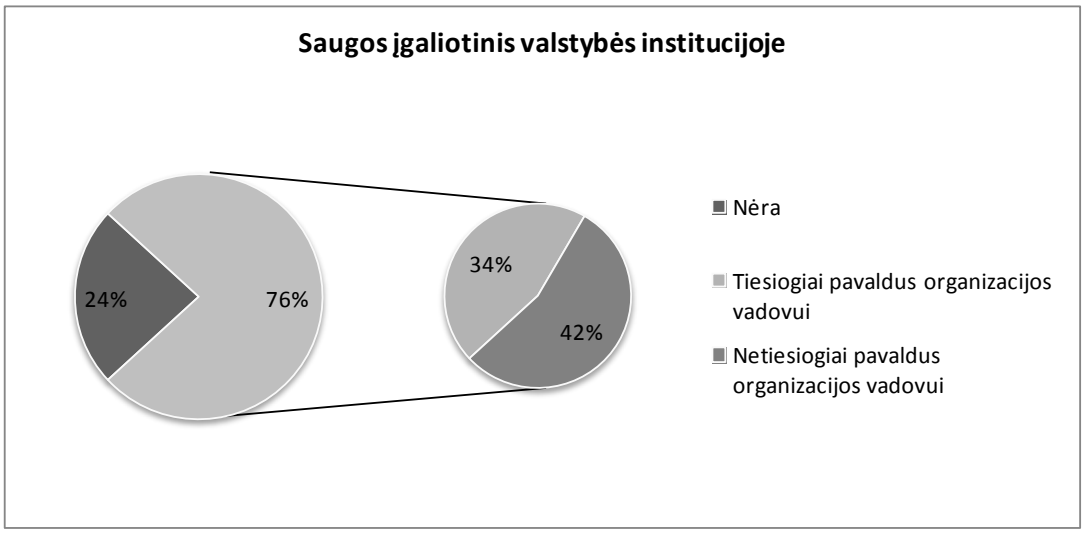




29 ir 30 pav. Lietuvos valstybės institucijų informacijos saugumo valdymo prioritetai ir taikomos priemonės.

Pagal Lietuvos valstybės institucijoms galiojančius informacijos saugumo valdymo reikalavimus, institucijos privalo paskirti saugos įgaliotinį, kuris tiesiogiai atsako už informacijos saugumo reikalavimų įgyvendinimą. 78 proc. apklaustų institucijų tokį įgaliotinį paskyrė (31 paveikslas), 36 proc. valstybės institucijų saugos įgaliotinis tiesiogiai pavaldus institucijos vadovui (ministerijose šis skaičius nesiekia 10 proc.). Saugos įgaliotinio pavaldumo reikalavimas nėra įtvirtintas teisės aktais, tačiau „gerosios praktikos“ nurodo, kad šis pareigūnas turėtų būti pavaldus tiesiogiai organizacijos vadovui.

Vertinant paskirto saugumo įgaliotinio užimamas pareigas institucijoje, galima konstatuoti, kad beveik 60 proc. atvejų paskirtasis saugumo įgaliotinis kartu yra ir institucijos informacinių technologijų padalinio darbuotojas, o 33 proc. atveju netgi šio padalinio vadovas (savivaldybių administracijų atveju atitinkamai 73 proc. ir 50 proc., ministerijų – 50 proc. ir 10 proc.). Taigi galima konstatuoti, kad valstybės institucijose vyrauja techninis požiūris į informacijos saugumo valdymą, o neatskirtas vadovavimas informacinių technologijų ir informacijos saugumo valdymo veikloms aiškiai pažeidžia įgyvendinimo ir priežiūros funkcijų atskyrimo principą. Ši problema ypač ryški savivaldybių administracijose.

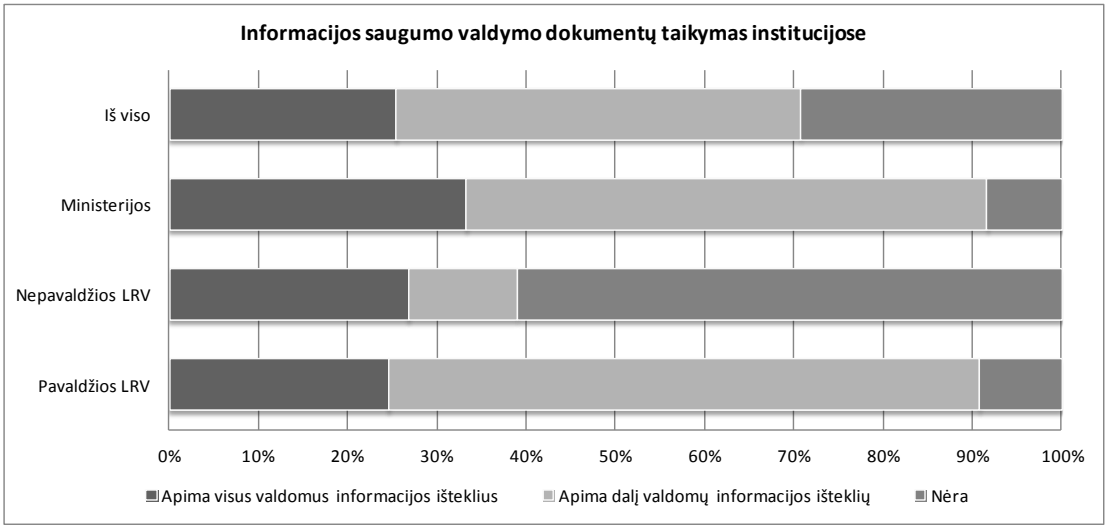


31 pav. Saugos įgaliotinis Lietuvos valstybės institucijose.

Analizuojant Lietuvos valstybės institucijų informacijos saugumo valdymo dokumentų turinį, pastebėta, kad tik 38 proc. tiesiogiai nepavaldžių Lietuvos Respublikos Vyriausybei institucijų nurodė, jog turi patvirtintą informacijos saugumo politikos dokumentą – duomenų saugos nuostatus, o iš pavaldžių Lietuvos Respublikos Vyriausybei valstybės institucijos per 90 proc. turi bent vieną tokį dokumentą. Vertinant optimalią situaciją, kai institucija turi vienus visus jos informacinius išteklius apimančius duomenų saugos nuostatus abiejuose institucijų grupėse, šis rodiklis siekia apie ketvirtį institucijų (32 paveikslas). Vertinant Lietuvos Respublikos ministerijas, trečdalyje jų situaciją galima įvardyti kaip optimalią, 8 proc. informacijos saugumo valdymo reikalavimų netaiko (palyginti su žvalgomo tyrimo duomenimis (aprašyti disertacijos 1.3 skyriuje) – optimali situacija buvo 7 proc. ministerijų, reikalavimų netaikė – 14 proc.).

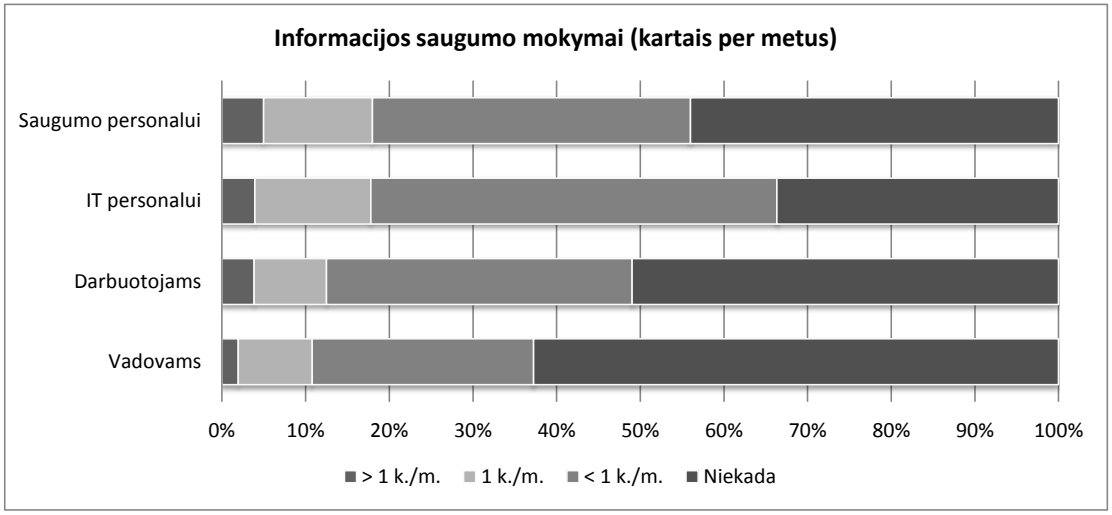
Gretinant aptartus kiekybinio tyrimo rezultatus ryškėja, kad nemažai valstybės institucijų tik deklaruoja taikančios *Bendruosius elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimuos.* Šie reikalavimai nurodo, kad valstybės institucijos vadovas turi paskirti saugos įgaliotinį bei patvirtinti duomenų saugos nuostatus. Tačiau nors 96 proc. valstybės institucijų deklaravo taikančios šiuos reikalavimus, tyrimo rezultatai parodė, kad tik 76 proc. iš jų turi paskirtą saugos įgaliotinį ir tik 72

proc. – patvirtintus duomenų saugos nuostatus. Dar ryškiau ši tendencija atsispindi savivaldos lygmenyje – 93 proc. savivaldybių administracijų nurodė taikančios *Bendruosius elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimus*, tačiau tik 65 proc. jų turi paskirtus saugos įgaliotinius ir tik 38 proc. – patvirtintus duomenų saugos nuostatus.



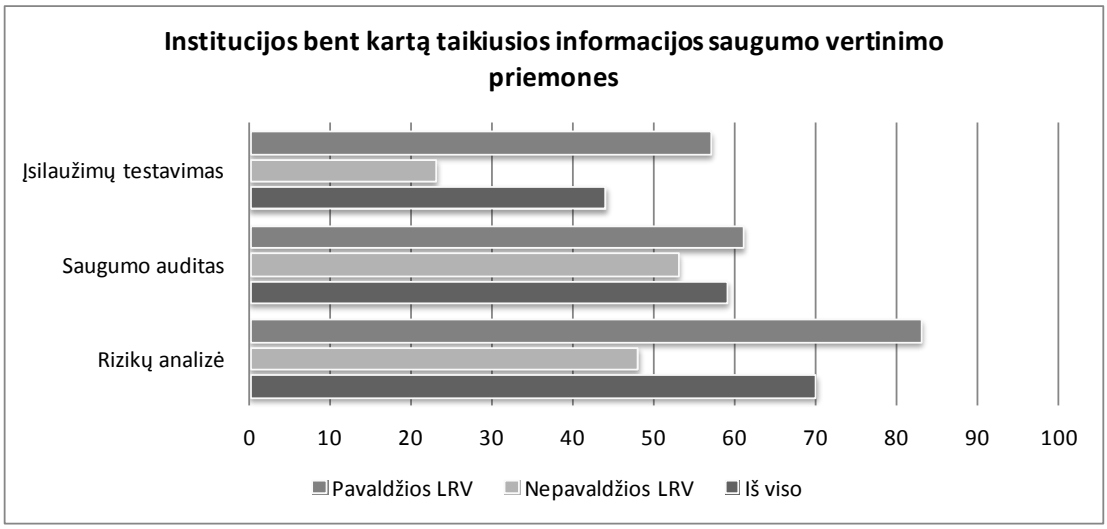
32 pav. Informacijos saugumo valdymo dokumentai Lietuvos valstybės institucijose.

Vertinant informacijos saugumo mokymų organizavimą Lietuvos valstybės institucijose, daugiausia tokių mokymų vykdoma informacinių technologijų personalui – beveik du trečdaliai jų yra dalyvavę mokymuose; mažiausiai valstybės institucijų vadovai – tik apie trečdalis jų dalyvavo tokiuose mokymuose (33 paveikslas). Tyrimo rezultatai taip pat akivaizdžiai atskleidžia, kad informacijos saugumo mokymai nėra nuolatinio pobūdžio: bent kartą per metus saugumo mokymuose yra dalyvę mažiau nei 20 proc. informacinių technologijų ar informacijos saugumo personalo, o dažniau nei kartą per metus tokiuose mokymuose dalyvauja vos 5 proc.



33 pav. Informacijos saugumo mokymų vykdymas Lietuvos valstybės institucijose.

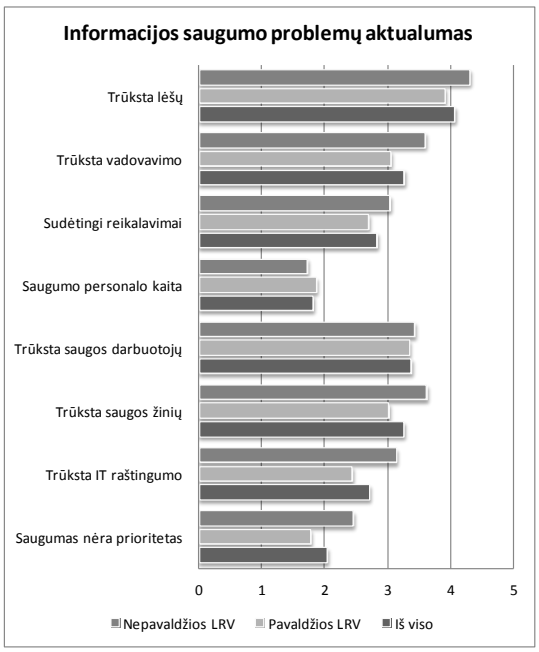
Analizuojant valstybės institucijose taikomas informacijos saugumo vertinimo priemones, populiariausios priemonės – rizikų analizė ir saugumo auditas, atitinkamai apie 70 proc. ir 60 proc. tyrime dalyvavusių institucijų yra jas bent kartą taikiusios. Įsilaužimų testavimą išbandė 44 proc. tirtų institucijų. Vertinant nuolatinį tokių priemonių taikymą, jis nesiekia nei 10 proc. (34 paveikslas). Informacijos saugumo vertinimo priemonių taikymo skirtumai itin ryškūs atsižvelgiant į valstybės institucijų statusą – 83 proc. pavaldžių Lietuvos Respublikos Vyriausybei institucijų nors kartą taikė rizikų analizę (ministerijų atveju – 92 proc.), o tarp nepavaldžių Vyriausybei institucijų – mažiau nei 50 proc.; įsilaužimų testavimo priemones taikė atitinkamai 57 ir 23 proc. institucijų. Manytina, kad šie skirtumai susiformavo dėl galiojančių informacijos saugumo valdymo reikalavimų pobūdžio – rizikų analizės vykdymas yra apibrėžtas Vyriausybės patvirtintuose *Bendruosiuose elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimuose*, taigi yra privalomas pavaldžioms Vyriausybei institucijoms ir tik rekomendacinio pobūdžio – nepavaldžioms. Šie kiekybinio tyrimo rezultatai akivaizdžiai iliustruoja, kad, siekiant užtikrinti reikalavimų laikymąsi (efektyvų informacijos saugumo valdymą), vien rekomendacijų neužtenka.

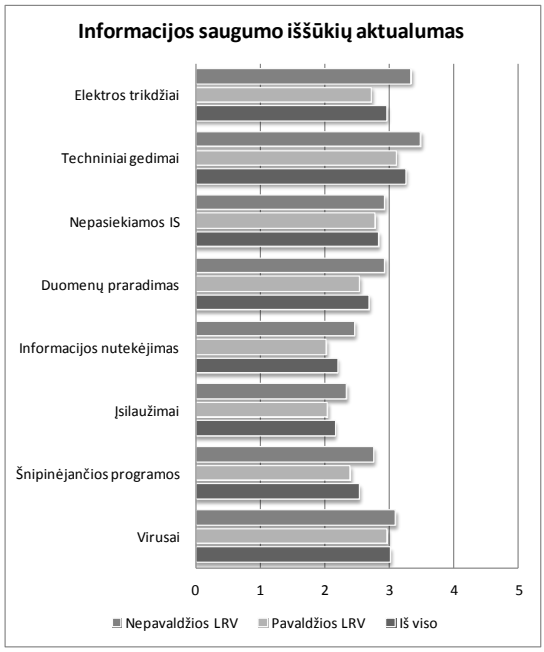


34 pav. Informacijos saugumo vertinimo priemonių taikymas Lietuvos valstybės institucijose.

Išanalizavus Lietuvos valstybės institucijų deklaruotų informacijos saugumo iššūkių ir problemų vertinimo duomenis, kaip bendrą tendenciją galima pastebėti tai, kad valstybės institucijos, tiesiogiai pavaldžios Lietuvos Respublikos Vyriausybei, yra šiek tiek mažiau „jautrios“ informacijos saugumo iššūkiams ir problemoms, tačiau bendros tendencijos yra pakankamai panašios. Valstybės institucijos kaip pagrindinę informacijos saugumo problemą įvardija lėšų trūkumą. Nedaug atsilieka centralizuoto vadovavimo, informacijos saugumo žinių bei informacijos saugumo darbuotojų trūkumas; kaip mažiausia problema įvardijama dažna informacijos saugumo personalo kaita (35 paveikslas).

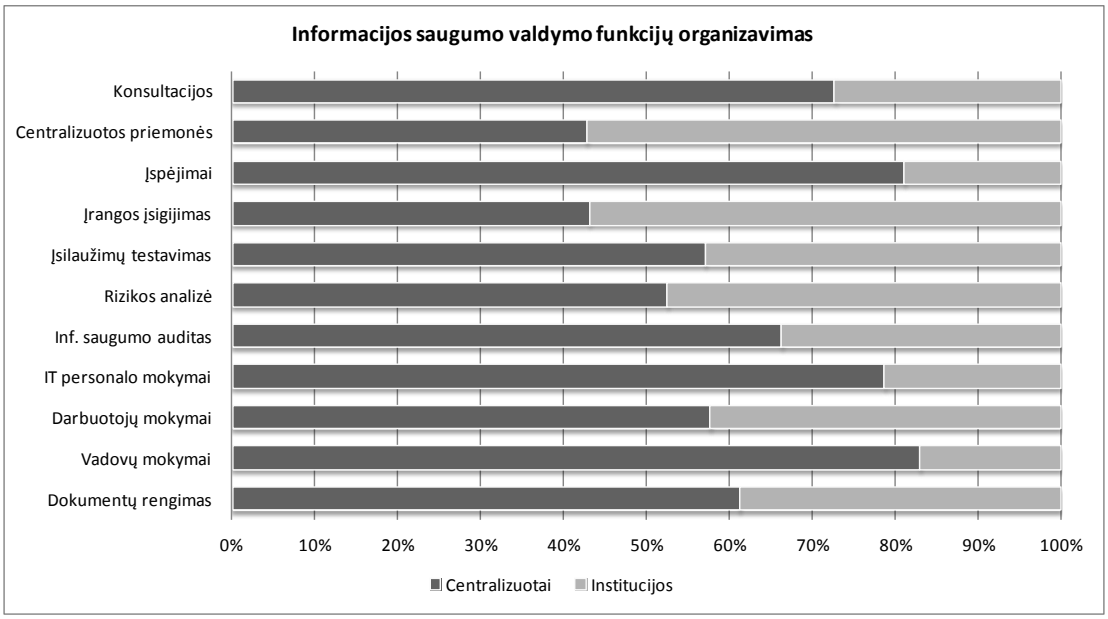
Vertinant saugumo iššūkius keliančias priežastis, kaip svarbiausias valstybės institucijos išskyrė – techninius gedimus, elektros trikdžius (ypač akcentuota institucijų, nepavaldžių Lietuvos Respublikos Vyriausybei, (savivaldos)) ir virusus; mažiausiai problemų tyrime dalyvavusioms valstybės institucijoms kelia įsilaužimai į informacines sistemas ir konfidencialios informacijos nutekėjimas (36 paveikslas).





35 ir 36 pav. Informacijos saugumo problemų ir iššūkių aktualumas.

Vertinant institucijų nuomonę apie informacijos saugumo valdymo funkcijų centralizavimą, labai aiškiai galima išskirti vyraujančius institucijų atsakymus apie tai, kokios funkcijos turėtų būti organizuojamos centralizuotai, – institucijų vadovų ir informacijos technologijų personalo informacijos saugumo mokymai, įspėjimai apie aktualias grėsmes, konsultacijos informacijos saugumo klausimais; prie centralizuotai vykdytinų funkcijų siūloma priskirti informacijos saugumo auditą, informacijos saugumo valdymo dokumentų rengimą, darbuotojų mokymus bei įsilaužimų testavimą. Mažiausio „kišimosi“ tyrime dalyvavusios institucijos pageidautų taikant centralizuotas informacijos saugumo priemones ir įsigyjant informacijos saugumo įrangą (37 paveikslas). Pažymėtina, kad vertinant institucijų pavaldumą nuomonė dėl funkcijų, kurios turėtų būti centralizuotos (vykdomos pačios institucijos), nesikeitė. Savivaldos institucijos tik dar ryškiau akcentavo visų funkcijų centralizuoto vykdymo poreikį (išskyrus tas pačias informacijos saugumo priemonių įsigijimo ir diegimo funkcijas).



37 pav. Valstybės institucijų nuomonė dėl informacijos saugumo valdymo funkcijų organizavimo pobūdžio.

3.7. Empirinio tyrimo išvados

Informacijos saugumo valdymo empirinių tyrimų rezultatai leido pagrįsti integralaus informacijos saugumo valdymo modelio praktinio taikymo galimybes. Taikant šio modelio pagrindu suformuotą informacijos saugumo valdymo vertinimo prieigą, nustatytos informacijos saugumo valdymo problemos Lietuvos valstybės institucijose.

Informacijos saugumo politikos lygmuo.

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, apdorojamą valstybės informaciniais ištekliais (valstybės registrais, žinybiniais registrais, valstybės informacinėmis sistemomis ir vidaus administravimui skirtomis informacinėmis sistemomis).

Šiuo metu galiojantys informacijos saugumo valdymo reikalavimai, taikomi pavieniams valstybės informaciniams ištekliams, turi trūkumų dėl to,

kad šis objektas vienareikšmiškai neapima visos valstybės institucijos valdomos informacijos, taip pat dėl to, jog šiuo metu privalomi informacijos saugumo valdymo reikalavimai nepatvirtinti vidaus administravimui skirtoms sistemoms, kurios sudaro 48 proc. visų Lietuvos valstybės institucijose valdomų informacinių išteklių. Empirinio tyrimo rezultatai atskleidė, kad rekomendacinių informacijos saugumo valdymo reikalavimų nesilaiko daugiau nei pusė Lietuvos valstybės institucijų. Taigi siekiant efektyvaus informacijos saugumo valdymo, turėtų būti patvirtinti privalomi informacijos saugumo valdymo reikalavimai, apimantys visus valstybės informacinius išteklius ir nustatantys, kad kiekvienoje valstybės institucijoje būtų vienas informacijos saugumo valdymo politikos dokumentas (duomenų saugos nuostatai), kuriuo būtų bendrai apibrėžiami visi tos valstybės institucijos valdomi informaciniai ištekliai.

Informacijos saugumo valdymo reikalavimų tikslas turėtų būti – užtikrinti visos valstybės institucijos valdomos informacijos konfidencialumą, vientisumą ir prieinamumą (šiuo metu nėra vienareikšmiškai apibrėžtas prieinamumo tikslo siekinys). Šių tikslų prioritetai turėtų būti nusistatomi pagal konkrečios institucijos valdomos informacijos specifiką, pagal tai parenkant ir taikomas informacijos saugumo užtikrinimo strategines, žmogiškąsias ir technines priemones. Atsižvelgiant į empirinio tyrimo rezultatus, kurie išryškino, kad institucijos neturi pakankamai kompetencijos pačios nusistatyti prioritetų efektyviam ir bendram informacijos saugumo valdymo procesui užtikrinti, turėtų būti parengti aiškūs prioritetų nustatymo ir priemonių pasirinkimo kriterijai.

Informacijos saugumo strategijos lygmuo.

Empirinio tyrimo metu buvo nustatyta, kad valstybės informacijos saugumo valdymo strategija patvirtinta ir nustato ilgalaikius tikslus, uždavinius bei šių siekinių vertinimo kriterijus, tačiau vis dar neapsispręsta dėl detalių įgyvendinimo veiksmų. Taip pat pažymėtina, kad strategijai įgyvendinti nėra užtikrintas nuolatinis informacijos saugumo valdymo ciklas – tik 7 proc. valstybės institucijų nuolat taiko reagavimo į aplinkos pokyčius priemones

(rizikų analizes ir pan.), o informacijos saugumo valdymo priemonės nustatytos neįvertinus ekonominio konteksto (kai kurių galiojančių informacijos saugumo priemonių įgyvendinimas nepagrįstai brangiai kainuoja), taip pat per mažas dėmesys skiriamas žmogiškajam faktoriui.

Informacijos saugumo audito lygmuo.

Lietuvos Respublikos valstybės informacinių išteklių įstatymas ir kiti norminiai dokumentai, formuojantys informacijos saugumo reikalavimus Lietuvos valstybės institucijoms, nustato informacijos saugumo audito vykdymą. Tačiau empirinio tyrimo rezultatai išryškino, kad informacijos saugumo audito procesas nėra tinkamai apibrėžtas ir vykdomas, neužtikrinama kontrolė, kaip valstybės institucijos įgyvendina informacijos saugumo valdymo reikalavimus. Tinkamai neauditуojamas informacijos saugumo politikos įgyvendinimo procesas, atsakingų už informacijos saugumo valdymo koordinavimą institucijų funkcijų vykdymas, dėl to didelė dalis institucijų galiojančius reikalavimus taiko tik formaliai, o informacijos saugumo koordinavimo funkcijas turinčios vykdyti institucijos nėra pajėgios vykdyti savo funkcijų.

Informacijos saugumo veikėjų lygmuo.

Empirinio tyrimo metu nustatytas decentralizuotas informacijos saugumo valdymo organizavimo ir koordinavimo modelis – pavienės sritys formaliai išdalintos atsakingoms valstybės institucijoms (išskyrus kritinės infrastruktūros apsaugos funkciją, kuri vienareikšmiškai niekam nepriskirta), veiklos tarpinstituciniam koordinavimui įkurta kolegiali koordinacinė komisija. Išanalizavus kompetentingų institucijų funkcijas ir jas palyginus su institucijų struktūra, etatų sąrašais bei pareigybių aprašymais, akivaizdžiai matyti, kad koordinuojančios institucijos nėra pajėgios vykdyti iškeltų joms uždavinių – informacijos saugumo organizavimas pasižymi žema institucijų kompetencija, specialistų trūkumu, lėtu paskirtų užduočių sprendimu (pavyzdžiui, Lietuvos Respublikos valstybės informacinių išteklių įstatymas įsigaliojo 2012 m. sausio 1 d., tačiau dauguma jam įgyvendinti reikalingų teisės aktų vis dar neparengta). Kiekybinis informacijos saugumo valdymo Lietuvos valstybės institucijose

tyrimas taip pat padėjo nustatyti rimtą spragą institucijų lygmenyje – 60 proc. atvejų valstybės institucijose už informacijos saugumo valdymą paskirti informacinių technologijų padalinių darbuotojai ar net vadovai. Tokia situacija aiškiai prieštarauja vykdymo ir kontrolės funkcijų atskyrimo principui bei trukdo efektyviai užtikrinti informacijos saugumo valdymą. Šie tyrimų rezultatai taip pat atskleidžia valstybės institucijose vyraujantį techninį požiūrį į informacijos saugumo valdymą.

Siekiant valstybės institucijų veiklos efektyvumo, reikėtų stiprinti koordinuojančias institucijas (vienareikšmiškai ir konkrečiai paskiriant atsakomybę), joms pavesti centralizuoti informacinės infrastruktūros naudojimą (prieš tai ją inventorizavus), teikti centralizuotą metodologinę pagalbą institucijoms (pasitelkiant viešojo, privataus ir mokslo sektorių bendradarbiavimą) bei užtikrinti nuolatinį informacijos saugumo valdymo vertinimą ir kontrolę pagal vienodą metodiką ir aiškius vertinimo kriterijus.

Informacijos saugumo brandos lygmuo.

Empirinio tyrimo metu buvo išryškinti brandos lygių nustatymo ir vertinimo privalumai. Pagal institucijų brandos lygį galėtų būti parenkamos informacijos saugumo valdymo priemonės, svarbesnius išteklius valdančios institucijos turėtų siekti atitinkamai aukštesnio brandos lygmens. Dokumentų turinio analizė leido nustatyti tai, kad valstybės institucijoms informacijos saugumo brandos lygiai ir jų įvertinimo tvarka neapibrėžta. Informacijos saugumo brandos lygiams apibrėžti ir vertinimo tvarkai nustatyti tikslinga pasiremti tarptautinėmis metodikomis ir praktikomis.

Apibendrinant informacijos saugumo valdymo Lietuvos valstybės institucijose tyrimų rezultatus, galima teigti, kad šiuo metu valdomos tik pavienės informacijos saugumo užtikrinimo dalys, trūksta visuminio požiūrio, netaikomi įrankiai, kurie įgalintų valdomo informacijos saugumo, kaip objektyvios saugumo būsenos, sukūrimą ir išlaikymą.

Remiantis aptartais empirinio tyrimo rezultatais, galima išskirti, kokie integralaus informacijos saugumo valdymo modelio elementai neįgyvendinami valdant informacijos saugumą Lietuvos valstybės institucijose.

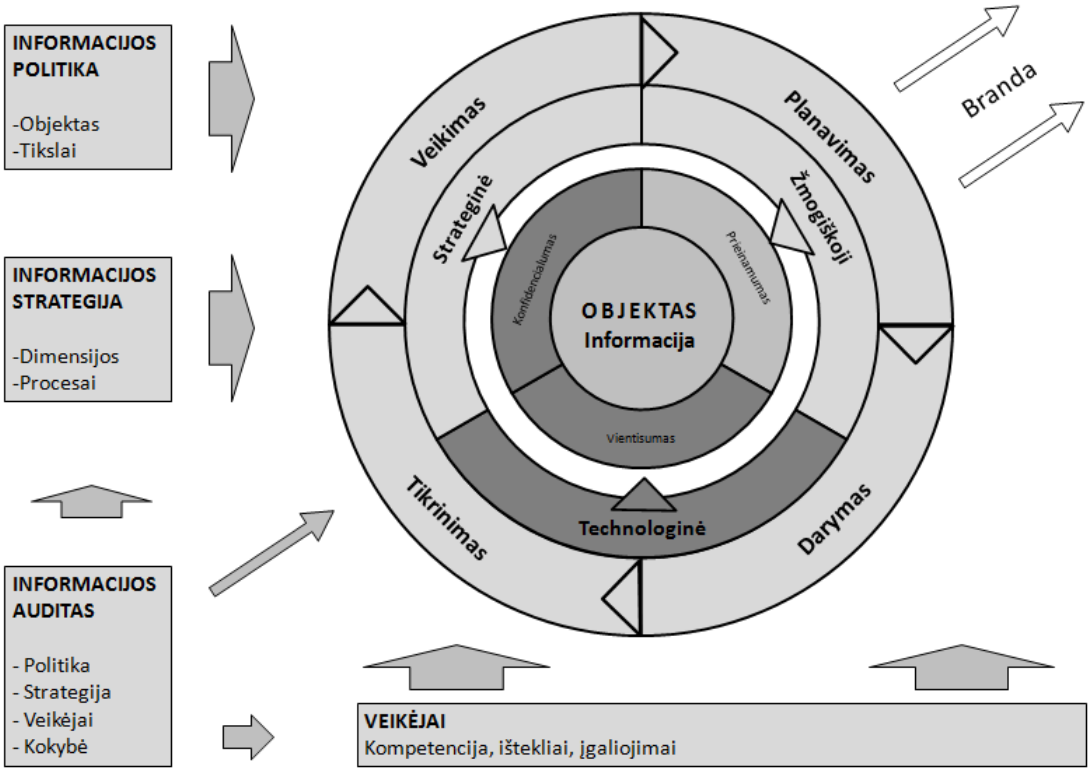
Politikos lygmenyje rastos dvi spragos. Informacijos saugumo valdymo *objektas* (informaciniai ištekliai) turi būti keičiamas arba visiems jo elementams (vidaus administravimo sistemoms, kurios sudaro 48 proc. visų informacinių išteklių) turi būti nustatyti trūkstami tiek gyvavimo ciklo, tiek ir informacijos saugumo reikalavimai. Informacijos saugumo reikalavimai (įtvirtinti įstatymu ir Vyriausybės nutarimais) neapima informacijos *prieinamumo tikslo*. Šio tikslo siekis tampa ypač aktualus vertinant paskutinių metų tendencijas – įvairias kibernetinės erdvės atakas, kai informacijos ištekliai tampa neprieinami.

Strategijos lygmenyje išskirta problema, kad nėra užtikrinamas strategijos įgyvendinimas valstybės lygmenyje, t. y. tiek priimtam *Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymui*, tiek *Elektroninės informacijos saugos (kibernetinio saugumo) programai* įgyvendinti reikalingi teisės aktai dar nepriimti.

Didžiausia problema pastebėta audito lygmenyje – valdant informacijos saugumą Lietuvos valstybės institucijose, neužtikrinama audito funkcija nei valstybės, nei instituciniame lygmenyse. Ši problema lemia tai, kad valstybės institucijos daugumą informacijos saugumo valdymo pareigų atlieka tik formaliai, nėra užtikrinama informacijos saugumo reikalavimų įgyvendinimo kontrolė, nežinoma reali situacija Lietuvos valstybės institucijose, nevaldomi informacijos saugumo procesai.

Vertinant bandos ir veikėjų lygmenis, tyrimo metu paaiškėjo, kad pagrindinės už informacijos saugumo valdymą atsakingos institucijos neturi žmogiškųjų išteklių vykdyti savo funkcijoms, institucijose nepaskirti arba paskirti netinkami saugos įgaliotiniai, o bendrai informacijos saugumo valdymo kokybei (brandai) kelti trūksta esminio elemento – neapibrėžti brandos lygiai ir vertinimo sistema.

Tyrimo rezultatų iliustracija pateikta 38 paveiksle. Šiame paveiksle tamsiai pilka spalva išskirti integralaus informacijos saugumo valdymo modelio elementai, kurie yra apibrėžti ir taikomi Lietuvos valstybės institucijose; šviesiai pilka spalva – nevisiškai apibrėžti arba apibrėžti, tačiau neįgyvendinami; balta spalva – neapibrėžti ir neįgyvendinami.



38 pav. Integralaus informacijos saugumo valdymo modelio įgyvendinimas Lietuvos valstybės institucijose (sudaryta autoriaus).

Empirinio tyrimo rezultatai, leidžia teigti, kad:

1) informacijos saugumo valdymui pasitelkiant informacijos vadybos įrankius gali būti užtikrintas efektyvus informacijos saugumo valdymas;

2) informacijos saugumo valdymo reikalavimai Lietuvos valstybės institucijoms yra fragmentiški;

3) valstybės institucijose, užtikrinant informacijos saugumą, vyrauja techninis formalus požiūris;

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

IŠVADOS

1. Nuolat augantys informacijos saugumo incidentų atvejai ir mastai iliustruoja, kad informacijos saugumo problemų aktualumas tampa kritinis, o esamos informacijos saugumo valdymo priemonės nėra pakankamos informacijos saugumui valdyti. Siaurą informacijos saugumo, kaip technologinės problemos, supratimą plečia ekonominių, vadybinių, psichologinių, teisinių ir kitų susijusių aspektų įtaka informacijos saugumui.

2. Informacijos saugumo valdymo mokslinės problemos laukas nėra visiškai susiformavęs, stebėtina tyrimų plėtra, tačiau vyrauja diskretyvi pavienių aspektų analizė: pernelyg ryškinami technologiniai aspektai; trūksta moksliškai pagrįstų sisteminių informacijos saugumo valdymo konceptų, kurie praplėstų informacijos saugumo valdymo teorinių tyrimų lauką bei lemtų teorinių paradigmų taikymą sprendžiant ryškėjančias praktines informacijos saugumo valdymo problemas tiek Lietuvoje, tiek ir globaliu mastu.

3. Informacijos saugumo valdymui tirti būtina sąlyga – vienareikšmiškai įvardytas objektas, tačiau mokslinių tyrimų bei praktinio taikymo kontekste nepakankamai aiškiai ir pagrįstai pateikiama informacijos saugumo valdymo objekto apibrėžtis (stebimas informacijos, informacinių sistemų, informacijos technologijų ir kitų saugumo objektų vartojimas).

4. Disertacijoje vienareikšmiškai įvardytas informacijos saugumo valdymo objektas – informacija. Objekto įvardijimas leidžia išskirti informacijos saugumo valdymo tikslus bei informacijos saugumo valdymui aktualius aspektus. Moksliniame darbe pagrindiniais informacijos saugumo valdymo tikslais išryškintas informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas, o aspektai, aktualūs informacijos saugumo valdymui, sugrupuoti į strateginę, žmogiškąją ir technologinę dimensijas. Apibendrinus šias įžvalgas, disertacijoje informacijos saugumo valdymas apibrėžtas kaip siekis užtikrinti informacijos konfidencialumą, vientisumą ir

prieinamumą subalansuotai derinant strateginę, žmogiškąją ir technologinę dimensijas.

5. Informacijos saugumo valdymui užtikrinti nepakanka suformuoti jo apibrėžtį, būtina numatyti ir priemones, kuriomis informacijos saugumas galėtų būti valdomas. Teigiant, kad informacijos saugumo valdymo objektas yra informacija, informacijos saugumui valdyti pasitelktini informacijos vadybos metodai ir būdai.

6. Efektyvi informacijos vadyba pasižymi suderintu įrankių taikymu. Informacijos saugumui valdyti išskirti informacijos vadybos įrankiai – politika, strategija, auditas, branda ir veikėjai. Jungiant informacijos saugumo valdymo apibrėžtį ir išskirtus informacijos vadybos įrankius, siekiama, kad būtų apibrėžta informacijos saugumo valdymo politika ir strategija, nuolat atliekamas auditas, valdomi visi informacijos saugumo užtikrinimo procesai, operatyviai prisitaikoma prie aplinkos pokyčių, paskirti kompetentingi veikėjai bei siekiamas aukštas brandos lygis. Suderinus šių įrankių taikymą, galima pagrįstai tikėtis, kad bus užtikrintas efektyvus informacijos saugumo valdymas.

Identifikavus ir kritiškai įvertinus informacijos vadybos bei informacijos saugumo valdymo diskursų sąsajas sukurtas teorinis pagrindas suformuoti integralų informacijos saugumo valdymo modelį.

7. Teorinis integralus informacijos saugumo valdymo modelis suformuoja sisteminį požiūrį į informacijos saugumo valdymo turinį, nusakantį objektą, tikslus bei priemones, ir apibrėžia informacijos vadybos įrankius, kurie sudaro sąlygas įvertinti ir užtikrinti informacijos saugumo valdymo kompleksiškumą. Modelio kompleksiškumą išryškina ir tai, kad modelyje integruoti informacijos vadybos įrankiai – politika, strategija, auditas, branda ir veikėjai – yra sietini ir su esamų informacijos saugumo valdymo priemonių trūkumais. Taigi informacijos vadybos įrankių įdiegimas informacijos saugumo valdymui leidžia sustiprinti esamas silpnas vietas ir taip užtikrinti efektyvų ir kompleksišką informacijos saugumo valdymą.

8. *Teoriniame lygmenyje sukonstruoto integralaus informacijos saugumo valdymo modelio praktinį reikšmingumą atskleidžia empirinio*

informacijos saugumo valdymo Lietuvos valstybės institucijose tyrimo rezultatai:

- ✓ Specialaus įstatymo, nuosekliai reglamentuojančio su informacijos saugumu susijusius santykius, Lietuvoje nėra. 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, apdorojamą valstybės informaciniais ištekliais (valstybės registrais, žinybiniais registrais, valstybės informacinėmis sistemomis ir vidaus administravimui skirtomis informacinėmis sistemomis).
- ✓ Informacijos saugumo valdymo reikalavimai, taikomi pavieniams valstybės informaciniams ištekliams, turi trūkumų – šis objektas vienareikšmiškai neapima visos valstybės institucijos valdomos informacijos, o privalomi informacijos saugumo valdymo reikalavimai nepatvirtinti vidaus administravimui skirtoms sistemoms, kurios sudaro 48 proc. visų Lietuvos valstybės institucijose valdomų informacinių išteklių (šiems ištekliams reikalavimai yra rekomendacinio pobūdžio, o rekomendacinių informacijos saugumo valdymo reikalavimų nesilaiko daugiau nei pusė Lietuvos valstybės institucijų).
- ✓ Valstybinė informacijos saugumo valdymo strategija dokumentuota, nustatyti ilgalaikiai tikslai, uždaviniai bei šių siekinių vertinimo kriterijai, tačiau vis dar neapsispręsta dėl detalių įgyvendinimo veiksmų bei nepriimti strateginiams nuostatams įgyvendinti reikalingi teisės aktai.
- ✓ Nuolatinis informacijos saugumo valdymo ciklas nėra užtikrintas – tik 7 proc. valstybės institucijų nuolat taiko reagavimo į aplinkos pokyčius priemones (rizikų analizes ir pan.), o informacijos saugumo valdymo priemonės nustatytos neįvertinus ekonominio konteksto (kai kurių galiojančių informacijos saugumo priemonių

įgyvendinimas nepagrįstai brangiai kainuoja), taip pat per mažas dėmesys skiriamas žmogiškajam faktoriui.

- ✓ Norminiai dokumentai, formuojantys informacijos saugumo reikalavimus Lietuvos valstybės institucijoms, nustato informacijos saugumo audito vykdymą. Tačiau pats informacijos saugumo audito procesas nėra tinkamai apibrėžtas ir vykdomas, neauditуojama informacijos saugumo politika ir jos įgyvendinimo procesas, atsakingų už informacijos saugumo valdymo koordinavimą institucijų funkcijų vykdymas, neužtikrinama kontrolė, kaip valstybės institucijos įgyvendina informacijos saugumo valdymo reikalavimus, nežinoma reali situacija Lietuvos valstybės institucijose, nevaldomi informacijos saugumo procesai. Didelė dalis valstybės institucijų galiojančius reikalavimus taiko tik formaliai.
- ✓ Informacijos saugumo valdymui koordinuoti Lietuvoje taikomas decentralizuotas modelis – su informacijos saugumo valdymo koordinavimu susijusios funkcijos paskirtos kelioms institucijoms (išskyrus kritinės infrastruktūros apsaugos funkciją, kuri vienareikšmiškai niekam nepriskirta), įkurtas kolegialus tarpinstitucinio koordinavimo organas – nuolatinė komisija. Tačiau informacijos saugumą koordinuojančios institucijos nėra pajėgios vykdyti iškeltų joms uždavinių – informacijos saugumo organizavimas pasižymi žema institucijų kompetencija, specialistų trūkumu, lėtu paskirtų užduočių sprendimu.
- ✓ Lietuvos valstybės institucijose vyrauja techninis požiūris į informacijos saugumą; tinkamai neatskirtos informacijos saugumo valdymo įgyvendinimo ir kontrolės funkcijos trukdo efektyviai užtikrinti informacijos saugumo valdymą (tyrimo rezultatai atskleidė, kad 60 proc. atvejų valstybės institucijose už informacijos saugumo valdymą paskirti informacinių technologijų padalinių darbuotojai ar net vadovai).

- ✓ Informacijos saugumo brandos lygiai ir jų įvertinimo tvarka Lietuvos valstybės institucijoms neapibrėžti. Branda yra vienas svarbiausių sėkmingo tikslų įgyvendinimo ir valdymo procesų tobulinimo veiksnių, pagal institucijų brandos lygį turėtų būti parenkamos informacijos saugumo valdymo priemonės, svarbesnius išteklius valdančios institucijos turėtų siekti atitinkamai aukštesnio brandos lygmens.

9. *Empirinio tyrimo rezultatai leidžia teigti:*

- ✓ užtikrinant informacijos saugumą Lietuvos valstybės institucijose valdomos tik pavienės informacijos saugumo užtikrinimo dalys, vyrauja formalus techninis požiūris, netaikomi įrankiai, kurie įgalintų valdomo informacijos saugumo, kaip objektyvios saugumo būsenos, sukūrimą ir išlaikymą;
- ✓ Lietuvos viešajame sektoriuje vyraujantis formalus požiūris į informacijos saugumą pasireiškia patvirtintų, tačiau neįgyvendintų teisės aktų ir neparengtų įgyvendinančių dokumentų gausa (trūksta informacijos saugumo reikalavimams, įtvirtintiems įstatymu ir strateginiais dokumentais, įgyvendinti būtinų teisės aktų; institucijų vidiniai informacijos saugumo valdymo dokumentai neperžiūrimi ir neatnaujinami; formaliai įtvirtintų priemonių tinkamas įgyvendinimas nekontroliuojamas);
- ✓ pastebėta didesnė branda valstybės institucijų, kurioms galiojantys informacijos saugumo valdymo reikalavimai jau ilgą laiką yra privalomojo pobūdžio (ministerijos, kitos Vyriausybei pavaldžios institucijos).

10. *Siekiant efektyvaus informacijos saugumo valdymo Lietuvos valstybės institucijose, šalia aptartų trūkumų šalinimo, informacijos saugumo valdymas turėtų būti tobulinamas šiomis kryptimis:*

- ✓ Lietuvos valstybės institucijoms turėtų būti patvirtinti privalomi informacijos saugumo valdymo reikalavimai, apimantys visus valstybės informacinius išteklius ir nustatantys, kad kiekvienoje

valstybės institucijoje būtų vienas informacijos saugumo valdymo politikos dokumentas (duomenų saugos nuostatai), kuriuo būtų bendrai apibrėžiami visi tos valstybės institucijos valdomi informaciniai ištekliai.

- ✓ Informacijos saugumo valdymo reikalavimų tikslas turėtų būti – užtikrinti visos valstybės institucijos valdomos informacijos konfidencialumą, vientisumą ir prieinamumą (šiuo metu nėra vienareikšmiškai apibrėžtas prieinamumo tikslo siekinys, o tai tampa ypač aktualu vertinant pastarųjų metų tendencijas – įvairias kibernetinės erdvės atakas, kurioms pavykus, informacijos ištekliai tampa neprieinami). Šių tikslų prioritetai turėtų būti nustatomi pagal konkrečios institucijos valdomos informacijos specifiką, pagal tai parenkant ir taikomas informacijos saugumo užtikrinimo strategines, žmogiškąsias ir technines priemones. Atsižvelgiant į tai, kad valstybės institucijos neturi pakankamai kompetencijos pačios nusistatyti prioritetų, bendram efektyviam informacijos saugumo valdymo procesui užtikrinti, turėtų būti parengti aiškūs prioritetų nustatymo ir priemonių pasirinkimo kriterijai.
- ✓ Siekiant valstybės institucijų veiklos efektyvumo, reikėtų stiprinti koordinuojančias institucijas (vienareikšmiškai ir konkrečiai paskiriant atsakomybę), joms pavesti centralizuoti informacinės infrastruktūros naudojimą (prieš tai ją inventorizavus), teikti centralizuotą metodologinę pagalbą institucijoms (pasitelkiant viešojo, privataus ir mokslo sektorių bendradarbiavimą) bei užtikrinti nuolatinį informacijos saugumo valdymo vertinimą ir kontrolę pagal vienodą metodiką ir aiškius vertinimo kriterijus. Informacijos saugumo brandos lygiams apibrėžti ir vertinimo tvarkai nustatyti tikslinga pasiremti tarptautinėmis metodikomis ir praktikomis.

11. Teoriniame lygmenyje sukonstruotas integralus informacijos saugumo valdymo modelis atskleidžia kompleksinį požiūrį į informacijos

saugumą, integruoja informacijos vadybą ir informacijos saugumo valdymą bei leidžia identifikuoti informacijos saugumo valdymo Lietuvos valstybės institucijose trūkumus, o šiuos trūkumus pašalinus, užtikrinti kompleksišką ir efektyvų informacijos saugumo valdymą. Empirinis tyrimas ir gauti rezultatai pagrindė teoriniame lygmenyje sukonstruoto modelio pritaikomumą tiek tolesniems teoriniams moksliniams tyrimams, tiek praktinėje Lietuvos valstybės institucijų veikloje.

Atliktų teorinių ir empirinių tyrimų rezultatai leidžia teigti, kad disertacijos tikslas pasiektas, – teoriniame lygmenyje suformuotas integralus informacijos saugumo valdymo modelis yra teoriškai bei empiriškai patikrintas ir gali būti taikomas Lietuvos Respublikos valstybės institucijoms.

PASIŪLYMAI

Siekiant užtikrinti efektyvų informacijos saugumo valdymą Lietuvos valstybės institucijose, atsižvelgiant į disertacijoje aptartus teorinių ir empirinių tyrimų rezultatus, galima pateikti šiuos apibendrintus siūlymus Lietuvos valstybės institucijų informacijos saugumo valdymo politiką formuojančiai institucijai:

1. Paskirti vieną informacijos saugumo valdymą koordinuojančią instituciją su aiškiai suformuluotomis funkcijomis ir dedikuotais žmogiškaisiais bei finansiniais ištekliais. Informacijos saugumo valdymą koordinuojanti institucija turėtų organizuoti informacijos saugumo valdymo politikos formavimą, reikalavimų rengimą, audito ir rizikų analizės vykdymą, brandos vertinimą, informacijos saugumo mokymus. Šiai institucijai turi būti suteikti aiškūs įgaliojimai ir pareiga kontroliuoti tai, kaip Lietuvos valstybės institucijos įgyvendina informacijos saugumo valdymo reikalavimus.

Sustiprinti ir kitas valstybės institucijas, kurioms paskirtos su informacijos saugumo koordinavimu susijusios funkcijos (elektroninių ryšių, asmens duomenų, incidentų stebėsena, nusikaltimų tyrimas), kad šios institucijos turėtų žmogiškųjų ir finansinių išteklių pavestoms funkcijoms vykdyti arba šias funkcijas perduoti informacijos saugumo valdymą koordinuojančiai institucijai.

Paskirti valstybės instituciją, atsakingą už kritinės infrastruktūros apsaugos funkcijų vykdymą, arba šią funkciją perduoti informacijos saugumo valdymą koordinuojančiai institucijai.

2. Apibrėžti trūkstamus gyvavimo ciklo ir informacijos saugumo valdymo reikalavimus informacinėms sistemoms, kuriose valdoma informacija skirta institucijų vidaus administravimo funkcijoms vykdyti.

3. Apibrėžti reikalavimus informacijos saugumo valdymo auditoriams, nustatyti informacijos saugumo audito vykdymo tvarką.

4. Apibrėžti informacijos saugumo brandos lygius ir nustatyti jų vertinimo tvarką.

5. Patvirtinti valstybiniams informacijos saugumo strateginiams dokumentams (*Valstybės informacinių išteklių valdymo įstatymo, Nacionalinio saugumo strategijos, Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos*) įgyvendinti reikalingas priemones.

6. Praplėsti Lietuvos valstybės institucijoms galiojančius informacijos saugumo valdymo reikalavimus:

a) į šiuos reikalavimus įtraukti informacijos saugumo prieinamumo tikslą;

b) nustatyti, kad šie reikalavimai turi remtis organizacijų branda, saugumo priemonės turi būti parenkamos pagal saugumo tikslų aktualumą, taikytiną konkrečios organizacijos valdomos informacijos svarbai;

c) nustatyti šiuo metu pavieniams valstybės institucijų informaciniams ištekliams taikomų duomenų saugos nuostatų privalomą taikymą bendrai visiems institucijos valdomiems informaciniams ištekliams;

d) nustatyti rekomenduotiną informacijos saugumo įgaliotinių pavaldumą tiesiogiai organizacijos vadovui, atskirti technines funkcijas nuo informacijos saugumo valdymo atsakomybių.

7. Papildyti detalius Lietuvos valstybės institucijoms galiojančius informacijos saugumo valdymo reikalavimus ir, nustatant konkrečias informacijos saugumo valdymo priemones, atsižvelgti į šiuo metu netinkamai reglamentuojamus ekonominius, saugumo kultūros, psichologinius ir kitus aspektus.

8. Viešojo ir privataus sektorių bendradarbiavimo pagrindu įtraukiant ir mokslo sektoriaus atstovus suformuoti patariamąjį informacijos saugumo kompetencijos centrą. Šis centras turėtų vykdyti ekspertinę funkciją padėdamas paskirtai informacijos saugumo valdymą koordinuojančiai institucijai spręsti strateginius informacijos saugumo valdymo klausimus, rengti informacijos saugumo valdymo reikalavimus, vertinti valstybės institucijas bei spręsti iškilusias kritines informacijos saugumo problemas ir incidentus.

LITERATŪRA IR ŠALTINIAI

1. ABBAS, Haider; MAGNUSSON, Christer; YNGSTROM, Louise; HEMANI, Ahmed (2011). Addressing dynamic issues in information security management. *Information Management & Computer Security*, Vol. 19(1), p. 5–24.

2. ABELS, Eileen; JONES, Rebecca; LATHAM, John; MAGNONI, Dee; MARSHALL, G. Joanne (2003) Competencies for Information Professionals of the 21st Century. [interaktyvus]. [žiūrėta 2011 m. rugsėjo 14 d.]. Prieiga per internetą: <http://www.sla.org/PDFs/Competencies2003_revised.pdf>.

3. ABU-MUSA, Ahmad (2009). Exploring the importance and implementation of COBIT processes in Saudi organizations. An empirical study. *Information Management & Computer Security*, Vol. 17(2), p. 73–95.

4. ALELIŪNAS, Irmantas; KINDURYTĖ, Živilė; KIŠKINA, Irina (2009). Valstybės kontrolė. Valstybinio audito ataskaita. Valstybinių institucijų informacinių sistemų valdymas elektroninės valdžios kontekste. 2007 m. rugsėjo 28 d. Vilnius. [interaktyvus]. [žiūrėta 2010 m. rugpjūčio 7 d.]. Prieiga per internetą: <www.vkontrole.lt/auditas_ataskaita.php?2015>.

5. ASCH, Solomon (1952). Social Psychology. Prentice–Hall. New York, p. 668.

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

7. ASLLANI, Arben; LUTHANS, Fred (2003). What knowledge managers really do: an empirical and comparative analysis, *Journal of Knowledge Management*, Vol. 7(3), p. 53–66.

8. Asmens duomenų teisinės apsaugos įstatymas. [interaktyvus]. [žiūrėta 2010 m. rugpjūčio 20 d.]. Prieiga per internetą: <http://www3.lrs.lt/pls/inter2/ dokpaieska.showdoc_l? p_ id=314940>.

9. AMARAL, Paulo (2007). Towards the creation of Security Ontologism for Information Technology, Communications, Information Systems, Information and Knowledge in Organizations. KNOP, J.; SALNIKOV, A.; YASCHENKO, V. NATO Science for Peace and Security Series: Human and Societal Dynamics. A Process for Developing a Common Vocabulary in the Information Security Area. 2007. Amsterdam: IOS Press, p. 62–69.

10. ANDERSON, Ross (1994). Why Cryptosystems Fail. In Communications of the ACM, Vol. 37(11). [interaktyvus]. [žiūrėta 2010 m. liepos 16 d.]. Prieiga per internetą: <http://www.cl.cam.ac.uk/~rja14/Papers/wcf.pdf>.

11. ANDERSON, Ross (2001). Why Information Security is Hard – An Economic Perspective. 17th Annual Computer Security Applications Conference. New Orleans, Louisiana. [interaktyvus]. [žiūrėta 2011 m. vasario 19 d.]. Prieiga per internetą: <http://www.acsac.org/2001/abstracts/thu-1530-b-anderson.html>

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

13. ATKOČIŪNIENĖ, Zenona; MARKEVIČIŪTĖ, Lina (2005). Informacijos išteklių valdymo modeliavimas kokybės vadybos sistemose. Informacijos mokslai, Nr. 32, p. 49–63.

14. ATKOČIŪNIENĖ, Zenona (2009a). Informacijos vadyba verslo organizacijos vadybos sistemoje. ATKOČIŪNIENĖ, Z., JANIŪNIENĖ, E., MATKEVIČIENĖ, R., PRANAITIS, R., STONKIENĖ, M. Informacijos ir žinių vadyba verslo organizacijoje. Monografija. – Vilnius: VU leidykla, 2009, p. 93–142.

15. ATKOČIŪNIENĖ, Zenona (2009b). Žinių vadyba – naujoji įvestis verslo organizacijos valdyme. ATKOČIŪNIENĖ, Z., JANIŪNIENĖ, E., MATKEVIČIENĖ, R., PRANAITIS, R., STONKIENĖ, M. Informacijos ir

žinių vadyba verslo organizacijoje. Monografija. – Vilnius: VU leidykla, 2009, p. 143–294.

16. AUDESTAD, Jan (2005). Four reasons why 100% security cannot be achieved. *Telektronikk*, Vol.1, p. 38–47.

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

18. BARNEY, Jay (1991). Firm Resources and Sustained Competitive Advantage. *Journal of Management*, Vol. 17(1), p. 99–120.

19. BERTINO, Elisa; KHAN, Latifur; SANDHU, Ravi; THURAISINGHAM, Bhavani (2006). Secure knowledge management: confidentiality, trust, and privacy. *Systems, Man and Cybernetics, Part A: Systems and Humans*, Vol. 36(3), p. 429–438.

20. Bendrieji duomenų apsaugos reikalavimai (1997). [interaktyvus]. Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimas Nr. 952 „Dėl duomenų apsaugos valstybės ir vietos savivaldos informacinėse sistemose“. [žiūrėta 2010 m. rugpjūčio 20 d.]. Prieiga per internetą: <http://www3.lrs.lt/pls/inter3/dokpaieska. showdoc_l?p_id=42817>.

21. Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai (2007). [interaktyvus]. Lietuvos Respublikos Vyriausybės 2007 m. balandžio 25 d. nutarimas Nr. 410 „Dėl Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimo Nr. 952 „Dėl duomenų saugos valstybės ir savivaldybių informacinėse sistemose“ pakeitimo“. [žiūrėta 2010 m. rugpjūčio 20 d.]. Prieiga per internetą: <http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=296510>.

22. BJORCK, Fredrik; YNGSTROM, Louise (2009). IFIP world computer congress / sec 2000 revisited. In H. Armstrong and L. Yngstrom, editors, WISE 2 – Proceedings of the IFIP TC11 WG 11.8 Second World Conference on Information Security Education, Perth, Australia, July 2001. International Federation for Information Processing, p. 209–223.

23. BLOODGOOD, James M.; SALISBURY, Wm. David (2001). Understanding the influence of organizational change strategies on information technology and knowledge management strategies. *Decision Support Systems*. Vol. 31(1), p. 55–69.

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

25. BRINKLEY, Donald L.; SCHELL, Roger R. (1995). What Is There to Worry About? An Introduction to the Computer Security Problem. Marshall D. Abrams, Sushil G. Jajodia, H. J. Podell (Eds.), *Information Security: An Integrated Collection of Essays* (1st ed.). IEEE Computer Society Press, Los Alamitos, CA, USA, p. 11–40.

26. BURK, Cornelius Franklin; HORTON, Forest W. (1988). Infomap. A complete guide to discovering corporate information resources. Englewood Cliffs, NJ: Prentice Hall, p. 254.

27. BUZAN, Barry (1997). Žmonės, valstybės ir baimė: tarptautinio saugumo studijos po Šaltojo karo. Vilnius: Eugrimas, 1997.

28. CAELLI, William (2002). Trusted ... Or ... Trustworthy: The Search For A New Paradigm For Computer And Network Security. *Computers and Security*, Vol. 21(5), p. 413–420.

29. CHAFFEY, Dave; WOOD, Steve (2005). Business Information Management. Harlow: Financial Time Prentice Hall, p. 662.

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

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

32. CHANG, Shuchih Ernest; HO, Chienta Bruce (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, Vol. 106(3), p. 345–361.

33. CHOI, Namjoo; KIM, Dan; GOO, Jahyun; WHITMORE, Andrew (2008). Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action. *Information Management & Computer Security*, Vol. 16(5), p. 484–501.

34. CHOO, Chun Wei (2008). [interaktyvus]. [žiūrėta 2011 m. rugsėjo 5 d.]. Prieiga per internetą: <http://choo.fis.utoronto.ca/Imfaq/>.

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

36. CIO Magazine, CSO Magazine, PricewaterhouseCoopers. The Global State of Information Security 2010. [interaktyvus]. [žiūrėta 2010 m. liepos 15 d.]. Prieiga per internetą: <http://www.pwc.com/en_GX/gx/information-securitysurvey/pdf/ pwcsurvey2010 _report.pdf>.

37. CIO Magazine, CSO Magazine, PricewaterhouseCoopers. 2012 Global State of Information Security Survey. [interaktyvus]. [žiūrėta 2012 m. vasario 1 d.]. Prieiga per internetą: <http://www.pwc.com/gx/en/information-security-survey>.

38. Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space (2009). [interaktyvus]. [žiūrėta 2011 m. sausio 16 d.]. Prieiga per internetą: <http://www.official-documents.gov.uk/document/ cm76/7642/ 7642.pdf>.

39. CHOOBINEH, Joobin; DHILLON, Gurpreet; GRIMAILA, Michael R.; REES, Jackie (2007). Management of Information Security: Challenges and Research Directions. Communications of AIS, No. 20, p. 958–971.

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

41. ČĖSNA, Rytis; ŠTITILIS Darius (2000). Kompiuterinės informacijos ir elektroninių dokumentų apsauga viešajame administravime. – Vilnius: LTU, p. 68.

42. D'ARCY, John; HOVAV, Anat. (2009). An Integrative Framework for the Study of Information Security Management Research. Jatinder Gupta

and Sushil Sharma (Eds.), Handbook of Research on Information Security and Assurance, Idea Group Publishing, p. 55–67.

43. DAVENPORT, Thomas; ECCLES, Robert; PRUSAK, Laurence (1992). Information Politics [interaktyvus]. [Žiūrėta 2012 m. vasario 3 d.]. Prieiga per internetą: <http://www.sims.monash.edu.au/subjects/ims5042/stuff/readings/Davenport_Eccles_Prusak.pdf>.

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

45. DEBOWSKI, Shelda (2006). Knowledge management. John Wiley & Sons Australia, Milton, Qld, p. 368.

46. Defence in depth. Summary Report for CIOs and CSO (2008). [interaktyvus]. [žiūrėta 2011 m. rugpjūčio 7 d.]. Prieiga per internetą: <http://tisn.gov.au/www/tisn/content.nsf/Page/Publications_PublicationsbyTopic>.

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

48. DENNING, E. Dorothy (1999). Information warfare and security. United States of America: ACM Press, p. 544.

49. DETLOR, Brian (2010). Information management. *International Journal of Information Management*, Vol. 30(2), p. 103–108.

50. DHILLON, Gurpreet; BACKHOUSE, James (2001). Current Directions in IS Security Research: Toward Socio-Organizational Perspectives, *Information Systems Journal*. Vol. 11(2), p. 127–153.

51. DLAMINI, Moses; ELOFF, Jan; ELOFF, Mariki (2009). Information security: The moving target, *Computers & Security*, Vol. 28, Issues 3–4, p. 189–198.

52. DOHERTY, Neil F.; FULFORD, Heather (2006). Aligning the information security policy with the strategic information systems plan. *Computers & security*. Vol. 25, p. 55–63.

53. EARL, Michael, J. (1996). Information Management: The Organizational Dimension. Oxford: Oxford University Press, p. 536.

54. EHMS, Karsten; LANGEN, Manfred (2002). Holistic Development of Knowledge Management with KMMM. [interaktyvus]. [žiūrėta 2012 m. sausio 17 d.]. Prieiga per internetą: <http://www.kmmm.org/objects/kmmm_article _siemens_2002.pdf>.

55. Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programa (2011). [interaktyvus]. Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimas Nr. 769 „Dėl Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo“. [žiūrėta 2010 m. rugpjūčio 7 d.]. Prieiga per internetą: < http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=403385&p_query=&p_tr2=2>.

56. Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinė strategija iki 2008 metų (2006). [interaktyvus]. Lietuvos Respublikos Vyriausybės 2006 m. birželio 19 d. nutarimas Nr. 601 „Dėl Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinės strategijos iki 2008 metų ir jos įgyvendinimo priemonių plano patvirtinimo“. [žiūrėta 2010 m. rugpjūčio 7 d.]. Prieiga per internetą: <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=278475&p_query=&p_tr2=>.

57. ELOFF, Jan; ELOFF, Mariki (2003). Information Security Management – A New Paradigm, Proceedings of the annual South African Institute of Computer Scientists and Information Technologists conference (SAICSIT), September 2003, Johannesburg, SA, Unisa Press, p. 130–136.

58. EMERY, Priscilla (2003). Document and Records Management: Understanding The Diferences and Embracing Integration. [interaktyvus]. [žiūrėta 2011 m. rugpjūčio 5 d.]. Prieiga per internetą: <http://www.zylab.com/downloads/whitepapers/White%20Paper%20-%20Document%20Management%20vs%20 Records%20Management.pdf>.

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

60. Ernst & Young's 12th annual global information security survey. [interaktyvus]. [žiūrėta 2010 m. liepos 15 d.]. Prieiga per internetą: <http://www.ey.com/Publication/vwLUAssets/12th_annual_GISS/$FILE/12th_annual_GISS.pdf>.

61. EVERARD, Jerry (2001). We are Plato's children. Library Management, Vol. 22(6/7), p. 297–302.

62. FISMA. Federal Information Security Management Act. [interaktyvus]. 2002. [žiūrėta 2010 m. liepos 15 d.]. Prieiga per internetą: <http://csrc.nist.gov/drivers/documents/ FISMA-final.pdf>.

63. FULFORD, Heather; DOHERTY, Neil F. (2003). The application of information security policies in large UK-based organizations: an exploratory investigation. *Information Management & Computer Security*, Vol. 11(3), p. 106–114.

64. GAO. United States Government Accountability Office. INFORMATION SECURITY: Weaknesses Continue Amid New Federal Efforts to Implement Requirements. 2011 m. spalio 3 d. [interaktyvus]. [žiūrėta 2012 m. rugpjūčio 20 d.]. Prieiga per internetą: <http://www.gao.gov/highlights/d12137high.pdf>.

65. GARTNER LTD (2005). Gartner Research Report: Program and Portfolio Information Management Maturity Model. [interaktyvus]. [žiūrėta 2012 m. kovo 2 d.]. Prieiga per internetą: <http://www.strategies-for-managing-change.com/support-files/gartnerprogramportfoliomaturity model.pdf >.

66. GAMULIS, Rimgaudas; KIŠKINA, Irina (2009). Valstybės kontrolė. Išankstinio tyrimo ataskaita. Strateginės informacijos sauga. 2009 m. kovo 16 d. Vilnius. [interaktyvus]. [žiūrėta 2010 m. rugpjūčio 7 d.]. Prieiga per internetą: <http://www.vkontrole.lt/auditas_ataskaita.php?3081>.

67. GARŠVA, Eimantas (2006). Kompiuterių sistemų saugumo modeliavimas. Daktaro disertacija. VGTU. Vilnius: Technika, 2006.

68. GHORMLEY, Yvette (2009). Security Policies and Procedures. Jatinder Gupta and Sushil Sharma (Eds.), Handbook of Research on Information Security and Assurance, Idea Group Publishing, p. 320–330.

69. GILLIES, Alan (2011). Improving the quality of information security management systems with ISO27000. *The TQM Journal*, Vol. 23(4), p. 367–376.

70. GOLD, Andrew H.; MALHOTRA, Arvind; SEGARS, Albert H. (2001). Knowledge Management: An Organizational Capabilities Perspective. *Journal of Management Information Systems*, Vol. 18(1), p. 185–214.

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

72. GORGE, Mathieu (2009). The Future of Security Standards and Laws. ISSA Journal. 2009 September. [interaktyvus]. [žiūrėta 2010 m. rugpjūčio 20 d.]. Prieiga per internetą: https://www.issa.org/Library/Journals/2009/September/Gorge-The%20Future%20of%20Security%20Standards%20and%20Laws.pdf>.

73. GRIFFIN, Jane (2006). Adding Value – Enterprise Information Maturity Model. DM Review Magazine. 2006 February, p. 11–13.

74. GUDAUSKAS, Renaldas (2004). Valstybės žinių ekonomikos politika: žinių vadyba ir entreprenerystė. *Informacijos mokslai*, t. 31, p. 18–34.

75. HALL, Jacqueline H.; SARKANI, Shahram; MAZZUCHI, Thomas A. (2011). Impacts of organizational capabilities in information security. *Information Management & Computer Security*, Vol. 19(3), p. 155–176.

76. HELMS, Marilyn M.; ETTKIN, Lawrence P.; MORRIS, Daniel J. (2000). Shielding your company against information compromise. *Information Management & Computer Security*, Vol. 8(3), p. 117–130.

77. HIGGINS, Huong Ngo (1999). Corporate system security: towards an integrated management approach. *Information Management & Computer Security*, Vol. 7(5), p. 217–222.

78. HIPAA. Health Insurance Portability and Accountability Act. [interaktyvus]. 1996. [žiūrėta 2010 m. liepos 15 d.]. Prieiga per internetą: <http://www.cms.gov/HIPAAGenInfo>.

79. HONG, Kwo-Shing; CHI, Yen-Ping; CHAO, Louis R.; TANG, Jih-Hsing (2003). An integrated system theory of information security management. *Information Management & Computer Security*, Vol. 11(5), p. 243–248.

80. HOVEN, John. (2001). Information Resource Management: Foundation for Knowledge Management. Information systems Management, Vol. 18(2), p. 80–83.

81. IBM (2006). IBM Information Security Framework. [interaktyvus]. [žiūrėta 2011 m. gruodžio 7 d.]. Prieiga per internetą: <http://www-935.ibm.com/services/us/igs/pdf/g510-6454-information-security-framework.pdf>.

82. Informacijos technologijų saugos valstybinė strategija. LR Vyriausybės 2001m. gruodžio 22d. nutarimas Nr. 1625. [interaktyvus]. [žiūrėta 2010 m. rugpjūčio 7 d.]. Prieiga per internetą: <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=157225>.

83. Infosecurity Europe. Information Security Breaches Survey 2010. [interaktyvus]. [žiūrėta 2012 m. liepos 15 d.]. Prieiga per internetą: <http://www.pwc.co.uk/audit-assurance/publications/isbs-survey-2010.jhtml>.

84. Infosecurity Europe. Information Security Breaches Survey 2012. [interaktyvus]. [žiūrėta 2012 m. rugsėjo 28 d.]. Prieiga per internetą: <http://www.pwc.co.uk/audit-assurance/publications/uk-information-security-breaches-survey-results-2012.jhtml>.

85. Išankstinio tyrimo ataskaita. Strateginės informacijos sauga (2009). [interaktyvus]. [žiūrėta 2012 m. liepos 28 d.]. Prieiga per internetą: <http://www.vkontrole.lt/failas_senas.aspx?id=3081>.

86. IT Governance Institute; Office of Government Commerce (2008). Aligning CobiT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit. A Management Briefing From ITGI and OGC. [interaktyvus]. [žiūrėta 2012 m. rugsėjo 28 d.]. Prieiga per internetą: <http://www.isaca.org/Knowledge-Center/Research/Documents/Aligning-COBIT,ITILV3,ISO27002-Bus-Benefit-12Nov08-Research.pdf>.

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

88. JANELIŪNAS, Tomas (2007). Komunikacinis saugumas. – Vilnius: VU leidykla, 2007, p. 219.

89. JENNEX, Murray E.; OLFMAN, Lorne (2005). Assessing Knowledge Management Success. *International Journal of Knowledge Management*, Vol. 1(2), p. 33–49.

90. JENNEX, Murray E.; ZYNGIER, Suzanne (2007). Security as a contributor to knowledge management success. *Information Systems Frontiers*, Vol. 9(5), p. 493–504.

91. JENNEX, Murray E.; SMOLNIK, Stefan; CROASDELL, David T. (2009). Towards a consensus knowledge management success definition. VINE, Vol. 39(2), p. 174–188.

92. JOHNSON, Alice M. (2009). Business and Security Executives Views of Information Security Investment Drivers: Results from a Delphi Study. *Journal of Information Privacy & Security*, Vol. 5(1), p. 3–27.

93. KAYWORTH, Tim; WHITTEN, Dwayne (2010). Effective Information Security Requires a Balance of Social and Technology Factors. MIS Quarterly Executive, Vol. 9(3). Mays Business School Research Paper No. 2012-52. [interaktyvus]. [žiūrėta 2012 m. birželio 15 d.]. Prieiga per internetą: < http://ssrn.com/abstract=2058035>.

94. KARDELIS, Kęstutis (2002). Mokslinių tyrimų metodologija ir metodai. Kaunas, p. 330.

95. KASPERAVIČIUS, Petras; ŽILINSKAS, Vytautas (2004). Intelektinė nuosavybė ir jos apsauga. – Klaipėda: Klaipėdos universiteto leidykla, 2004, p. 397.

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

97. KELLY, Maxim. (2007). Chocolate the key to uncovering PC passwords. The Register. [interaktyvus]. [žiūrėta 2012 m. kovo 15 d.]. Prieiga per internetą: <http://www.theregister.co.uk/2007/04/17/chocolate_password_survey/>.

98. KING, William R.; MARKS, Jr. Peter V.; McCOY, Scott (2002). The most important issues in knowledge management. Communications of the ACM, Vol. 45(9), p. 93–97.

99. KIŠKIS, Mindaugas (2009). Intelektinės nuosavybės elektroninėje erdvėje ypatumai ir teisinis reglamentavimas. Teisė: mokslo darbai. 2009, t. 71, p. 41–52.

100. KNAPP, Kenneth J.; MARSHALL, Thomas E.; RAINER, R. Kelly; FORD, F. Nelson (2006). Information security: management's effect on culture and policy. Information Management & Computer Security, Vol. 14(1), p. 24–36.

101. KUTTSCHREUTER, M.; GUTTELING, J.M (2004). Time will tell: changes in risk perception and the processing of risk information about the Y2K-risk. Computers in Human Behavior, 2004, p. 801–821.

102. LIEBESKIND, Julia Porter (1996). Knowledge, strategy, and the theory of the firm. Strategic Management Journal, Vol. 17, p. 93–107.

103. Lietuvos informacinės visuomenės plėtros 2011–2019 metų programa (2011). [interaktyvus]. Patvirtinta 2011 m. kovo 16 d. nutarimu Nr. 301 „Dėl Lietuvos informacinės visuomenės plėtros 2011–2019 metų programos patvirtinimo ir kai kurių Lietuvos Respublikos Vyriausybės nutarimų pripažinimo netekusiais galios“. [žiūrėta 2012 m. rugpjūčio 10 d.].

Prieiga per internetą: <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=394457&p_query=&p_tr2=>.

104. Lietuvos pažangos strategija „Lietuva 2030“ (2012). [interaktyvus]. [žiūrėta 2012 m. rugsėjo 10 d.]. Prieiga per internetą: <http://www.lietuva2030.lt/images/stories/2030.pdf>.

105. Lietuvos Respublikos elektroninių ryšių įstatymas. [interaktyvus]. [žiūrėta 2012 m. vasario 10 d.]. Prieiga per internetą: <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=232036>.

106. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. [interaktyvus]. [žiūrėta 2012 m. vasario 10 d.]. Prieiga per internetą: <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=400103>.

107. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas. [interaktyvus]. [žiūrėta 2012 m. rugsėjo 12 d.]. Prieiga per internetą: <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=415499&p_query=&p_tr2=2>.

108. Lietuvos Respublikos valstybės registrų įstatymas. [interaktyvus]. [žiūrėta 2012 m. rugpjūčio 20 d.]. Prieiga per internetą: <http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=359302>.

109. Lietuvos Respublikos vidaus reikalų ministerijos Elektroninės valdžios politikos skyriaus nuostatai (2011). [interaktyvus]. Patvirtinti 2011 m. kovo 24 d. įsakymu Nr. 1V-244 „Dėl Lietuvos Respublikos vidaus reikalų ministerijos Elektroninės valdžios politikos skyriaus nuostatų patvirtinimo“. [žiūrėta 2012 m. rugpjūčio 20 d.]. Prieiga per internetą: <http://www.vrm.lt/fileadmin/Padaliniu_failai/El_valdzios_politikos_sk/20110324_Nr1V-244_EVPS_nuostatai_pasirasyti.pdf>.

110. Lietuvos Respublikos vidaus reikalų ministerijos Elektroninės valdžios politikos skyriaus nuostatai (2012). [interaktyvus]. Patvirtinti 2012 m. lapkričio 5 d. įsakymu Nr. 1V-778 „Dėl Lietuvos Respublikos vidaus reikalų ministerijos Elektroninės valdžios politikos skyriaus nuostatų patvirtinimo“. [žiūrėta 2012 m. lapkričio 7 d.]. Prieiga per internetą: <http://www.vrm.lt/go.php/lit/ELEKTRONINES-VALDZIOS-POLITIKOS-SKYRIUS/15>.

111. LINDSEY, Kelley (2002). Measuring Knowledge Management Effectiveness: A Task-Contingent Organizational Capabilities Perspective, Eighth Americas Conference on Information Systems, p. 2085–2090.

112. LOMAS, Elizabeth (2010). Information governance: information security and access within a UK context. Records Management Journal, Vol. 20(2), p. 182–198.

113. LORENTS, Peeter; RAIN, Ottis; RIKK, Raul (2009). Cyber Society and Cooperative Cyber Defence. AYKIN, Nuray. Internationalization, Design and Global Development. Lecture Notes in Computer Science. 2009. Berlin: Springer/Heidelberg, p. 180–186.

114. LOUKIS, Euripidis; SPINELLIS, Diomidis (2001). Information systems security in the Greek public sector. *Information Management & Computer Security*, Vol. 9(1), p. 21–31.

115. MACEVIČIŪTĖ, Elena; WILSON, Tom (2005). The Development of the Information Management Research Area. Introducing information management: an information research reader. London: Facet publishing, p. 18–30.

116. MARKEVIČIŪTĖ, Lina (2008). Informacijos vadybos aprėptys ir sąsajos. *Informacijos mokslai*, Nr. 44, p. 56–76.

117. MARKEVIČIŪTĖ, Lina (2009). Informaciniai kokybės vadybos sistemos brandos veiksniai. Daktaro disertacija. Vilnius.

118. MARCHAND, Donald, HORTON, Forest (1986). Infotrends: Profiting from Your Information Resources. New York: John Wiley and Sons, p. 342.

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

120. McFADZEAN, Elspeth; EZINGEARD, Jean-Noël; BIRCHALL, David (2006). Anchoring information security governance research: sociological groundings and future directions. Journal of Information Systems Security, Vol. 2(3), p. 3–48.

121. McFADZEAN, Elspeth; EZINGEARD, Jean-Noel; BIRCHALL, David (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. Online Information Review, Vol. 31 (5), p. 622–660.

122. McLEAN, John Security Models and Information Flow. [interaktyvus]. [žiūrėta 2010 m. liepos 15 d.]. Prieiga per internetą: <http://www.cs.cornell.edu/andru/cs711/ 2003fa/reading/ 1990mclean-sp.pdf>.

123. MIKALAUSKIENĖ, Audronė; BRAZAITIS, Zenonas (2010). Informacinių sistemų sauga. Vilnius: VU leidykla, 2010, p. 280.

124. MIKUČIONIS, Mindaugas; TOLDINAS, Eugenijus; VENČKAUSKAS, Algimantas (2007). Korporacinių įmonių informacinės saugos architektūrų modeliavimas. Informacijos mokslai, t. 42–43, p. 175–181.

125. MITNICK, Kevin; SIMON, William (2002). The Art of deception: Controlling the Human Element of Security. Indianapolis, USA: Wiley Publishing, Inc., p. 352.

126. MOREIRA, Edson dos Santos; MARTIMIANO, Luciana Andréia Fondazzi; BRANDÃO, Antonio José dos Santos; BERNARDES, Mauro César (2008). Ontologies for information security management and governance. *Information Management & Computer Security*, Vol. 16(2), p. 150–165.

127. Nacionalinio saugumo strategija (2012). [interaktyvus]. Patvirtinta Lietuvos Respublikos Seimo 2012 m. birželio 26 d. nutarimu Nr. XI-2131 „Dėl Lietuvos Respublikos Seimo nutarimo „Dėl Nacionalinio saugumo strategijos patvirtinimo“ pakeitimo“. [žiūrėta 2012 m. rugsėjo 5 d.]. Prieiga per internetą: <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=428981&p_query=&p_tr2=2>.

128. NATO (2010). Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation. [interaktyvus]. 2010. [žiūrėta 2011 m. balandžio 5 d.]. Prieiga per internetą: <http://www.nato.int/cps/en/natolive/official_texts_68580.htm>.

129. NOHLBERG, Marcus (2008). Securing Information Assets: Understanding, Measuring and Protecting Against Social Engineering Attacks.

Department of Computer and Systems Sciences (together with KTH), Stockholm University, p. 88.

130. NONAKA, Ikujiro; TAKEUCHI, Hirotaka (1995). The Knowledge Creating Company: How Japanese Companies Create The Dynamics of Innovation, New York: Oxford University Press, p. 284.

131. NORDIN, Mohamed; PAULEEN, David J.; GORMAN, Gary (2009). Investigating KM antecedents: KM in the criminal justice system, *Journal of Knowledge Management*, Vol. 13(2), p. 4–20.

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

133. PARAKKATTU, Sindhuja; KUNNATHUR, Anand. S (2010). A Framework for research in information security management. Proceedings for the Northeast Region Decision Sciences Institute (NEDSI), 2010, p. 318–323.

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

135. PARKER, B. Donn (1998). Fighting computer crime: A new framework for protecting information. New York, USA: John Wiley & Sons, Inc., p. 528.

136. PAŠKAUSKAS, Žydrūnas (2007). Elektroninės informacijos saugos tarptautinio teisinio reguliavimo analizė: Lietuvos padėtis. Jurisprudencija. Mokslo darbai. Nr. 5(83), p. 82–89.

137. PAULAUSKAS, Nerijus (2009). Incidentų kompiuterių sistemose tyrimas ir saugumo lygio įvertinimas. Daktaro disertacija. VGTU. Vilnius: Technika, 2009.

138. POLANYI, Michael (1982). Personal Knowledge: Towards a Post-critical Philosophy. University of Chicago Press, p. 428.

139. PROBST, Gilbert; RAUB, Steffen; ROMHARDT, Kai (1999). Managing knowledge: building blocks for success. Chichester: John Wiley&Sons LTD, p. 368.

140. PRUSAK, Laurence (2001). Where did knowledge management come from? *IBM Systems Journal*, Vol. 40 (4), p. 1002–1007.

141. PSI. Payment Card Industry Data Security Standard. [interaktyvus]. 2008. [žiūrėta 2010 m. liepos 15 d.]. Prieiga per internetą: <https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml>.

142. RANDEREE, Ebrahim (2006). Knowledge management: securing the future. *Journal of Knowledge Management*, Vol. 10 (4), p. 145–156.

143. RATHNAM, R. G.; JOHNSEN, Justin; WEN, H. Joseph (2004). Alignment of business strategy and IT strategy: a case study of a fortune 50 financial services company. *Journal of Computer Information Systems*, Vol. 45(2), p. 1–8.

144. RYAN, Johnny. Analizė „I. karas“: nauja grėsmė, jos parankumas ir didėjantis mūsų pažeidžiamumas. [interaktyvus]. 2008. Nato apžvalga. [žiūrėta 2011 m. vasario 3 d.]. Prieiga per internetą: <http://www.nato.int/docu/review/2007/issue4/lithuanian/analysis2.html> .

145. RRT (2010). Ryšių reguliavimo tarnyba. Lietuvos Respublikos nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio informacija. [interaktyvus]. 2006–2010. [žiūrėta 2011 m. balandžio 5 d.]. Prieiga per internetą: <https://www.cert.lt>.

146. RUSSELL, Deborah; GANGEMI GT (1991). Computer security basics. United States of America: O'Reilly & Associates, Inc.

147. SALISBURY, W. Mark (2003). Putting theory into practice to build knowledge management systems. *Journal of Knowledge Management*. Vol. 7 (2), p. 128–141.

148. SCHELL, Rodger R. (2001). Information Security: Science, Pseudoscience, and Flying Pigs. Proceedings of the 17th Annual Computer Security Applications Conference, December 10–14, 2001, New Orleans, LA.

149. SCHLÖGL, Christian. (2005). Information and knowledge management: dimensions and approaches. Information Research, 10 (4) [interaktyvus]. [žiūrėta 2011 m. rugsėjo 2 d.]. Prieiga per internetą: <http://InformationR.net/ir/10-4/paper235.html>.

150. SHARMA, Sushil; GUPTA, Jatinder (2009). Information Security Policies: Precepts and Practices. Jatinder Gupta and Sushil Sharma (Eds.),

Handbook of Research on Information Security and Assurance, Idea Group Publishing, p. 341–346.

151. SIPONEN, Mikko; OINAS-KUKKONEN, Harri (2007). A Review of Information Security Issues and Respective Research Contributions, The Data Base for Advances in Information Systems, p. 60–80.

152. SKYRME, David (1999). Information resource management. Insight. [interaktyvus]. [žiūrėta 2011 m. rugsėjo 1 d.]. Prieiga per internetą: <http://www.skyrme.com/insights/8irm.htm>.

153. SMITH, Stephen; JAMIESON, Rodger; BUNKER, Deborah; WINCHESTER, Donald (2008). Moving Towards Information System Security Accreditation within Australian State Government Agencies. AMCIS 2008 Proceedings. Paper 46. [interaktyvus]. [žiūrėta 2010 m. rugpjūčio 7 d.]. Prieiga per internetą: <http://aisel.aisnet.org/amcis2008/46>.

154. SOX. Sarbanes-Oxley Act (2002). [interaktyvus]. [žiūrėta 2010 m. liepos 15 d.]. Prieiga per internetą: <http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/content-detail.html/>.

155. Strateginio planavimo metodika (2002). [interaktyvus]. Patvirtinta Lietuvos Respublikos Vyriausybės 2002 m. birželio 6 d. nutarimu Nr. 827 „Dėl Strateginio planavimo metodikos patvirtinimo“. [žiūrėta 2012 m. liepos 15 d.]. Prieiga per internetą: <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=397970&p_query=&p_tr2=2>.

156. STONKIENĖ, Marija (2009). Informacijos nuosavybės teisių apsauga verslo organizacijoje. ATKOČIŪNIENĖ, Z., JANIŪNIENĖ, E., MATKEVIČIENĖ, R., PRANAITIS, R., STONKIENĖ, M. Informacijos ir žinių vadyba verslo organizacijoje. Monografija. – Vilnius: VU leidykla, 2009, p. 347–415.

157. SUSANTO, Heru; ALMUNAWAR, Mohammad Nabil; TUAN, Yong Chee (2011). Information Security Management System Standards: A Comparative Study of the Big Five. International Journal of Engineering and Computer Science. IJENS Publishers. Vol. 11(5), p. 23–29.

158. ŠERPENSKAS, Eimantas (2001). Informacijos apsauga Lietuvoje. Informacijos mokslai, Nr. 18, p. 110–114.

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

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

161. TIMKO, Dan (2008). The Social Engineering Threat. ISSA Journal. [interaktyvus]. 2008 January. [žiūrėta 2010 m. liepos 16 d.]. Prieiga per internetą: <https://www.issa.org/Library/Journals/2008/January/Timko-The%20Social%20Engineering %20Threat.pdf>.

162. Tinklų ir informacijos saugumo būklės Lietuvoje tyrimas. Lietuvos Respublikos ryšių reguliavimo tarnyba. Tyrimai. 2009. [interaktyvus]. [žiūrėta 2010 m. rugpjūčio 15 d.]. Prieiga per internetą: <http://www.esaugumas.lt/index.php?43190571>.

163. TSOHOU, Angeliki; KOKOLAKIS, Spyros; KARYDA, Maria; KIOUNTOUZIS, Evangelos (2008). Process-variance models in information security awareness research. *Information Management & Computer Security*, Vol. 16(3), p. 271–287.

164. TSOHOU, Angeliki; KOKOLAKIS, Spyros; LAMBRINOUDAKIS, Costas; GRITZALIS, Stefanos (2010). A security standards' framework to facilitate best practices' awareness and conformity. Information Management & Computer Security, Vol. 18(5), p. 350–365.

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

166. UPADHYAYA, Shambhu; RAO, Raghav; PADMANABHAN, G. (2006). Secure knowledge management. In D. G. Schwartz (Ed.) Encyclopedia of knowledge management Hershey, PA: Group Reference, p. 795–801.

167. Valstybės informacinių sistemų steigimo ir įteisinimo taisyklės (2004). [interaktyvus]. Patvirtintos 2004 m. balandžio 19 d. nutarimu Nr. 451

„Dėl Valstybės informacinių sistemų steigimo ir įteisinimo taisyklių patvirtinimo“. [žiūrėta 2011 m. rugsėjo 15 d.]. Prieiga per internetą: <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=398483>.

168. Valstybės registrų ir kadastrų steigimo, reorganizavimo ir likvidavimo taisyklės (2005). [interaktyvus]. Patvirtintos 2005 m. gegužės 3 d. nutarimu Nr. 485 „Dėl Valstybės registrų ir kadastrų steigimo, reorganizavimo ir likvidavimo taisyklių ir Lietuvos Respublikos valstybės registro tipinių nuostatų patvirtinimo“. [žiūrėta 2011 m. rugsėjo 15 d.]. Prieiga per internetą: <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=386119>.

169. VENČKAUSKAS, Algimantas; KRIVICKIENĖ, Vita; TOLDINAS, Eugenijus (2009). Kompiuterių ir operacinių sistemų saugos modulio programos sudarymas. Informacijos mokslai, t. 50, p. 187–193.

170. VERVAFS (2007). Swedish Administrative Development Agency (VERVA), VERVA's regulation of government agencies' work on secure electronic exchange of information, VERVAFS 2007:2. [interaktyvus]. [žiūrėta 2010 m. kovo 13 d.]. Prieiga per internetą: <http://www.regeringen.se/content/1/c6/11/82/47/da357c5e.pdf>.

171. VODACEK, Leo. Information Management: Concept, Teaching, Applications. [interaktyvus]. [žiūrėta 2011 m. rugsėjo 13 d.]. Prieiga per internetą: <http://www.informationswissenschaft.org/download/isi1998/4_isi98-dv-vodacek-prag.pdf>.

172. von SOLMS, Basie (2000). Information Security – The Third Wave. *Computers and Security*, 2000, Vol. 19(7), p. 615–620.

173. von SOLMS, Basie (2001). Information security – A multidimensional discipline. *Computers and Security*, 2001, Vol. 20(6), p. 504–508.

174. von SOLMS, Basie (2005). Information Security governance: COBIT or ISO 17799 or both? *Computers and Security*, Vol. 24(2), p. 99–104.

175. von SOLMS, Basie (2006). Information Security – The Fourth Wave. *Computers and Security*, Vol. 25(6), p. 165–168.

176. 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.

177. WANG, Richard Y.; STRONG, Diane M. (1996). Beyond accuracy: What data means to data customers. *Journal of Management Information Systems*, Vol. 2, p. 210–232.

178. WEISE, Joel (2009). Why Security Standards? ISSA Journal. 2009 August. [interaktyvus]. [žiūrėta 2012 m. vasario 1 d.]. Prieiga per internetą: <http://www.issa.org/Library/Journals/2009/August/Weise-Why%20Security%20Standards.pdf>.

179. WERLINGER, Rodrigo; HAWKEY, Kirstie; BEZNOSOV, Konstantin (2009). An integrated view of human, organizational and technological challenges of IT security management. *Information management & Computer Security*, Vol. 17(1), p. 4–19. [interaktyvus]. [žiūrėta 2011 m. sausio 16 d.]. Prieiga per internetą: <http://lersse-dl.ece.ubc.ca/record/153/files/153.pdf>.

180. WHITE, Garry (2009). Strategic, tactical, & operational management security model. Journal of Computer Information Systems, Vol. 49(3), p. 71–75.

181. WHITTEN, Alma, TYGAR, J. D (1999). Why Johnny can't encrypt. In Proc. Eighth USENIX Security Symposium, Washington, DC, 23–26 August 1999, p. 169–184.

182. WIIG, Karl M. (2002). Knowledge management in public administration. Journal of Knowledge Management, Vol. 6(3), p. 224–239.

183. WILLARD, Nick (1993). Information Resources Management. *Aslib Information*, Vol. 21(5), p. 201–205.

184. WILLARD, Nick (2003). The Willard Model of IRM. [interaktyvus]. [žiūrėta 2011 m. rugsėjo 1 d.]. Prieiga per internetą: <http://www.skyrme.com/kmroadmap/willard.htm>.

185. WILLIS, Anthony (2005). Corporate governance and management of information and records. *Records Management Journal*, Vol. 15(2), p. 86–97.

186. WILSON, Tom D. (1997). Information management. International Encyclopedia of Information and Library Science, London: Routledge, p. 187–196.

187. WILSON, Tom D. (2002). The nonsense of „knowledge management“. Information Research, Vol. 8(1). [interaktyvus]. [žiūrėta 2011 spalio 15 d.]. Prieiga per internetą: <http://InformationR.net/ir/8-1/paper144.html>.

188. WOLLNIK, Michael (1988). Ein Referenzmodell des Informationsmanagements. Information Management, Vol 3, p. 34–43.

189. WORKMAN, Michael (2008). A test of interventions for security threats from social engineering, Information Management & Computer Security, Vol. 16(5), p. 463–483.

190. YAMANE, Taro (1967). Elementary Sampling Theory. New Jersey: Prentice Hall, 1967, p. 560.

191. ZAFAR, Humayun; CLARK, Jan Guynes (2009). Current State of Information Security Research In IS. Communications of the Association for Information Systems, No. 24, p. 571–596.

192. ZELTSER, Lenny; KENT, Karen; NORTHCUTT, Stephen; RITCHEY, W. Ronald; WINTERS, Scott (2005). Perimeter Security Fundamentals. [interaktyvus]. [žiūrėta 2011 m. birželio 28 d.]. Prieiga per internetą: <http://www.informit.com/articles/article.aspx?p=376256>.

193. XIAOMI, An (2003). An integrated approach to records management. The information Management Journal, Vol. 37(4), p. 24–30.

Kiti šaltiniai

194. The CERT Coordination Center. CERT research annual report. 2008. [interaktyvus]. [žiūrėta 2011 m. sausio 16 d.]. Prieiga per internetą: <http://www.cert.org/cert/information/researchers.html>.

195. Carnegie Mellon University Software Engineering Institute. The CERT Coordination Center. [interaktyvus]. [žiūrėta 2011 m. sausio 16 d.]. Prieiga per internetą: <http://www.cert.org>.

196. Centre for the Protection of National Infrastructure. [interaktyvus]. [žiūrėta 2011 m. sausio 16 d.]. Prieiga per internetą: <http://www.cpni.gov.uk/>.

197. Bundesamt für Sicherheit in der Informationstechnik. [interaktyvus]. [žiūrėta 2011 m. sausio 16 d.]. Prieiga per internetą: <http://www.bsi.de>.

198. European Network and Information Security Agency. [interaktyvus]. [žiūrėta 2011 m. sausio 16 d.]. Prieiga per internetą: <http://www.enisa. europa.eu/>.

199. OECD Principles of Corporate Governance. [interaktyvus]. [žiūrėta 2011 m. sausio 16 d.]. Prieiga per internetą: <http://www.oecd.org/ dataoecd/32/18/ 31557724.pdf>.

200. LR vidaus reikalų ministerijos svetainė. [interaktyvus]. [žiūrėta 2011 m. sausio 16 d.]. Prieiga per internetą: <www.vrm.lt>.

201. LR Valstybės kontrolės svetainė. [interaktyvus]. [žiūrėta 2011 m. sausio 16 d.]. Prieiga per internetą: <www.vkontole.lt>.

202. LR Ryšių reguliavimo tarnybos svetainės. [interaktyvus]. [žiūrėta 2011 m. sausio 16 d.]. Prieiga per internetą: <www.rrt.lt>, <www.esaugumas.lt>.

203. Tarptautinės standartizacijos organizacijos svetainė. [interaktyvus]. [žiūrėta 2011 m. sausio 16 d.]. Prieiga per internetą: <http://www.iso.org>.

204. Tarptautinės elektrotechnikos komisijos svetainė. [interaktyvus]. [žiūrėta 2011 m. sausio 16 d.]. Prieiga per internetą: <http://www.iec.ch/>.

205. Tarptautinės telekomunikacijų sąjungos svetainė. [interaktyvus]. [žiūrėta 2011 m. sausio 16 d.]. Prieiga per internetą: <http://www.itu.int>.

206. Informacinių technologijų valdymo instituto svetainė. [interaktyvus]. [žiūrėta 2011 m. sausio 16 d.]. Prieiga per internetą: <http://www.itgi.org/>.

207. Informacinių sistemų audito ir valdymo asociacijos svetainė. [interaktyvus]. [žiūrėta 2011 m. sausio 16 d.]. Prieiga per internetą: <http://www.isaca.org/>.

1 Priedas. VALSTYBINIAI INFORMACIJOS SAUGUMO AUDITAI

Valstybiniai auditai, kuriuose analizuotos problemos, susijusios su informacijos saugumo valdymu[26]

Nr.	Data	Pavadinimas	Objektas	Tikslai	Subjektai
1.	2006 m.	Lietuvos Respublikos krašto apsaugo ministerijos (KAM) valdomų kompiuterizuotų finansinių ir kitų informacinių sistemų bendrosios kontrolės vertinimas	KAM valdomos kompiuterizuotos finansinės ir kitos IS	Įvertinti KAM valdomų kompiuterizuotų finansinių ir kitų IS bendrąją kontrolę ir pateikti rekomendacijas	KAM
2.	2006 m.	Valstybinių informacinių sistemų bendroji kontrolė	Valstybinių institucijų informacinių sistemų bendroji kontrolė	1. Siekta įvertinti valstybinių institucijų informacinių sistemų valstybinio lygmens bendrąją kontrolę. 2. Siekta apibendrinti informacinių sistemų bendrosios kontrolės būklę valstybinėse institucijose.	Lietuvos Respublikos vidaus reikalų ministerija (VRM), Informacinės visuomenės plėtros komitetas (IVPK) ir kitos valstybinės institucijos, kuriose iki 2006 metų rugpjūčio buvo atlikti informacinių sistemų bendrosios kontrolės vertinimai.
3.	2007 m.	VRM informacinių sistemų bendrosios kontrolės vertinimas	VRM informacinių sistemų bendroji kontrolė	Įvertinti VRM informacinių sistemų bendrąją ir kūrimo kontrolę ir pateikti rekomendacijas.	VRM, Informatikos ir ryšių departamentas prie VRM (IRD)
4.	2007 m.	Akcinės bendrovės Rytų skirstomųjų tinklų informacinės sistemos bendrosios kontrolės vertinimas	Informacinių sistemų bendrosios kontrolės vertinimas	Įvertinti informacinių sistemų bendrąją kontrolę ir pateikti rekomendacijas	AB Rytų skirstomieji tinklai
5.	2007 m.	Valstybinių institucijų informacinių sistemų valdymas elektroninės valdžios kontekste	Valstybės informacinių sistemų bendrosios kontrolės organizavimas	Apibendrinti valstybės informacinių sistemų bendrosios kontrolės būklę atsižvelgiant į el. valdžios kontekstą; įvertinti valstybės informacinių sistemų kūrimo, steigimo, saugos teisinį reglamentavimą;	VRM, IVPK, Valstybinė duomenų apsaugos inspekcija

[26] Valstybės kontrolė. Audito ataskaitos. http://www.vkontrole.lt/meniu.aspx?id=3 (žiūrėta 2012 m. spalio 6 d.)

Nr.	Data	Pavadinimas	Objektas	Tikslai	Subjektai
				įvertinti el. valdžios projektų įgyvendinimo prielaidas ir eigą; įvertinti 2006 metų valstybės informacinių sistemų bendrosios kontrolės vertinimo valstybinio audito rekomendacijų įgyvendinimą; pateikti valstybinių auditorių pastebėjimus, išvadas ir rekomendacijas nustatytiems veiklos trūkumams šalinti.	
6.	2008 m.	Europos Sąjungos struktūrinių fondų lėšomis finansuojamų informacinės visuomenės plėtros projektų valdymas	ES struktūrinių fondų lėšomis finansuojamų IVP projektų valdymas	Surinkti, papildyti ir atnaujinti informaciją apie 2004–2006 m. ES struktūrinių fondų lėšomis finansuojamus IVP projektus ir jų valdymą; įvertinti IVP projektų atrankos ir derinimo procedūrų vykdymą; įvertinti, kaip vykdoma IVP projektų įgyvendinimo stebėsena; įvertinti, kaip vykdomas IVP projektų rezultatų vertinimas; nustatyti problemas, susijusias su ES struktūrinių fondų lėšomis finansuojamų IVP projektų valdymu, ir pateikti rekomendacijas.	IVPK, VšĮ Centrinė projektų valdymo agentūra (CPVA)
7.	2008 m.	Saugaus valstybinio duomenų perdavimo tinklo operatoriaus veikla	Saugaus valstybinio duomenų perdavimo tinklo operatoriaus veikla	Įvertinti Saugaus valstybinio duomenų perdavimo tinklo operatoriaus veiklą	VĮ „Infostruktūra“ VRM
8.	2008 m.	Ekstremalių situacijų valdymo organizavimas	Ekstremalių situacijų valdymas	Įvertinti ekstremalių situacijų valdymo organizavimą	VRM, Priešgaisrinės apsaugos ir gelbėjimo departamentas prie VRM
9.	2009 m.	Strateginės informacijos sauga	Strateginės informacijos sauga	Išnagrinėti su strateginės elektroninės informacijos sauga susijusį teisinį reglamentavimą, sritį koordinuojančių institucijų funkcijas ir jų taikomų priemonių efektyvumą, nustatyti strateginės elektroninės informacijos saugos problemines sritis. Išnagrinėjus numatytas sritis, nustatyti audito tikslus ir subjektus, nuspręsti, ar tikslinga pradėti pagrindinį tyrimą	Valstybės institucijos

Nr.	Data	Pavadinimas	Objektas	Tikslai	Subjektai
10.	2009 m.	Valstybės įmonės registrų centro informacinių sistemų kontrolė	VĮ Registrų centro informacinių sistemų kontrolė	Įvertinti VĮ Registrų centro informacinių sistemų bendrąją kontrolę ir nekilnojamojo turto sandorių viešosios elektroninės paslaugos projektą	VĮ Registrų centras (RC)
11.	2009 m.	Vyriausiosios rinkimų komisijos informacinių sistemų kontrolė	Vyriausiosios rinkimų komisijos informacinės sistemos	Įvertinti Vyriausiosios rinkimų komisijos informacinių sistemų kontrolę	Lietuvos Respublikos vyriausioji rinkimų komisija
12.	2010 m.	Valstybinės mokesčių inspekcijos (VMI) informacinių sistemų kontrolė	VMI informacinių sistemų kontrolė	Įvertinti VMI IS vidaus kontrolę ir su mokesčių apskaita susijusių IS kūrimą, projektavimą ir diegimą	VMI
13.	2010 m.	Valstybės tarnautojų pažymėjimų panaudojimas elektroninėje erdvėje	Valstybės tarnautojų pažymėjimų panaudojimas elektroninėje erdvėje	Vertinti valstybės tarnautojų pažymėjimų panaudojimo elektroninėje erdvėje efektyvumą ir rezultatyvumą. Pateikti rekomendacijas, kurios leistų suaktyvinti el. dokumentų mainus, užtikrintų galimybę valstybės tarnautojams naudoti informacinių sistemų ir registrų duomenis panaudojant pažymėjimus	VRM, IVPK, Lietuvos archyvų departamentas prie LRV, Gyventojų registro tarnyba prie VRM, Valstybės tarnybos departamentas prie VRM, Asmens dokumentų išrašymo centras prie VRM, RC
14.	2011 m.	Elektroninės sveikatos informacinės sistemos plėtra ir audito rekomendacijų įgyvendinimas	Elektroninės sveikatos informacinės sistemos plėtra ir audito rekomendacijų įgyvendinimas	Įvertinti elektroninės sveikatos informacinės sistemos plėtros efektyvumą ir audito rekomendacijų įgyvendinimą	Lietuvos Respublikos sveikatos apsaugos ministerija
15.	2011 m.	Viešojo transporto elektroninio bilieto sistemos Lietuvoje	Viešojo transporto elektroninio bilieto sistemos	Vertinti viešojo transporto elektroninio bilieto sistemų kūrimo rezultatyvumą	Lietuvos Respublikos susisiekimo ministerija, Vilniaus, Kauno ir Klaipėdos miestų savivaldybių administracijos, AB „Lietuvos geležinkeliai“ ir CPVA
16.	2012 m.	Finansų ministerijos informacinių sistemų bendroji ir kūrimo kontrolė	Finansų ministerijos informacinių sistemų bendroji ir kūrimo kontrolė	Įvertinti Finansų ministerijos informacinių sistemų bendrąją ir kūrimo kontrolę	Lietuvos Respublikos finansų ministerija

2 Priedas. INFORMACIJOS SAUGUMO VALDYMO STANDARTŲ 27000 GRUPĖ

ISO 27000 standartų grupė

Ši standartų grupė kilusi iš britiškojo standarto BS-7799 ir pakeitusi informacijos saugumo valdymo tarptautinį standartą ISO 17799. Šios grupės standartai skirti tiesiogiai informacijos saugumo valdymui, saugumo valdymo sistemai kurti, praktinėms diegimo priemonėms, įvertinimui ir organizacijos sertifikavimui. Tai plačiausiai taikomi informacijos saugumo valdymo standartai.

Šiuo metu yra išleisti šie grupės standartai:

ISO/IEC 27000:2009. Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo sistemos. Apžvalga ir žodynas.

ISO/IEC 27001:2005. Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai.

ISO/IEC 27002:2005. Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo praktikos kodeksas.

ISO/IEC 27003:2010. Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo sistemos diegimo gairės.

ISO/IEC 27004:2009. Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo sistemos. Įvertinimas.

ISO/IEC 27005:2008. Informacijos technologija. Saugumo metodai. Informacijos saugumo rizikos valdymas.

ISO/IEC 27006:2011. Informacijos technologija. Saugumo metodai. Reikalavimai, keliami įstaigoms, atliekančioms auditą ir sertifikuojančioms informacijos saugumo valdymo sistemas.

ISO/IEC 27007:2011. Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo sistemų auditavimo gairės.

ISO/IEC TR 27008:2011. Informacijos technologija. Saugumo metodai. Informacijos saugumo kontrolės priemonių gairės auditoriams.

ISO/IEC 27010:2012. Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymas komunikacijose tarp organizacijų ir sektorių.

ISO/IEC 27011:2008. Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo gairės elektroninių ryšių organizacijoms.

ISO/IEC 27031:2011. Informacijos technologija. Saugumo metodai. Informacijos ir ryšių technologijų parengimo veiklos tęstinumui gairės.

ISO/IEC 27032:2011. Informacijos technologija. Saugumo metodai. Kibernetinio saugumo gairės.

ISO/IEC 27033-1:2009, ISO/IEC 27033-2:2012, ISO/IEC 27033-3:2010 – trijų dalių standartas, skirtas ryšių tinklų saugumo technologijų valdymui.

ISO/IEC 27034-1:2011. Informacijos technologija. Saugumo metodai. Aplikacijų saugumas. 1 dalis. Apžvalga ir žodynas.

ISO/IEC 27035:2011. Informacinės technologijos. Saugumo metodai. Informacijos saugumo incidentų valdymas.

Taip pat šiuo metu rengiami dar 33 šios grupės standartai, kurie nustatys gaires informacijos saugumo valdymo auditui, kontrolės priemonėms diegti, rizikai valdyti, informacijos saugumo valdymo sistemoms diegti, debesų kompiuterijos saugumui, incidentams valdyti, įkalčiams elektroninėje erdvėje rinkti, programinės įrangos kūrimui saugoti, ISO 27000 ir ISO 20000 (Cobit) gairių integruotam diegimui, specifines informacijos saugumo valdymo gairės finansinių ir draudimo paslaugų saugumui, ryšių tinklų saugumo valdymui, bevielėms ryšių tinklų technologijoms ir kitos informacijos saugumo valdymo sritims.

3 Priedas. INFORMACIJOS SAUGUMĄ REGLAMENTUOJANTYS LIETUVOS TEISĖS AKTAI

Lietuvoje su informacijos saugumo reglamentavimu susijusi daug teisės aktų. Šiame disertacijos priede pristatomi svarbiausi įstatymai ir poįstatyminiai aktai, reglamentuojantys informacijos saugumą. Šie dokumentai naudoti kaip šaltinis dokumentų turinio analizei nagrinėjant informacijos saugumo valdymą Lietuvos valstybės institucijose.

1996 m. sausio 30 d. priimtas **Lietuvos Respublikos kompiuterių programų ir duomenų bazių teisinės apsaugos įstatymas,** kuris **„***atsižvelgiant į kompiuterių programų ir duomenų bazių, kaip autoriaus teisės dalyko, specifiką, nustato asmeninius neturtinius ir turtinius santykius, kurie atsiranda ryšium su kompiuterių programų ir duomenų bazių sukūrimu, jų apsauga ir naudojimu“*. 1999 m. gegužės 18 d. šį įstatymą pakeitė **Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymas** (nauja reakcija nuo 2003 m. kovo 31 d.). Šiais įstatymais reguliuojama autorių teisių į kūrinius, tarp jų ir duomenų bazes, apsauga.

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 santykius, kurie atsiranda tvarkant asmens duomenis automatiniu būdu, taip pat neautomatiniu būdu tvarkant asmens duomenų susistemintas rinkmenas: sąrašus, kartotekas, bylas, sąvadus ir kita. Įstatymas nustato fizinių asmenų, kaip duomenų subjektų, teises, šių teisių apsaugos tvarką, juridinių ir fizinių asmenų teises, pareigas ir atsakomybę tvarkant asmens duomenis“*.

Įstatymas nustato, kad *„duomenų valdytojas ir duomenų tvarkytojas privalo įgyvendinti tinkamas organizacines ir technines priemones, skirtas apsaugoti asmens duomenims nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo. Minėtos*

priemonės turi užtikrinti tokį saugumo lygį, kuris atitiktų saugotinų asmens duomenų pobūdį ir jų tvarkymo keliamą riziką, ir turi būti išdėstytos rašytinės formos dokumente (duomenų valdytojo patvirtintose asmens duomenų tvarkymo taisyklėse, duomenų valdytojo ir duomenų tvarkytojo sudarytoje sutartyje ir pan.)". Įstatymas taip pat apibrėžia, kad bendruosius reikalavimus organizacinėms ir techninėms duomenų saugumo priemonėms nustato ir šio įstatymo vykdymo priežiūrą bei kontrolę vykdo Valstybinė duomenų apsaugos inspekcija.

1996 m. liepos 2 d. buvo priimtas **Lietuvos Respublikos visuomenės informavimo įstatymas,** kuris 2006 m. išdėstytas nauja redakcija. Šis įstatymas aktualus tuo, kad nustato, kokia informacija yra vieša ir galima viešai skelbti.

1996 m. rugpjūčio 13 d. buvo priimtas **Lietuvos Respublikos valstybės registrų įstatymas** (2004 m. nauja redakcija). Šis įstatymas nustatė *„valstybės registrų (kadastrų) steigimą, tvarkymą, reorganizavimą ir likvidavimą; valstybės registrų sistemą ir bendruosius valstybės registrų sąveikos principus ir vadovaujančiųjų valstybės registrų tvarkymo įstaigų, valstybės registrų tvarkymo įstaigų, valstybės registrų priežiūros institucijų, valstybės registrų tvarkytojų, valstybės registrų duomenų teikėjų ir gavėjų teises ir pareigas"*. Aktualiausia įstatymo dalis – duomenų, tvarkomų registre, saugumo reglamentavimas. Įstatyme nustatoma pareiga užtikrinti duomenų saugą, vadovaujantis Lietuvos Respublikos Vyriausybės patvirtintais bendraisiais duomenų saugos reikalavimais.

1996 m. lapkričio 29 d. Lietuvos Respublikos Vyriausybė savo nutarimu Nr. 1418 susistemino valstybės registrų steigimo tvarką ir patvirtino **Valstybės kadastrų, klasifikatorių, registrų steigimo, projektavimo ir reorganizavimo tvarką bei Lietuvos Respublikos valstybės registro tipinius nuostatus** (2005 m. ir 2012 m. naujos redakcijos) bei nustatė registro duomenų apsaugos užtikrinimo pareigą ir tvarką.

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**, kurių tikslas – *„sudaryti sąlygas saugiai automatiniu būdu tvarkyti elektroninę informaciją valstybės informacinėse sistemose ir valstybės ar žinybiniuose registruose arba kitose informacinėse sistemose“*.

Šie reikalavimai nustatė, kad *„užtikrinant informacijos saugą, rekomenduojama vadovautis Lietuvos standartais LST ISO/IEC 17799:2006, LST ISO/IEC 27001:2006, taip pat kitais Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo metodai“ grupės standartais, apibūdinančiais saugų informacinės sistemos duomenų tvarkymą“* bei apibrėžė, kad informacinių sistemų valdytojai privalo turėti saugos politikos dokumentą, kuris apibrėžtas kaip *„pagrindiniai taikytini informacijos saugos užtikrinimo ir valdymo principai, pagrindinės taisyklės, į kuriuos atsižvelgiant turi būti derinami informacinės sistemos (ar informacinių sistemų) veiklos ir naudojimo procesai, procedūros ir rengiami juos reglamentuojantys dokumentai“*. Informacijos saugos politika išdėstoma informacinės sistemos valdytojo tvirtinamuose Informacinės sistemos duomenų saugos nuostatuose, taip pat privalo būti patvirtinti šią politiką įgyvendinantys dokumentai.

1999 m. lapkričio 25 d. buvo priimtas **Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymas**, o 2004 m. įsigaliojo nauja įstatymo redakcija. Įstatymas reguliuoja automatizuotų duomenų apdorojimo (ADA) sistemų ir tinklų, kuriuose yra saugoma, apdorojama ar kuriais perduodama įslaptinta informacija, apsaugą, leidimų apdoroti įslaptintą informaciją ADA sistemomis ir tinklais išdavimą.

2000 m. liepos 11 d. buvo priimtas **Lietuvos Respublikos elektroninio parašo įstatymas**. Šis įstatymas reglamentuoja elektroninio parašo kūrimą, tikrinimą, galiojimą, parašo naudotojų teises ir atsakomybę, nustato sertifikavimo paslaugas ir reikalavimus jų teikėjams bei elektroninio parašo priežiūros institucijos teises ir funkcijas.

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 valstybine strategija:

1. 2002 m. gruodžio 31 d. nutarimu Nr. 2105 Lietuvos Respublikos Vyriausybė patvirtino naują Bendrųjų duomenų saugos reikalavimų redakciją. Naujoje redakcijoje buvo nurodytas šių reikalavimų tikslas – saugiai tvarkyti automatizuotu būdu duomenis valstybės registruose ir kitose valstybės informacinėse sistemose sąlygų sudarymas.

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“. 2004 m. šis tinklas sujungtas su ES institucijomis ir valstybių narių administracijų duomenų perdavimo tinklu TESTA (angl. Trans-European Telematics Networks for Administrations). SVDPT paskirtis apima: LR ir ES institucijų saugaus duomenų keitimosi sąlygų sudarymą; LR institucijų tarpusavio saugaus duomenų keitimosi sąlygų sudarymą; LR institucijų IT priemonių kaštų mažinimo sąlygų sudarymą; LR fizinių ir juridinių asmenų saugaus darbo elektroninės valdžios aplinkoje sąlygų sudarymą, užtikrinant saugų bendravimą su ES institucijomis ir ES valstybių narių administracijomis.

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

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. Šis tarptautinis standartas buvo parengtas pagal Didžiosios Britanijos standartą BS 7799.

2004 m. balandžio 19 d. nutarimu Nr. 451 Lietuvos Respublikos Vyriausybė patvirtino **Valstybės informacinių sistemų 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 anksčiau nurodytus Tipinius duomenų saugos nuostatus.

2006 metų birželio 19 dieną Lietuvos Respublikos Vyriausybė, įgyvendindama savo 2004–2008 metų programą, 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 naujai patvirtino atnaujintus **Bendruosius duomenų saugos reikalavimus.**

3. 2007 m. gegužės 8 d. įsakymu Nr. 1V-172 Lietuvos Respublikos vidaus reikalų ministras patvirtino **Saugos dokumentų turinio gaires**, pakeitusias 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.**

2011 metų birželio 29 d. Lietuvos Respublikos Vyriausybė patvirtino naują strateginį dokumentą – **Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programą**. Šio dokumento tikslas – apimti visus, ne tik viešąjį, sektorius, tačiau dar nepatvirtinti jokie dokumentui įgyvendinti reikalingi teisės aktai, todėl šiuo metu nėra galimybių atlikti detalesnės dokumento analizės ir vertinimo.

2012 metų sausio 1 d. įsigaliojo **Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas**. Šio įstatymo tikslas – užtikrinti tinkamą valstybės informacinių išteklių kūrimą, tvarkymą, valdymą,

naudojimą, priežiūrą, sąveiką, planavimą, finansavimą ir saugą. Šiuo įstatymu taip pat pripažintas netekusiu galios Valstybės registrų įstatymas.

2012 metų birželio 26 d. Lietuvos Respublikos Seimo patvirtino **Nacionalinio saugumo strategija.** Šioje strategijoje informacijos ir kibernetinis saugumas minimi tarp pirmaeilių Lietuvos nacionalinio saugumo interesų, joje išdėstyti tikslai – „*visapusiškai stiprinti nacionalinės kibernetinės erdvės saugumą, užtikrinti elektroninės informacijos konfidencialumą, vientisumą ir prieinamumą*“ – bei šių tikslų įgyvendinimo uždaviniai. Strategijos įgyvendinimas deleguotas Lietuvos Respublikos Vyriausybei.

4 Priedas. INFORMACIJOS SAUGUMO REIKALAVIMAI

Šiame priede pateikta Lietuvos valstybės institucijoms galiojančių informacijos saugumo reikalavimų, nustatytų Lietuvos Respublikos teisės aktuose, turinio analizė. Analizės vykdymo laikotarpis – 2010–2011 metai.

Analizė pateikta vertinant informacijos saugumą reglamentuojančias nuostatas, įtvirtintas įstatymais (4 priedo 1 lentelė), Lietuvos Respublikos Vyriausybės nutarimais (4 priedo 2 lentelė) ir Lietuvos Respublikos vidaus reikalų ministro įsakymais (4 priedo 3 lentelė).

Analizuojamu laikotarpiu Lietuvos valstybės institucijos valdė 4 rūšių informacinius išteklius – valstybės registrus, žinybinius registrus, valstybės informacines sistemas ir vidaus administravimo informacines sistemas.

Tikslinga aptarti kiekvienos išteklių rūšies veiklos (a) ir informacijos saugumo užtikrinimo (b) reikalavimus:

1. *Valstybės registrai (kadastrai):* a) veikla, reglamentuota Valstybės registrų įstatymu, jų steigimas, reorganizavimas ir likvidavimas nustatytas Vyriausybės patvirtintomis taisyklėmis; b) valstybės registruose tvarkomos informacijos saugumas užtikrinamas Vyriausybės patvirtintuose Bendruosiuose informacijos saugumo reikalavimuose nustatyta tvarka.

2. *Žinybiniai registrai:* a) veiklą, kai žinybinį registrą valdo institucijos, pavaldžios Vyriausybei, pavesta organizuoti vadovaujantis Vyriausybės patvirtintomis valstybės registrų veiklą reglamentuojančiomis taisyklėmis, kiek tai atitinka žinybinių registrų specifiką, kitoms įstaigoms rekomenduojama vadovautis šiomis taisyklėmis; b) žinybiniuose registruose tvarkomos informacijos saugumas turi būti užtikrinamas vadovaujantis Vyriausybės patvirtintais Bendraisiais informacijos saugumo reikalavimais.

3. *Valstybės informacinės sistemos:* a) veikla, reglamentuota Vyriausybės patvirtintomis informacinių sistemų steigimo ir įteisinimo taisyklėmis, įstaigoms, nepavaldžioms Vyriausybei, šias taisykles taikyti

rekomenduojama; b) valstybės informacinėse sistemose tvarkomos informacijos saugumas turi būti užtikrinamas vadovaujantis Vyriausybės patvirtintais Bendraisiais informacijos saugumo reikalavimais.

4. *Vidaus administravimo informacinės sistemos:* a) veiklos tiesiogiai nereglamentuoja jokie teisės aktai; b) tvarkomos informacijos saugumui užtikrinti taikytini Vyriausybės patvirtinti Bendrieji informacijos saugumo reikalavimai.

4 priedo 1 lentelė. Lietuvos Respublikos įstatymai, reglamentuojantys informacijos saugumo kontekstą

Pavadinimas	**Valstybės registrų įstatymas**	**Asmens duomenų teisinės apsaugos įstatymas**	**Elektroninių ryšių įstatymas**
Patvirtino	Lietuvos Respublikos Seimas	Lietuvos Respublikos Seimas	Lietuvos Respublikos Seimas
Priėmimo data	1996 m. rugpjūčio 13 d.	1996 m. birželio 11 d.	2004 m. balandžio 15 d.
Paskutinis atnaujinimas	2009 m. lapkričio 12 d.	2011 m. gegužės 12 d.	2011 m. birželio 28 d.
Taikymas	Įstatymas nustato: 1) valstybės registrų (kadastrų) steigimą, tvarkymą, reorganizavimą ir likvidavimą; 2) valstybės registrų sistemą ir bendruosius valstybės registrų sąveikos principus; 3) vadovaujančiųjų valstybės registrų tvarkymo įstaigų, valstybės registrų tvarkymo įstaigų, valstybės registrų priežiūros institucijų, valstybės registrų tvarkytojų, valstybės registrų duomenų teikėjų ir gavėjų teises ir pareigas.	Įstatymas reglamentuoja santykius, kurie atsiranda tvarkant asmens duomenis automatiniu būdu, taip pat neautomatiniu būdu tvarkant asmens duomenų susistemintas rinkmenas: sąrašus, kartotekas, bylas, sąvadus ir kita. Įstatymas nustato fizinių asmenų, kaip duomenų subjektų, teises, šių teisių apsaugos tvarką, juridinių ir fizinių asmenų teises, pareigas ir atsakomybę tvarkant asmens duomenis.	Įstatymas reglamentuoja 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.
Apribojimai	*Nėra*	Įstatymas netaikomas jeigu asmens duomenis tvarko fizinis asmuo ir tik asmeniniams poreikiams, nesusijusiems su verslu ar profesija, tenkinti. Įstatymas netaikomas mirusių asmenų asmens duomenų tvarkymui. Tvarkant asmens duomenis valstybės saugumo, gynybos tikslais, šis įstatymas taikomas tiek, kiek kiti įstatymai nenustato kitaip.	Įstatymas nereglamentuoja visuomeninių santykių, susijusių su paslaugomis, teikiamomis naudojant elektroninių ryšių tinklus ir paslaugas, taip pat elektroninių ryšių tinklais perduodamo turinio ir su juo susijusių paslaugų.
Tikslas	*Žr. Taikymas*	Ginti žmogaus privataus gyvenimo neliečiamumo teisę tvarkant asmens duomenis.	Nustato reikalavimus viešųjų ryšių tinklų ir viešųjų elektroninių ryšių paslaugų saugumui ir vientisumui bei asmens duomenų saugumui.
Aktualios sąvokos	Valstybės registras (kadastras) – teisinių, organizacinių, technologinių priemonių visuma, skirta registruoti įstatymų nustatytus registro objektus, rinkti, kaupti, apdoroti, sisteminti, saugoti bei teikti fiziniams ir juridiniams asmenims registruojamų objektų kiekybinius, kokybinius, geografinius ir kitus duomenis bei dokumentus. Žinybinis registras – teisinių, organizacinių, technologinių priemonių visuma, skirta registruoti valstybės ar savivaldybės institucijos ar įstaigos sprendimu nustatytus registro objektus ir tvarkyti registro objektų registravimo duomenis.	Asmens duomenys – bet kuri informacija, susijusi su fiziniu asmeniu – duomenų subjektu, kurio tapatybė yra žinoma arba gali būti tiesiogiai ar netiesiogiai nustatyta pasinaudojant tokiais duomenimis kaip asmens kodas, vienas arba keli asmeniui būdingi fizinio, fiziologinio, psichologinio, ekonominio, kultūrinio ar socialinio pobūdžio požymiai.	Elektroninių ryšių paslauga – paprastai už atlygį teikiama paslauga, kurią visiškai ar daugiausia sudaro signalų perdavimas elektroninių ryšių tinklais, įskaitant telekomunikacijų paslaugas ir perdavimo (siuntimo) paslaugas transliavimui (retransliavimui) naudojamais tinklais. Elektroninių ryšių paslaugos neapima elektroninių ryšių tinklais ar naudojant elektroninių ryšių paslaugas perduodamos informacijos turinio teikimo ar redakcinės turinio kontrolės paslaugų, tarp jų informacinės visuomenės paslaugų, kurių visiškai ar daugiausia nesudaro signalų perdavimas elektroninių ryšių tinklais. Saugumo incidentas – įvykis, veiksmas ar neveikimas, kuris sukelia ar gali sukelti neteisėtą prisijungimą ar

Pavadinimas	Valstybės registrų įstatymas	Asmens duomenų teisinės apsaugos įstatymas	Elektroninių ryšių įstatymas
			sudaryti sąlygas neteisėtai prisijungti prie informacinės sistemos ar elektroninių ryšių tinklo, sutrikdyti ar pakeisti, įskaitant valdymo perėmimą, informacinės sistemos ar elektroninių ryšių tinklo veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninius duomenis, panaikinti ar apriboti galimybę naudotis elektroniniais duomenimis, taip pat sudaryti sąlygas pasisavinti ar kitaip panaudoti neviešus elektroninius duomenis tokios teisės neturintiems asmenims.
Įgyvendinantys dokumentai	Registrai steigiami, reorganizuojami ir likviduojami šio įstatymo ir Vyriausybės nustatyta tvarka. Registro duomenų saugos nuostatai rengiami vadovaujantis Vyriausybės patvirtintais bendraisiais duomenų saugos reikalavimais.	Valstybinė duomenų apsaugos inspekcija nustato bendruosius reikalavimus organizacinėms ir techninėms duomenų saugumo priemonėms.	Valstybinės duomenų apsaugos inspekcijos parengtos metodinės rekomendacijos asmens duomenų saugumui užtikrinti. Ryšių reguliavimo tarnyba gali nustatyti techninius ir organizacinius reikalavimus viešųjų ryšių tinklų ir viešųjų elektroninių ryšių paslaugų saugumui ir vientisumui užtikrinti.
Kita aktuali informacija	Kad būtų užtikrinta registro duomenų sauga, vadovaujantis Vyriausybės patvirtintais bendraisiais duomenų saugos reikalavimais, rengiami ir vadovaujančiosios registro tvarkymo įstaigos tvirtinami registro duomenų saugos nuostatai. Juose nustatomos reikiamos registro duomenų saugos priemonės, registro duomenų saugaus tvarkymo reikalavimai ir jų įgyvendinimas.	Duomenų valdytojas ir duomenų tvarkytojas privalo įgyvendinti tinkamas organizacines ir technines priemones, skirtas apsaugoti asmens duomenims nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo. Minėtos priemonės turi užtikrinti tokį saugumo lygį, kuris atitiktų saugotinų asmens duomenų pobūdį ir jų tvarkymo keliamą riziką, ir turi būti išdėstytos rašytinės formos dokumente (duomenų valdytojo patvirtintose asmens duomenų tvarkymo taisyklėse, duomenų valdytojo ir duomenų tvarkytojo sudarytoje sutartyje ir pan.).	

4 priedo 2 lentelė. Lietuvos Respublikos Vyriausybės patvirtinti norminiai dokumentai, reglamentuojantys informacijos saugumo kontekstą

Pavadinimas	**Valstybės informacinių sistemų steigimo ir įteisinimo taisyklės**	**Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai**	**Valstybės registrų ir kadastrų steigimo, reorganizavimo ir likvidavimo taisyklės**
Patvirtino	LRV	LRV	LRV
Priėmimo data	2004 m. balandžio 19 d.	1997 m. rugsėjo 4 d., 2002 m. gruodžio 31 d., 2007 m. balandžio 25 d.	1996 m. lapkričio 29 d.
Paskutinis atnaujinimas	2011 m. gegužės 4 d.	2011 m. gegužės 4 d.	2010 m. lapkričio 10 d.
Taikymas ir apribojimai	Ministerijų, Vyriausybės įstaigų, įstaigų prie ministerijų ir kitų Lietuvos Respublikos Vyriausybei atskaitingų valstybės institucijų ir įstaigų valstybės informacinėms sistemoms. Netaikomos informacinėms sistemoms, kuriose tvarkomi duomenys yra valstybės ar tarnybos paslaptis.	Valstybės informacinės sistemos ir valstybės ar žinybiniai registrai arba kitos informacinės sistemos. Netaikomi įslaptintos informacijos tvarkymui automatiniu būdu, išskyrus riboto naudojimo informaciją.	Valstybės registrams ir kadastrams. Valstybės institucijoms ir įstaigoms, pavaldžioms Lietuvos Respublikos Vyriausybei, pavesta vadovautis šiomis taisyklėmis steigiant ir kuriant žinybinius registrus, kiek tai atitinka žinybinių registrų specifiką. Kitoms įstaigoms rekomenduojama vadovautis šiomis taisyklėmis.
Tikslas	Nustato valstybės informacinių sistemų (išskyrus valstybės ir žinybinius registrus) steigimo, kūrimo ir įteisinimo, modernizavimo ir likvidavimo procedūras.	Informacija turi būti patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, kokio nors kitokio neteisėto jos tvarkymo.	Reglamentuoja valstybės registrų ir kadastrų steigimą, reorganizavimą ir likvidavimą.
Sąvoka	Valstybės informacinė sistema – valstybės institucijai teisės aktų nustatytoms funkcijoms, išskyrus vidaus administravimą, atlikti reikiamos informacijos apdorojimo procesus (duomenų ir dokumentų tvarkymo, skaičiavimo, bendravimo nuotoliniu būdu ir t. t.) vykdanti sistema, kuri veikia informacinių technologijų pagrindu.	Informacijos saugos politika išdėstoma informacinės sistemos valdytojo tvirtinamuose Informacinės sistemos duomenų saugos nuostatuose.	Nustatytos Valstybės registrų įstatyme.
Įgyvendinantys dokumentai	Informacinės sistemos nuostatai, Informacinės sistemos duomenų saugos nuostatai.	Informacinės sistemos valdytojas privalo turėti pagal Vidaus reikalų ministerijos tvirtinamas Saugos dokumentų turinio gaires parengtus, su Vidaus reikalų ministerija suderintus ir patvirtintus šiuos saugos dokumentus: 1. Informacinės sistemos duomenų saugos nuostatus; 2. Saugaus elektroninės informacijos tvarkymo taisykles; 3. Informacinės sistemos veiklos tęstinumo valdymo planą; 4. Informacinės sistemos naudotojų administravimo taisykles.	Registro nuostatai ir kiti steigimo dokumentai, Registro duomenų saugos nuostatai.
Kita informacija	Informacinės sistemos duomenų saugos nuostatai ir kiti saugos dokumentai rengiami, derinami ir tvirtinami Bendrųjų elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimų nustatyta tvarka.	Rekomenduojama vadovautis Lietuvos standartais LST ISO/IEC 17799:2006, LST ISO/IEC 27001:2006, taip pat kitais Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo metodai“ grupės standartais, apibūdinančiais saugų informacinės sistemos duomenų tvarkymą.	Registro duomenų saugą reglamentuoja duomenų saugos nuostatai ir kiti saugos dokumentai, kurie rengiami, derinami ir tvirtinami Bendrųjų elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimų nustatyta tvarka.

4 priedo 3 lentelė. Lietuvos Respublikos vidaus reikalų ministro norminiais dokumentais patvirtintos informacinių sistemų kategorijos ir joms taikomi informacijos saugumo reikalavimai[27]

Pavadinimas	**Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairės**	**Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniai saugos reikalavimai**
Informacinės sistemos kategorija	Informacinės sistemos charakteristika	Reikalavimai
Pirma kategorija	1. Informacinė sistema, kurioje logiškai tarpusavyje susijusių duomenų konfidencialumo, vientisumo ir (ar) prieinamumo praradimas gali sukelti ypač sunkius padarinius valstybei; 2. Informacinė sistema, kurios pagrindu funkcionuoja pagrindinis valstybės registras; 3. Valstybinio socialinio draudimo fondo funkcijų vykdymą užtikrinanti informacinė sistema; 4. Mokesčių administratoriaus funkcijų vykdymą užtikrinanti informacinė sistema; 5. Informacinė sistema skirta valstybės piniginiams ištekliams planuoti, kaupti, išduoti, jų apskaitai tvarkyti, naudojimo kontrolei atlikti, rengti atskaitomybę ir stebėti valstybės piniginių išteklių srautus.	1. Taikomi visi žemesnių kategorijų informacinių sistemų reikalavimai. 2. Institucija turi įgyvendinti Lietuvos standarte LST ISO/IEC 17799:2006 nurodytas technines saugos priemones, išskyrus priemones, kurios netaikytinos dėl institucijos veiklos, informacinės sistemos ar naudojamos informacinėje sistemoje techninės įrangos pobūdžio. 3. Atliekant atitikties vertinimą, turi būti atliekamas atitikties reikalavimų vertinimas, kurį turi atlikti nepriklausomi specialistai.
Antra kategorija	1. Informacinė sistema, kurioje logiškai tarpusavyje susijusių duomenų konfidencialumo, vientisumo ir (ar) prieinamumo praradimas gali turėti sunkių padarinių valstybės institucijos ar įstaigos darbui bei turėti neigiamą įtaką kitų valstybės institucijų ar įstaigų veiklai. 2. Informacinė sistema, kurioje tvarkomi duomenys yra teikiami pirmos kategorijos informacinei sistemai. 3. Informacinė sistema, kurioje tvarkomi ypatingi asmens duomenys, išskyrus duomenis, susijusius su asmens sveikata. 4. Informacinė sistema, kuri užtikrina pirmos kategorijos informacinių sistemų sąveiką. 5. Informacinė sistema, kurioje tvarkomi iš pirmos kategorijos informacinės sistemos gauti duomenys. 6. Informacinė sistema, kurios pagrindu funkcionuoja valstybės registras. 7. Informacinė sistema sudaryta iš ne mažiau kaip 5 posistemių,	1. Taikomi visi žemesnių kategorijų informacinių sistemų reikalavimai. 2. Atitikties vertinimas turi būti atliekamas ne rečiau kaip kartą per metus, jei teisės aktuose nenustatyta kitaip. 3. Turi būti reglamentuota nešiojamųjų kompiuterių, skirtų informacinės sistemos elektroninės informacijos tvarkymui, naudojimo ne institucijos patalpose tvarka. 4. Svarbiausia kompiuterinė įranga ir duomenų perdavimo tinklo mazgai turi turėti rezervinį maitinimo šaltinį, užtikrinantį šios įrangos veikimą ne mažiau kaip 30 min. 5. Svarbiausia kompiuterinė įranga, duomenų perdavimo tinklo mazgai ir ryšio linijos turi būti dubliuoti ir jų techninė būklė nuolat stebima. 6. Kompiuterinės įrangos gedimai turi būti registruojami žurnale. 7. Kompiuterinėse darbo vietose turi būti naudojamos centralizuotai valdomos kenksmingosios programinės įrangos aptikimo priemonės, kurios turi būti reguliariai atnaujinamos. 8. Programinės įrangos diegimą turi atlikti tik įgalioti asmenys. 9. Programinės įrangos testavimas turi būti atliekamas naudojant atskirą tam skirtą testavimo aplinką. 10. Informacinė sistema turi registruoti visus elektroninės informacijos pakeitimus, juos atlikusį

[27] Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairės // http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=301844&p_query=&p_tr2=, (žiūrėta 2012 m. liepos 4 d.)
Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniai saugos reikalavimai // http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=330054, (žiūrėta 2012 m. liepos 4 d.)

Pavadinimas	Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairės	Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniai saugos reikalavimai
	vykdančių elektroninės informacijos, reikalingos valstybės institucijai teisės aktų nustatytoms funkcijoms, išskyrus vidaus administravimą, atlikti, apdorojimo procesus.	naudotoją ir pakeitimų atlikimo laiką. 11. Tarnybinių stočių įvykių žurnaluose (angl. event log) turi būti registruojami ir nustatytą laiką saugomi duomenys apie: įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis informacinėje sistemoje, bandymus prieiti prie informacinių išteklių, kitus svarbius saugai įvykius, nurodant informacinės sistemos naudotojo identifikatorių ir įvykio laiką, ši informacija turi būti reguliariai analizuojama. 12. Patekimas į tarnybinių stočių patalpas turi būti registruojamas. 13. Tarnybinių stočių patalpų durys turi būti šarvuotos ir apsaugotos bent dviem skirtingos konstrukcijos spynomis. 14. Tarnybinių stočių patalpose turi būti oro kondicionavimo ir drėgmės kontrolės įranga. 15. Visose patalpose turi būti įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir apsaugos tarnybų. 16. Patekimas prie darbo vietų turi būti kontroliuojamas. 17. Atsarginės patalpos turėtų tenkinti pagrindinėms patalpoms keliamus reikalavimus arba institucijos informacinės sistemos veiklos tęstinumo valdymo planas turi nustatyti, kaip per minimalų laikotarpį pasiekti šių reikalavimų atitiktį. 18. Kopijos turi būti saugomos užrakintoje nedegioje spintoje, kitose patalpose, nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota, arba kitame pastate. 19. Patekimas į patalpas, kuriose laikomos kopijos, turi būti registruojamas žurnale. 20. Slaptažodis turi būti keičiamas ne rečiau kaip kas 3 mėnesius. 21. Slaptažodį turi sudaryti ne mažiau kaip 8 simboliai. 22. Keičiant slaptažodį informacinė sistema neturi leisti nustatyti slaptažodžio iš buvusių 6 paskutinių slaptažodžių. 23. Administratorius savo tapatybę turi patvirtinti slaptažodžiu, kuriam keliami aukštesni reikalavimai negu naudotojų slaptažodžiams, arba kitomis autentiškumo patvirtinimo priemonėmis (pvz., biometrinėmis, lustinėmis kortelėmis ir pan.).
Trečia kategorija	1. Informacinė sistema, kurioje logiškai tarpusavyje susijusių duomenų konfidencialumo, vientisumo ir (ar) prieinamumo praradimas gali turėti neigiamą įtaką valstybės institucijos ar įstaigos veiklai. 2. Informacinė sistema, kurioje tvarkomi asmens duomenys. 3. Informacinė sistema, kurioje tvarkomi iš pirmos kategorijos informacinės sistemos gauti apibendrinti arba nuasmeninti duomenys. 4. Informacinė sistema, kurios pagrindu funkcionuoja žinybinis registras. 5. Informacinė sistema sudaryta iš ne mažiau kaip 3 posistemių, vykdančių elektroninės informacijos, reikalingos valstybės institucijai teisės aktų nustatytoms funkcijoms, išskyrus vidaus administravimą, atlikti, apdorojimo procesus.	1. Atitikties vertinimas turi būti atliekamas ne rečiau kaip kartą per dvejus metus, jei teisės aktuose nenustatyta kitaip. 2. Informacinė sistema turi perspėti administratorių, kai pagrindinėje informacinės sistemos kompiuterinėje įrangoje sumažėja iki nustatytos pavojingos ribos laisvos kompiuterio atminties ar vietos diske, ilgą laiką stipriai apkraunamas centrinis procesorius ar kompiuterių tinklo sąsaja. 3. Viešaisiais telekomunikaciniais tinklais perduodamos informacinės sistemos elektroninės informacijos konfidencialumas turi būti užtikrintas naudojant šifravimą, virtualų privatų tinklą (angl. virtual private network), skirtines linijas, saugų valstybinį duomenų perdavimo tinklą ar kitas priemones. 4. Informacinė sistema turi turėti įvestos elektroninės informacijos tikslumo, užbaigtumo ir patikimumo tikrinimo priemones. 5. Informacinėje sistemoje turi būti registruojami ir nustatytą laiką saugomi duomenys apie informacinės sistemos įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis informacinėje sistemoje, kitus saugai svarbius įvykius, nurodant informacinės sistemos

Pavadinimas	Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairės	Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniai saugos reikalavimai
		naudotojo identifikatorių ir įvykio laiką; ši informacija turi būti reguliariai analizuojama. 6. Patekimas į informacinės sistemos tarnybinių stočių patalpas turi būti kontroliuojamas; 7. Rezervinis maitinimo šaltinis turi užtikrinti informacinės sistemos pagrindinės kompiuterinės įrangos veikimą ne mažiau nei 10 min. 8. Jei informacinės sistemos tarnybinių stočių patalpose esančios įrangos bendras galingumas yra daugiau nei 10 kilovatų, turi būti įrengta oro kondicionavimo įranga. 9. Institucija turi numatyti atsargines patalpas, į kurias galėtų laikinai perkelti informacinės sistemos įrangą, nesant galimybių tęsti veiklą pagrindinėse patalpose; institucijos informacinės sistemos veiklos tęstinumo valdymo planas turi užtikrinti informacinės sistemos veiklos atnaujinimą atsarginėse patalpose per tokį laikotarpį, kad nebūtų nusižengta institucijos įsipareigojimams, susijusiems su informacinės sistemos veikla. 10. Kopijų darymas turi būti fiksuojamas žurnale. 11. Kopijos turi būti saugomos užrakintoje nedegioje spintoje. 12. Elektroninė informacija kopijose turi būti užšifruota arba turi būti imtasi kitų priemonių, neleidžiančių panaudoti kopijų neteisėtam elektroninės informacijos atkūrimui. 13. Periodiškai turi būti atliekami elektroninės informacijos atkūrimo iš kopijų bandymai. 14. Atsarginės laikmenos su programine įranga turi būti laikomos nedegioje spintoje. 15. Slaptažodis turi būti keičiamas ne rečiau kaip kas 6 mėnesius. 16. Slaptažodį turi sudaryti ne mažiau kaip 6 simboliai. 17. Slaptažodis turi būti sudarytas iš raidžių, skaičių ir specialiųjų simbolių. 18. Keičiant slaptažodį informacinė sistema neturi leisti nustatyti slaptažodžio iš buvusių 3 paskutinių slaptažodžių. 19. Slaptažodžiams neturi būti naudojama asmeninio pobūdžio informacija. 20. Pirmojo prisijungimo prie informacinės sistemos metu iš informacinės sistemos naudotojo turi būti reikalaujama, kad jis pakeistų slaptažodį; 21. Turi būti draudžiama slaptažodžius atskleisti tretiesiems asmenims.
Ketvirta kategorija	Visos kitos informacinės sistemos.	Bendrieji informacinių sistemų elektroninės informacijos techniniai saugos reikalavimai: 1. Turi būti periodiškai atliekamas informacinės sistemos informacinių technologijų saugos atitikties vertinimas. 2. Informacinė sistema turi registruoti bent vieną paskutinį informacinės sistemos elektroninės informacijos pakeitimą atlikusį informacinės sistemos naudotoją ir pakeitimo laiką. 3. Informacinės sistemos priežiūros funkcijos turi būti atliekamos naudojant atskirą tam skirtą administratoriaus identifikatorių, kuriuo naudojantis nebūtų galima atlikti informacinės sistemos naudotojo funkcijų. 4. Kiekvienas informacinės sistemos naudotojas turi būti informacinėje sistemoje unikaliai identifikuojamas – informacinės sistemos naudotojas turi patvirtinti savo tapatybę slaptažodžiu arba kita autentiškumo patvirtinimo priemone. 5. Informacinės sistemos naudotojui teisė dirbti su konkrečia elektronine informacija turi būti ribojama ar sustabdoma, kai informacinės sistemos naudotojas atostogauja, vykdomas informacinės sistemos naudotojo veiklos tyrimas ir pan.; pasibaigus tarnybos (darbo) santykiams, informacinės sistemos naudotojo teisė naudotis informacine sistema turi būti

Pavadinimas	Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairės	Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniai saugos reikalavimai
		panaikinta. 6. Baigus darbą turi būti imamasi priemonių, kad su elektronine informacija negalėtų susipažinti pašaliniai asmenys: atsijungiama nuo informacinės sistemos, įjungiama ekrano užsklanda su slaptažodžiu, dokumentai padedami į pašaliniams asmenims neprieinamą vietą ir pan. 7. Informacinės sistemos naudotojui neatliekant jokių veiksmų, informacinė sistema turi užsirakinti, kad toliau naudotis informacine sistema galima būtų tik pakartojus tapatybės nustatymo ir autentiškumo patvirtinimo veiksmus. 8. Institucija turi išsiaiškinti, kiek ji ilgiausiai gali tęsti savo funkcijų įgyvendinimą neveikiant informacinei sistemai ar jos daliai; institucijos informacinės sistemos veiklos tęstinumo valdymo planas turi užtikrinti informacinės sistemos veiklos atkūrimą per šį laikotarpį; turi būti parengtas veiksmų planas, užtikrinantis informacinės sistemos veiklos atnaujinimą ketvirtosios kategorijos informacinėms sistemoms per 16 val., trečiosios kategorijos informacinėms sistemoms – per 8 val., antrosios kategorijos informacinėms sistemoms – per 1 val., pirmosios kategorijos informacinėms sistemoms – per 15 min. Reikalavimai informacinės sistemos įrangai ir patalpoms: 1. Pagrindinė informacinės sistemos kompiuterinė įranga turi turėti įtampos filtrą arba (ir) rezervinį maitinimo šaltinį; 2. Turi būti naudojamos kenksmingosios informacinės sistemos programinės įrangos aptikimo priemonės, kurios turi būti reguliariai atnaujinamos. 3. Turi būti operatyviai įdiegiami informacinės sistemos operacinės sistemos ir naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai. 4. Informacinėje sistemoje turi būti naudojama tik legali programinė įranga. 5. Įranga turi būti prižiūrima laikantis gamintojo rekomendacijų. 6. Įrangos priežiūrą ir gedimų šalinimą turi atlikti kvalifikuoti specialistai. 7. Turi būti apribota fizinė prieiga prie informacinės sistemos tarnybinių stočių (atskiros rakinamos patalpos arba rakinama spinta). 8. Patalpose, kuriose yra informacinės sistemos tarnybinės stotys, turi būti įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir apsaugos tarnybų. 9. Turi būti užtikrintas informacinės sistemos prieinamumas ketvirtosios kategorijos informacinėms sistemoms ne mažiau kaip 70 proc. laiko darbo metu darbo dienomis, trečiosios kategorijos informacinėms sistemoms – ne mažiau kaip 90 proc. laiko darbo metu darbo dienomis, antrosios kategorijos informacinėms sistemoms – ne mažiau kaip 96 proc. laiko visą parą, pirmosios kategorijos informacinėms sistemoms – ne mažiau kaip 99 proc. laiko visą parą. 10. Turi būti daromos atsarginės elektroninės informacijos kopijos (toliau – kopijos), kurios turi būti laikomos atskiroje patalpoje. 11. Informacinės sistemos elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų telekomunikacinių tinklų naudojant užkardą ar kitas priemones.

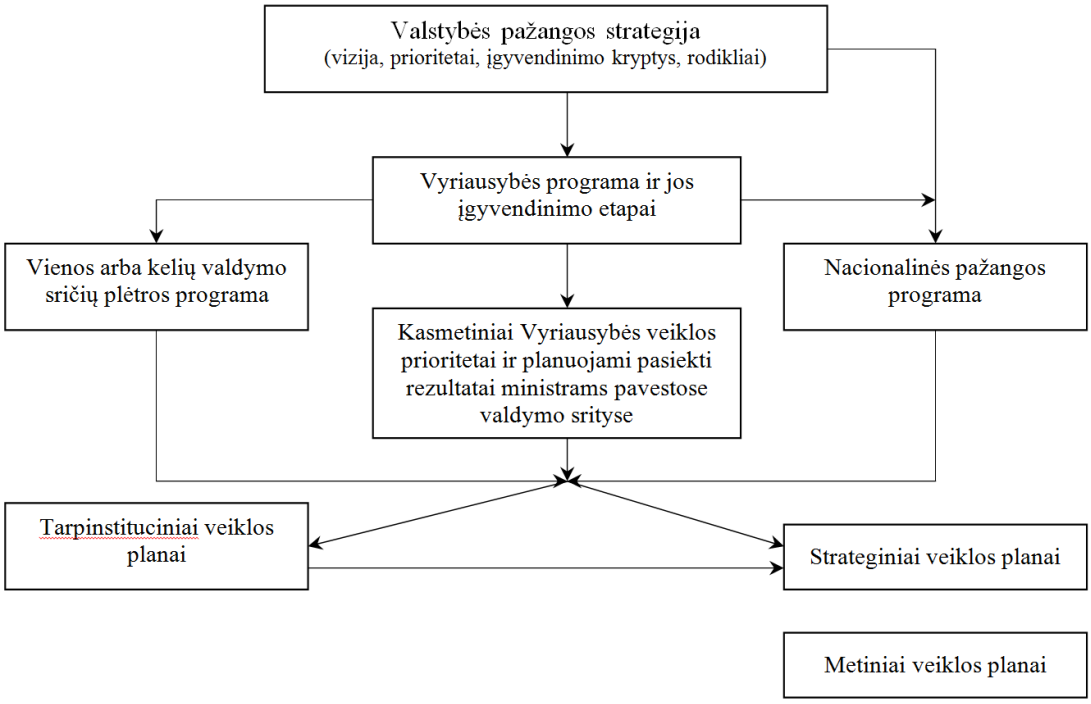
5 Priedas. LIETUVOS IR TARPTAUTINIŲ INFORMACIJOS SAUGUMO REIKALAVIMŲ LYGINAMOJI LENTELĖ

Informacijos saugumo valdymo priemonė	**ISO 27000**	**COBIT**	**Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai**
Saugumo objektas	Informacija	Informacinės technologijos	Informacija
Saugumo tikslai	Konfidencialumas Prieinamumas Vientisumas	Konfidencialumas Prieinamumas Vientisumas	Patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, kokio nors kitokio neteisėto jos tvarkymo
Saugumo dimensijos	Saugumo politika; saugumo organizavimas; vertybių klasifikavimas ir kontrolė; personalo saugumas; fizinis ir aplinkos saugumas; komunikacijos ir operacijų valdymas; prieigos kontrolė; sistemų kūrimas ir priežiūra; incidentų valdymas; veiklos tęstinumo valdymas; atitikimas	Saugumo valdymas; saugumo planas; tapatybės valdymas; naudotojo paskyros valdymas; saugumo testavimas, priežiūra ir stebėsena; saugumo incidento apibrėžimas; saugumo technologijų apsauga; kriptografinio rakto valdymas; kenksmingos programinės įrangos prevencija, aptikimas ir koregavimas; tinklo saugumas; keitimasis diskretiškais duomenimis	Informacinės sistemos duomenų saugos nuostatuose nustatoma: 1. Informacijos saugumo tikslai, svarba ir esama būklė; 2. Informacijos saugumo užtikrinimo prioritetinės kryptys; 3. Informacinės sistemos ir šioje sistemoje tvarkomų duomenų svarba ir pagrindiniai informacinei sistemai, jos dalims ir funkcijoms keliami saugos reikalavimai, pagal kuriuos bus parenkamos atitinkamos saugos priemonės; 4. Saugaus duomenų tvarkymo reikalavimai, kurie apima: 4.1. teisės aktų, kuriais vadovaujamasi tvarkant duomenis ir užtikrinant jų saugumą, sąrašą; 4.2. informacinės sistemos valdytojo personalo kvalifikacinius reikalavimus; 4.3. pagrindines informacinės sistemos valdytojo nuostatas dėl rizikos veiksnių vertinimo, pagrindinių rizikos vertinimo kriterijų apibūdinimą; 5. Informacinės sistemos naudotojų supažindinimo su saugos dokumentais principai; 6. Atsakomybė už saugos dokumentų reikalavimų pažeidimus; Saugaus elektroninės informacijos tvarkymo taisyklėse pateikiama: 1. Informacinėje sistemoje esančios informacijos kategorijų sąrašas ir kiekvienai kategorijai priskirtini duomenys; 2. Techninių ir kitų saugos priemonių aprašymas, apimantis kompiuterinės įrangos, sisteminės ir taikomosios programinės įrangos duomenų perdavimo tinklais saugumo užtikrinimo, patalpų ir aplinkos (įėjimo kontrolė, elektros tiekimas, aplinkos drėgnumas, darbo vietos temperatūra, priešgaisrinė sauga), informacinės sistemos darbo apskaitos ir kitas priemones informacijos saugai užtikrinti; 3. Informacinės sistemos saugą užtikrinantys reikalavimai, keliami nuomojamų ar perkamų informacinių sistemų funkcionavimui reikalingoms paslaugoms (patalpos, įrangos ir sistemų priežiūra, duomenų perdavimas tinklais ir kitos paslaugos); 4. Informacinės sistemos ir duomenų vientisumo pažeidimų fiksavimo ir pažeistų duomenų atkūrimo tvarka (naudotojų veiksmų registravimas, atsarginės duomenų kopijos, jų saugojimas, saugojimo kontrolė ir kita); 5. Saugaus duomenų perkėlimo ar perdavimo tvarka, Nuostatų įgyvendinimo kontrolės tvarka; 6. Duomenų perdavimo tinklais reikalavimai.

Informacijos saugumo valdymo priemonė	ISO 27000	COBIT	Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai
			Informacinės sistemos veiklos tęstinumo valdymo planui keliami šie reikalavimai: 1. Informacinės sistemos veiklos tęstinumo valdymo plane turi būti nurodyta saugos įgaliotinio, administratorių, informacinės sistemos naudotojų funkcijos, įgaliojimai ir veiksmai atkuriant informacinių sistemų veiklą, informacijos saugos incidentų, įvykusių informacinėje sistemoje, tyrimo tvarka. 2. Informacinės sistemos veiklos tęstinumo valdymo plano nuostatos turi būti pagrįstos tam tikrais principais. Privalomi šie pagrindiniai principai: 2.1. informacinės sistemos naudotojų gyvybės ir sveikatos apsauga (būtina užtikrinti visų informacinės sistemos naudotojų gyvybės ir sveikatos apsaugą ir saugumą, kol trunka nenumatyta situacija ir likviduojami avarijų padariniai); 2.2. informacinės sistemos veiklos atkūrimas (informacinių sistemų veikla atkuriama pagal šiame plane numatytą informacinių sistemų funkcijų prioritetą); 2.3. informacinės sistemos naudotojų mokymas (informacinės sistemos naudotojai turi būti supažindinti su minėtu planu ir teisės aktais, nustatančiais kiekvieno informacinės sistemos naudotojo atsakomybę); 2.4. reguliarus šio plano veiksmingumo išbandymas (plano veiksmingumas turi būti reguliariai išbandomas praktinio mokymo metu; plano veiksmingumo išbandymas gali būti planinis arba neplaninis; atsižvelgiant į gautus rezultatus, šis planas turi būti atitinkamai tikslinamas). 3. Informacinės sistemos veiklos tęstinumo valdymo plano nuostatos, be to, gali būti pagrįstos nenumatytų situacijų ir likviduojamų avarijų padarinių valdymo, valstybės institucijos veiklos atkūrimo ir kitais principais. Informacinės sistemos naudotojų administravimo taisyklėse nustatoma: 1. prieinamumo prie duomenų principai; 2. informacinės sistemos naudotojų supažindinimo su saugos dokumentais tvarka; 3. saugaus duomenų teikimo informacinės sistemos naudotojams kontrolės tvarka (informacinės sistemos naudotojų registravimas, teisės dirbti su informacinės sistemos duomenimis suteikimas, informacinės sistemos naudotojų išregistravimas, informacinės sistemos naudotojų tapatybės nustatymas, specialios informacinės sistemos naudotojų tapatybės nustatymo priemonės, elektroninis parašas ir kita); 4. informacinės sistemos naudotojų, turinčių prieigą prie informacinės sistemos ar atskirų jos komponentų, įgaliojimai, teisės ir pareigos.
Saugumo sistemiškumo valdymas	Planuoti, daryti, tikrinti, veikti	Planavimas ir organizavimas, įsigijimas ir įdiegimas, paslaugų teikimas ir palaikymas, stebėjimas ir įvertinimas	

6 Priedas. STRATEGINIO PLANAVIMO DOKUMENTŲ SCHEMA

Planavimo dokumentų schema (Pagal *Strateginio planavimo metodiką*):



7 Priedas. INFORMACIJOS SAUGUMO, ŽINIŲ VADYBOS IR INFORMACINĖS BRANDOS LYGIŲ LYGINAMOJI LENTELĖ

Lygis	**Informacijos saugumo brandos lygiai (COBIT metodika)**	**Žinių vadybos brandos lygiai (Ehms, Langen, 2002)**	**Informacinės brandos lygiai (English, 2004)**
Nulinis	Organizacija nesupranta IT saugos poreikio. Nepaskirta atsakomybė ir atskaitingumas už saugos užtikrinimą. Nevykdomos priemonės, palaikančios IT saugos valdymą. Neinformuojama apie IT saugą ir nereaguojama į IT saugos pažeidimus. Visiškai nėra atpažįstamo sistemos saugos administravimo proceso.		
Pirminis / Ad hoc	Organizacija *supranta poreikį* IT saugai. Supratimas apie saugos poreikį visų pirma priklauso nuo individualių darbuotojų. Į IT *saugą* atsižvelgiama pagal aplinkybes, ji *nevertinama*. Aptikus IT saugos pažeidimus, ieškoma kaltųjų nes *neaiški atsakomybė*. Reagavimas į IT saugos pažeidimus yra nenuspėjamas.	*Procesai nėra sąmoningai kontroliuojami*; dideli pasiekimai dėl turimų žinių vertinami kaip sėkmė, o ne kaip tikslų nustatymo ir planavimo rezultatas.	Neapibrėžtumas. Mes *nežinome, kodėl* mes *turime* informacijos kokybės *problemų*.
Pasikartojantis, bet intuityvus	*Atsakomybė* ir *atskaitingumas* už IT saugą yra *paskirti* IT saugos koordinatoriui, *nors* koordinatoriaus vadovavimo *įgaliojimai* yra *riboti*. Supratimas apie saugos poreikį yra fragmentiškas ir ribotas. Nors sistemos teikia tiesiogiai su sauga susijusią *informaciją*, ji *neanalizuojama*. Trečiųjų šalių paslaugos gali neatsižvelgti į konkrečius organizacijos saugos poreikius. *Formuojama* saugos *politika*, tačiau *įgūdžiai* ir priemonės *nepakankami*. *Atsiskaitymas* apie IT saugą *nepakankamas*, klaidinantis ar netinkamas. Saugos *mokymai* prieinami, tačiau daugiausia vyksta *pavienių darbuotojų iniciatyva*. Į IT saugą visų pirma žiūrima kaip į IT atsakomybę. *Veikla nelaiko, kad* IT *sauga* yra *jos* atsakomybių *srityje*.	Organizacija *pripažįsta* žinių vadybos *reikšmę* verslui; organizaciniai *procesai pavienių* žinių vadybos *pionierių* iš dalies apibūdinami kaip žinių vadybos veiklos; vykdomi *bandomieji* žinių vadybos *projektai*.	Prabudimas. *Ar neišvengiama* yra nuolat *turėti problemų* su informacijos kokybe?
Apibrėžtas	*Vadovai skatina supratimą* apie saugą. IT *saugos procedūros* apibrėžtos ir *suderintos su* IT *saugos politika*. *Atsakomybė* už IT saugą yra *paskirta* ir *suprantama, bet* vykdoma *nenuosekliai*. Sukurtas IT saugos planas ir saugos sprendimai, juos palaiko rizikos analizė. *Informavimas* apie saugą *nėra aiškiai orientuotas į veiklą*. Atliekamas ad hoc saugos testavimas (pvz., įsibrovimo testavimas). Saugos *mokymai prieinami* IT ir veiklos atstovams, bet *planuojami* ir valdomi tik *neformaliai*.	*Nuolat praktikuojamos veiklos, kurios* efektyviai *remia* žinių *vadybą* pavieniuose organizacijos *sektoriuose*; šios *veiklos yra integruotos į* kasdienio darbo *procesus* ir *palaikomos* atitinkamų technologinių *sistemų*.	Suvokimas. Didėjant valdymo įsipareigojimams ir gerėjant informacijos kokybei, *identifikuojamos* ir *sprendžiamos problemos*.

Lygis	**Informacijos saugumo brandos lygiai (COBIT metodika)**	**Žinių vadybos brandos lygiai (Ehms, Langen, 2002)**	**Informacinės brandos lygiai (English, 2004)**
Valdomas ir vertinamas	*Atsakomybė* už IT saugą yra *aiškiai paskirta*, *valdoma* ir *vykdoma*. *Nuosekliai atliekama* IT saugos rizikos ir poveikio *analizė*. Saugos politika ir *procedūros atliekamos remiantis* konkrečiais saugos *baziniais rodikliais*. *Privaloma taikyti metodus*, skatinančius supratimą apie saugą. Standartizuotas naudotojo identifikavimas, autentiškumo patvirtinimas ir įgaliojimų suteikimas. *Vykdomas* už saugos auditą ir valdymą atsakingų *darbuotojų saugos sertifikavimas*. Saugos testavimas atliekamas remiantis *standartizuotais* įformintais *procesais*, vedančiais prie saugos lygių gerinimo. IT saugos procesai koreliuoja su bendra organizacijos saugos funkcija. *Atsiskaitymas* apie IT saugą yra *susietas su veiklos tikslais*. IT *saugos mokymai* teikiami tiek veiklai, tiek IT. Jie *planuojami* ir valdomi taip, *kad atitiktų veiklos poreikius* ir apibrėžtus saugos rizikos profilius. *Saugos* valdymo *tikslai* ir metrikos yra *apibrėžti*, bet dar nevertinami.	*Nuolat matuojami* žinių vadybos *veiklos efektyvumo rodikliai*; ši veikla atlieka ilgalaikį vaidmenį organizacijoje ir yra suderinta su socialinėmis technologinėmis žinių vadybos sistemomis.	Išmintis. Informacijos kokybės *problemų prevencija* yra *nuolatinė* mūsų *operacijų dalis*.
Optimalus	IT *sauga yra bendra* veiklos ir IT *vadovų atsakomybė*, *integruota į organizacijos* saugos *veiklos tikslus*. IT saugos *reikalavimai* aiškiai apibrėžti, *optimizuoti* ir *įtraukti į* patvirtintą saugos *planą*. Naudotojai ir klientai vis labiau atskaitingi už saugos reikalavimų apibrėžtį, o projektavimo etape saugos funkcijos integruotos į taikomąsias programas. *Saugos incidentai* tuojau pat *sprendžiami įformintomis* reagavimo į incidentus *procedūromis*, *palaikomomis automatizuotų priemonių*. *Periodiškai atliekamas* saugos *vertinimas* siekiant įvertinti saugos plano įgyvendinimo rezultatyvumą. *Sistemiškai* renkama ir *analizuojama informacija* apie grėsmes ir silpnąsias vietas. Tuojau pat pranešama apie atitinkamas rizikos mažinimo kontrolės priemones ir imama jas taikyti. Saugos testavimas, saugos incidentų esminių priežasčių *analizė* ir aktyvus rizikos nustatymas naudojamas nuolat *tobulinti procesą*. Saugos procesai ir technologijos *integruojamos į visą organizaciją*. Saugos valdymo metrika vertinama, kaupiama ir apie ją informuojama. *Vadovybė* šiuos vertinimo rodiklius *naudoja nuolatiniame tobulėjimo procese* saugos planui koreguoti.	Žinių vadybos *matavimo priemonės derinamos su* kitais *strateginės kontrolės instrumentais*; *nėra* jokių *iššūkių*, *kurie negalėtų būti įveikti pasitelkiant* žinių *vadybos priemones*.	Įsitikinimas. Mes *žinome*, *kodėl* mes *neturime* informacijos kokybės *problemų*.

8 Priedas. EKSPERTŲ INTERVIU IŠRAŠAI

Ekspertas 01

Informacijos saugumo valdymo objektas ir tikslai.

(Informacijos saugumo objektas: informacija, informacinės sistemos, technologijos, tinklai; Saugumo tikslai: CIA triada – konfidencialumas (confidentiality), vientisumas (integrity) ir prieinamumas (availability)).

Europos Sąjungoje nėra bendros nuomonės, kas turėtų būti informacijos saugumo objektas. Rengiant strateginius saugumo dokumentus netgi galvojama apie Europos Sąjungos Interneto saugumo programą, manoma, kad Kibernetinio saugumo strategija skamba per daug techniškai, ypač aukščiausio lygio vadovybei, todėl sunku atkreipti vadovų dėmesį į saugumo problemas. Lietuvoje informacijos saugumo objektu, priėmus naują įstatymą, tapo informacijos ištekliai; Latvijoje, Estijoje – daugiau akcentuojami ryšių tinklai, kibernetinė erdvė.

Saugant informaciją, tikslais pagal prioritetus galėtų būti įvardinti – CIA, tinklus – AIC. Lietuvoje galbūt formaliai šie tikslai nėra tiesiogiai deklaruoti, tačiau vertinant visą teisės aktų ir reikalavimų visumą, galima juos įžvelgti. Pačių institucijų požiūris į saugumo prioritetus, vertinant savo situaciją, nėra tirtas, būtų įdomu išsiaiškinti jų požiūrį, kas joms svarbiausia, o ypač vertinant deklaruojamus prioritetus su realiai taikomomis saugos priemonėmis.

Informacijos saugumo valdymo organizavimas, kompetencijos ir atsakomybės.

Tarpinstitucinę koordinacinę funkciją Lietuvoje vykdo išplėsta Saugos koordinavimo komisija. Patvirtinus naują Elektroninės informacijos saugos (kibernetinio saugumo) plėtros programą, jos įgyvendinimo koordinatore paskirta Vidaus reikalų ministerija. Kibernetinio saugumo programoje numatytas naujas patariamasis organas – konsultacinė taryba. Jos sudarymas planuojamas artimiausiu metu. Įgyvendinant pavienes saugos funkcijas, atsakomybe dalinasi kelios institucijos – pvz., Susisiekimo ministerija atsako už tinklų saugumą ir pan. Lietuvoje vėliausiai

susirūpinta kritinės infrastruktūros saugumo funkcijomis, šiuo metu tik pradedami veiksmai siekiant identifikuoti tokią infrastruktūrą, parengti saugumo reikalavimus.

Bendra tendencija valstybiniame sektoriuje – trūksta resursų saugos funkcijoms vykdyti ir institucijose, besirūpinančiose savo saugumu, ir institucijose, vykdančiose platesnes priežiūros ar koordinavimo funkcijas. Trūksta tiek etatų, tiek kompetencijos, tiek ir finansų.

Privalumas būtų – veikianti idėjų generavimo, konsultacinė struktūra, kitas klausimas, ar ji sugebės ką nors nuveikti. Čia būtų galima pasimokyti iš Estijos, kurioje labai sėkmingai veikia savanoriška organizacija – Saugumo lyga, pavyzdžio. 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, veikianti pagal griežtas taisykles, o valstybė išlaiko tik nedidelę administraciją, visi kiti dirba neatlygintinai. Beje, šiuo pavyzdžiu ketina sekti ir kaimynai latviai, susidomėjimą išreiškė ir kitos šalys.

Informacijos saugumo brandos vertinimo kriterijai ir poreikis. Institucijų situacija.

Pagal Kibernetinio saugumo programą numatytas brandos stebėjimas, tačiau kol kas nėra bendros metodikos brandai vertinti, nebuvo vykdyti platūs tyrimai. Tokia metodika galėtų remtis COBIT, ITIL ar kitos tarptautinės metodikos principais. Iš pavienių tyrimų galima numanyti, kad maždaug du trečdaliai Lietuvos institucijų atitinka maždaug pirmą, trečdalis antrą brandos lygį (iš penkių), galbūt su labai retomis išimtimis.

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.

Informacijos saugumo funkcijų centralizavimo poreikis ir apimtys.

Funkcijos galėtų būti centralizuojamos įvairiais lygmenimis, pavyzdžiui, „vyriausybės debesis“ (*angl. Government Cloud*), kolektyvinės ryšių gynybos sistemos ar kitos infrastruktūrinės priemonės.

Taip pat galėtų būti rengiamos vienodos metodikos, daromos rizikos analizės ar intervenciniai auditai. Tai leistų taupyti finansinius išteklius, lengviau palyginti institucijų situaciją.

Informacijos saugumo stebėsenos ir kontrolės sistemos kūrimas ir vertinimo kriterijai.

Įgyvendinant Kibernetinio saugumo programą planuojamas stebėsenos sistemos kūrimas. Tokia sistema leistų stebėti institucijų atitiktį saugos reikalavimams, dokumentų savalaikį parengimą ir atnaujinimą. Sistema apimtų rizikos analizes, išorinius ir vidinius auditus, jų rezultatus bei šių rezultatų įgyvendinimą. Galėtų būti stebimas ir organizacijų brandos lygis ir jo kitimas.

Ekspertas 02

Informacijos saugumo valdymo objektas ir tikslai.

(Informacijos saugumo objektas: informacija, informacinės sistemos, technologijos, tinklai; Saugumo tikslai: CIA triada – konfidencialumas (confidentiality), vientisumas (integrity) ir prieinamumas (availability)).

Informacijos saugumo objektu valstybės institucijose susiklostė informacinės sistemos, tačiau šiuo metu vis daugiau duomenų perduodami ryšių tinklais, ypač vertinant įsivyraujančias „debesų kompiuterijos“ tendencijas. Iškyla opus klausimas – kaip apsaugoti informaciją, kai ji perduodama iš sistemos į sistemą, akivaizdu, kad derėtų apmąstyti saugumo objekto plėtimą, galbūt susijungiant informacines sistemas ir ryšių tinklus, taip pat svarstytinas klausimas dėl informacijos, kaip bendrinio saugos objekto, apibrėžimo.

Įvairaus lygio teisės aktuose įtvirtinti saugumo tikslai, apimantys konfidencialumą, taip pat jau formalizuotas vientisumo užtikrinimo poreikis. Šiuo metu kaip tik rengiami reikalavimai, kurie detalizuotų vientisumo apibrėžimą ir apimtį. Prieinamumo klausimai taip pat svarbūs, kokia nauda iš sistemų, jei jomis

negalima pasinaudoti. Šie klausimai galbūt nėra aiškiai ir formaliai deklaruoti, tačiau galima įžvelgti šio tikslo siekimą per kritinių incidentų turinį. Šiuo metu Europos Sąjungos mastu bandoma apibrėžti kritinius incidentus, kurie išreiškiami per incidento poveikį vartotojų skaičiui ir per incidento trukmę. Taigi prieinamumo užtikrinimo siekį galima įžvelgti.

Informacijos saugumo valdymo organizavimas, kompetencijos ir atsakomybės.

Lietuvoje, įsigaliojus naujai Kibernetinio saugumo programai, koordinavimo klausimai deleguoti tarpinstitucinei komisijai, konsultavimo klausimai – konsultacinei tarybai, deja, šiuo metu ji dar nesudaryta. Galima pastebėti tiek verslo, tiek ir akademinio sluoksnių pageidavimus dalyvauti platesnio pobūdžio konsultaciniame procese. Formaliai institucijoms išdalintos atsakomybės sritys, šiuo metu daug institucijų dalyvauja įgyvendinant Kibernetinio saugumo programą (Susisiekimo, Švietimo ir mokslo, Vidaus reikalų ir kitos ministerijos, Ryšių reguliavimo tarnyba, Valstybinė asmens duomenų apsaugo inspekcija ir kitos), veiksmų koordinavimas paskirtas Vidaus reikalų ministerijai. Kitas klausimas – kaip šioms institucijoms sekasi realiai įgyvendinti savo funkcijas? Pastebima gana aiški valstybiniam sektoriui būdinga tendencija – kompetentingų specialistų, finansų ir kitų resursų trūkumas. Dažnai saugos prioritetai pasimeta tarp kitų institucijų funkcijų. Galima pastebėti, kad ir kritinės infrastruktūros klausimai nėra tinkamai sprendžiami, – neturime ne tik vienareikšmiškai atsakingos institucijos, bet net ir šios infrastruktūros apibrėžimo. Galbūt paminėčiau šiokią tokią Valstybės kontrolės auditų teigiamą įtaka institucijų veiksmams stiprinant saugumą.

Informacijos saugumo brandos vertinimo kriterijai ir poreikis. Institucijų situacija.

Galima numanyti, kad institucijų branda yra labai įvairi, tikrai yra institucijų, smarkiai pažengusių, tačiau kas darosi, pavyzdžiui, savivaldybių lygmenyje, labai sunku pasakyti. Tyrimai šiame kontekste nedaryti ir tikrai būtų aktualūs.

Informacijos saugumo funkcijų centralizavimo poreikis ir apimtys.

Šis klausimas gali būti siejamas tiek su institucijų branda, tiek ir su valdomos informacijos svarba. Labiau brandžios institucijos galbūt gali „savimi pasirūpinti“, tačiau mažiau brandžioms tikrai praverstų centralizuota pagalba – kompetencijos kėlimo, audito, rizikos analizės klausimais. Kita vertus, net ir brandžioms institucijoms vertinga gali būti išorės audito nuomonė „iš šalies“. Verta būtų svarstyti tokių funkcijų kaip atsakomybės ir finansinių resursų paieškos klausimų centralizuotą paskyrimą kokiai nors institucijai.

Informacijos saugumo stebėsenos ir kontrolės sistemos kūrimas ir vertinimo kriterijai.

Šiuo metu egzistuoja rimta automatizuota incidentų ir anomalijų tinkluose stebėsenos sistema. Taip pat aktyviai dirbama su operatoriais, užsienio partneriais, ENISA. Galima pastebėti, kad tokios sistemos imlios ir žmogaus darbui, tačiau ne visada tam pakanka resursų.

Stebėsenos ir tyrimų organizacinių priemonių, institucijų kompetencijų kaip ir brandos lygmenyje trūksta.

Ekspertas 03

Informacijos saugumo valdymo objektas ir tikslai.

(Informacijos saugumo objektas: informacija, informacinės sistemos, technologijos, tinklai; Saugumo tikslai: CIA triada – konfidencialumas (confidentiality), vientisumas (integrity) ir prieinamumas (availability)).

Remiantis teisės aktais, valdytojai rengia saugos dokumentus, anksčiau objektas buvo registrai ir informacinės sistemos, įsigaliojus Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymui, objektu tapo informaciniai ištekliai. Kol kas nėra priimti reikalingi teisės aktai, todėl sunku prognozuoti, ar kas nors keisis, tačiau informaciniai ištekliai – tai tie patys registrai ir informacinės sistemos. Galbūt vertėtų mažinti objektų skaičių, informacijos saugumo reglamentavimą galima būti sieti su organizacija. Tai aktualu daugiau išteklių valdančioms institucijoms.

Galiojančiuose informacijos saugumo reikalavimuose pirmos kategorijos (svarbiausioms) sistemoms neproporcingai sureikšmintas informacijos prieinamumo reikalavimas – sistemos atstatymas per 15 min. nepasiekiamas net ir institucijoms, valdančioms kritinės svarbos sistemas. Iš esmės šis reikalavimas įgyvendinamas tik formaliai, tinkamas jo realizavimas pareikalautų labai daug finansinių resursų. Net tarptautinės svarbos duomenis valdančioms sistemoms ir Europos Sąjungos reikalavimus turinčioms tenkinti institucijoms prieinamumo reikalavimai nėra tokie griežti. Reikalavimai turėtų būti labiau detalizuojami pagal duomenų svarbumą, daugeliui valdytojų gali būti reikšmingesnis pačių duomenų išsaugojimo (vientisumo) ar konfidencialumo reikalavimas. Pagal šiuos reikalavimus operatorių darbo vietoms taikome griežtas tinklo atskyrimo nuo išorės tinklų bei identifikavimo priemones, kurias dar labiau stiprinsime pasitelkdami Europos Sąjungos paramą.

Informacijos saugumo valdymo organizavimas, kompetencijos ir atsakomybės.

Įsigaliojus minėtam Valstybės informacinių išteklių valdymo įstatymui, atsakingos institucijos (ministerijos) pradėjo tikslinti savo nuostatus, kurie šiuo metu derinami. Parengtas ir pavirtintas šiam įstatymui įgyvendinti reikalingų teisės aktų sąrašas. Tikėtinas institucijų funkcijų ir atsakomybių persiskirstymas, naujų ar patikslintų saugumo reikalavimų atsiradimas. Bendra tendencija – kompetencijos trūkumas ir žmonių stoka. Su esamu etatų skaičiumi iš atsakingų institucijų sunku tikėtis proveržio ar didelių darbų. Jau kurį laiką galima stebėti lėtą reikalingų teisės aktų rengimą, užtrunkantį nuostatų ir kitų saugos dokumentų derinimą.

Informacijos saugumo brandos vertinimo kriterijai ir poreikis. Institucijų situacija.

Institucijų branda ir saugumo reikšmės supratimas tikrai įvairus, vienose saugumu rūpinasi vos vienas darbuotojas, kuris turi ir kitų, nesusijusių su saugumu, funkcijų, kitose tuo užsiima dedikuoti skyriai. Kai kurios institucijos užsisako išorinio atitikties vertinimo paslaugas ir jau dabar atitinka saugumo valdymo standartus.

Informacijos saugumo funkcijų centralizavimo poreikis ir apimtys.

Galėtų būti centralizuojamos funkcijos bent jau apimant valdomas sistemas pagal veiklos sritis. Ministerijos galėtų centralizuotai vykdyti mokymus, saugos vertinimą, tipinių teisės aktų rengimą visoms savo pavaldžioms institucijoms. Taip pat būtų sveikintinas dalykas – infrastruktūros centralizavimas, pavyzdžiui, dviejų valstybės „debesų“ sukūrimas. Institucijoms tai leistų mažiau rūpintis su tiesiogine veikla nesusijusiomis funkcijomis, lengviau atitikti iškeltus saugos reikalavimus, stebėti jų pokyčius.

Informacijos saugumo stebėsenos ir kontrolės sistemos kūrimas ir vertinimo kriterijai.

Su esama kompetencija ir resursais sunkiai tikėtina reikšminga stebėsena ir kontrolė. Tikėtina, kad įgyvendinus numatytus darbus tai bus sukurta.

Ekspertas 04

Informacijos saugumo valdymo objektas ir tikslai.

(Informacijos saugumo objektas: informacija, informacinės sistemos, technologijos, tinklai; Saugumo tikslai: CIA triada – konfidencialumas (confidentiality), vientisumas (integrity) ir prieinamumas (availability)).

Buvo diskusijų dėl objekto keitimo, tačiau istoriškai susiklosčiusią situaciją labai sudėtinga pakeisti, tam reikėtų labai daug resursų ir pastangų. Galbūt vertėtų sujungti daugiau išteklių valdančių institucijų rengiamus saugos dokumentus, galima stiprinti reikalavimus Elektroninių ryšių įstatyme.

Derėtų peržiūrėti reikalavimus įgyvendinant naujus teisės aktus – Valstybės informacinių išteklių valdymo įstatymą, Kibernetinio saugumo programą. Institucijoms turėtų būti labiau leidžiama pasirinkti joms aktualius saugumo tikslus ir atitinkamai jų siekimo priemones, tačiau procesas turi būti gerai apgalvotas, nepamatuoti keitimai gali sukurti daug bereikalingo biurokratinio darbo ir neatnešti jokios papildomos naudos saugumui.

Informacijos saugumo valdymo organizavimas, kompetencijos ir atsakomybės.

Neseniai iš naujo sudaryta Elektroninės informacijos saugos (kibernetinio saugumo) koordinavimo komisija, joje atsirado Užsienio reikalų ministerijos, Valstybės saugumo departamento atstovai. Galima tikėtis, komisija pradės koordinuoti darbus, rinkti ir svarstyti institucijų ataskaitas. Komisijai tebevadovauja Vidaus reikalų ministerijos viceministras, ši institucija taip tik keičia savo nuostatus, planuojama įrašyti platesnę saugumo koordinavimo funkciją. Taip pat sudarytas sąrašas teisės aktų, kuriuos būtina parengti naujam Valstybės informacinių išteklių valdymui įgyvendinti, tarp jų yra ir susijusių su saugumu.

Šiaip saugumo srityje, kaip dažnai būna valstybės institucijų sektoriuje, koordinatorių daug, o realius darbus dirbti nėra kam, ką yra pastebėjusi ir Valstybės kontrolė. Aišku, tam reikia ir kompetencijos, po kelis žmones institucijose, ypač vertinant biurokratinio darbo mastus, tikrai negali nuveikti didelių darbų. Su šia valdžia iki naujų rinkimų mažai tikėtinas koks nors proveržis.

Informacijos saugumo brandos vertinimo kriterijai ir poreikis. Institucijų situacija.

Institucijos paliktos savieigai, stipresnės juda, silpnesnės – labai sunkiai. Vertinimai labiau proginės veiklos nei sistema. Net ir didelės institucijos, investavusios ženklias sumas į sistemas ir saugą, nesugeba išvengti incidentų. Taip neturėtų būti.

Informacijos saugumo funkcijų centralizavimo poreikis ir apimtys.

Centralizuoti funkcijas tikrai yra poreikis. Esant tokiai kompetencijos situacijai valstybės sektoriuje, tikrai reikia galvoti apie kompetencijų centrus, institucijos nesugebės kiekviena sau išlaikyti profesionalių specialistų. Vertėtų jungti pajėgumus ir saugos srityje, turi atsirasti saugumo kompetencijos centras.

Kompetencijos centrai galėtų būti ir pagal funkcines sritis, pavyzdžiui, savo kompetenciją ir kitus pajėgumus galėtų sujungti Valstybinė mokesčių inspekcija, SODRA, Muitinės departamentas.

Informacijos saugumo stebėsenos ir kontrolės sistemos kūrimas ir vertinimo kriterijai.

Numatytos kelios priemonės Kibernetinio saugumo programos įgyvendinimo plane, iš tiesų tokios sistemos poreikis yra.

Ekspertas 05

Informacijos saugumo valdymo objektas ir tikslai.

(Informacijos saugumo objektas: informacija, informacinės sistemos, technologijos, tinklai; Saugumo tikslai: CIA triada – konfidencialumas (confidentiality), vientisumas (integrity) ir prieinamumas (availability)).

Tarp saugos specialistų nuolat kyla diskusijų dėl informacijos saugumo objekto – sistemos ar tinklai, o pagrindas yra informacija ir duomenys, juos ir reikėtų saugoti. Deja, jie dažniausiai apdorojami informacinėmis technologijomis, todėl dažnai galima sutikti dar ir sureikšminamą informacinių technologijų saugumo sąvoką. Nuo seno Lietuvoje susiklostė informacinės sistemos kaip saugumo objektas, jose kaip ir registruose tikrai valdoma svarbiausia valstybei informacija, tačiau buvo didelė spraga vertinant bendrą institucijose valdomos informacijos kiekį, kuriam saugumo reikalavimai nebuvo taikomi. Naujasis Valstybės informacinių išteklių valdymo įstatymas apėmė daug didesnį išteklių skaičių ir praktiškai dengia visas informacijos valdymo formas institucijose, vertinant tai, kad institucijos, valdančios kelis ar keliolika informacijos išteklių gali sujungti jų saugos reglamentavimą viename pagrindiniame dokumente. Šis įstatymas sudaro kaip niekad geras prielaidas informacijos saugai užtikrinti.

Informacijos prioritetai tikrai svarbus klausimas, tačiau esama situacija, suvienodinusi visas institucijas prioritetų klausimu, tikrai nėra pati tinkamiausia. Brandžios institucijos turėtų turėti galimybę pačios pasirinkti – konfidencialumas, prieinamumas ar vientisumas joms didesnis prioritetas, ir pagal tai rinktųsi saugos priemones.

Informacijos saugumo valdymo organizavimas, kompetencijos ir atsakomybės.

Saugumo valdymo organizavimas tikrai neblogas formaliąja prasme – yra įstatymas, reikalavimai, institucijų įdirbis, tačiau paskutiniu metu atsakingų institucijų, gal išskyrus Ryšių reguliavimo tarnybą, kompetencija saugos srityje pastebimai sumenko. Pagrindinė koordinatorė – Vidaus reikalų ministerija, turėjusi dedikuotus padalinius saugos problemoms koordinuoti ir spręsti, krizės metu visai išbarstė kompetenciją, panašios tendencijos pastebimos ir kitose institucijose, saugos atsakomybės išdalintos po truputį daugelyje institucijų. Šioks toks kompensavimo mechanizmas yra neseniai iš naujo sudaryta Elektroninės informacijos saugos koordinavimo komisija, ją sustiprino Užsienio reikalų ministerijos bei Valstybės saugumo atstovai. Galbūt tai duos kažkokių rezultatų. Šia kolegialią instituciją galėtų pastiprinti viešojo ir privataus sektorių bendradarbiavimo pagrindu veikiantis kompetencijos centras, kuris galėtų jungti ir akademinio sluoksnio specialistus.

Galbūt daugiau tvarkos padėtų įnešti ir Valstybės kontrolės aktyvesnė veikla analizuojant saugos įgyvendinimą institucijose.

Informacijos saugumo brandos vertinimo kriterijai ir poreikis. Institucijų situacija.

Neteko girdėti apie platesnius brandos vertinimus, galima numanyti „mažąsias“ institucijas esant nuliniame ar pirmajame lygyje, matyt, daugiau palypėjusios būtų labiau finansuojamos Finansų ar Krašto apsaugos ministerijų kuruojamos įstaigos. Tikrai vertėtų sukurti brandos vertinimo sistemą valstybės institucijoms, kad ir COBIT ar panašios metodikos pagrindu.

Informacijos saugumo funkcijų centralizavimo poreikis ir apimtys.

Manyčiau, be bent jau kai kurių funkcijų ir veiklų centralizavimo, valstybės institucijoms sunkiai pavyks ką nors reikšmingo nuveikti. Centralizavimas tikrai praverstų techninės infrastruktūros lygmenyje – apsaugotas valstybės institucijų tinklas, „dubliuotas valstybinis debesis“, kolektyvinė gynybos sistema tikrai ženkliai sustiprintų institucijų situaciją.

Kitas labai svarbus veiksnys – stipri koordinuojanti institucija, turinti pakankamai kompetencijos koordinuoti darbus, organizuoti centralizuotus saugos vertinimus, auditus, rizikos analizes, metodinius dokumentus, mokymus ir pan.

Informacijos saugumo stebėsenos ir kontrolės sistemos kūrimas ir vertinimo kriterijai.

Tokia sistema turėtų būti esminis koordinuojančios institucijos darbo įrankis.

Ekspertas 06

Informacijos saugumo valdymo objektas ir tikslai.

Informacijos saugumo objektas turėtų būti informacija, kaip vienetas, tiesiogiai nesiejant nei su informacinėmis sistemomis ar ištekliais, nei su ryšių tinklais. Šiuo metu yra tarpinis laikotarpis, nors įprastai poįstatyminiai aktai turėtų įsigalioti kartu su įstatymu, šiuo atveju Valstybės informacinių išteklių valdymo įstatymas jau galioja nuo metų pradžios, tačiau teisės aktai, kurių reikia šiam įstatymui įgyvendinti, dar tik planuojami. Tam yra parengtas specialus planas. Dalis šių teisės aktų turėtų būti priimti iki metų pabaigos, kiti 2013-aisiais. Tačiau reiktų vertinti, kad šie metai yra rinkiminiai, todėl sunku prognozuoti, ar planuojami teisės aktai laiku ir tinkamai bus priimti. Beje, institucijų veiksmų „nespartina“ ir tai, kad Kibernetinio saugumo programoje numatyti vertinimo kriterijai tik 2015 ir 2019 metams.

Saugumo tikslai, taikomos saugos priemonės turėtų remtis informacijos klasifikavimu. Pastebėtina, kad šiuo metu galioja kiek komplikuotas informacijos klasifikavimas, anksčiau buvo keturios kategorijos, įsigaliojęs įstatymas numato kiek kitokią klasifikaciją, išskiriami ypatingos svarbos, svarbūs ir pan. informaciniai ištekliai. Taip pat reiktų vertinti asmens duomenų, viešos informacijos kategorijas. Asmens duomenims apsaugoti taikomi specializuoti reikalavimai. Galėtų būti ieškoma bendrumų tarp šių kategorijų ir tik esant išskirtiems ypatumams taikomi specializuoti reikalavimai.

Informacijos saugumo valdymo organizavimas, kompetencijos ir atsakomybės.

Institucijų kompetencijos gana aiškios, Valstybės informacinių išteklių valdymo įstatymas taip pat sudėliojo kai kuriuos klausimus. Daugiausiai neatsakytų klausimų išlieka dėl kritinės infrastruktūros identifikavimo ir apsaugos. Šiuo metu šiek tiek išsiskiria institucijų nuomonės dėl tolesnio (platesnio) informacijos saugumo reglamentavimo – Seimo informacinės visuomenės plėtros komiteto atstovai yra išsakę nuomonę dėl informacijos saugumo reglamentavimo specialiu saugos įstatymu, tačiau Vidaus reikalų ministerija laikėsi pozicijos, kad galima modernizuoti saugumo reglamentavimą esamo, Valstybės informacinių išteklių valdymo, įstatymo bazėje. Galėtų būti ir keli įstatymai, svarbu jie veiktų.

Paminėtina ir numatyta steigti tarpinstitucinė, konsultacinė Taryba, nors jos statusas vis dar nėra aiškus, tačiau galėtų būti pasisemta patirties, kaip tokie dariniai veikia užsienio šalyse, ir išnaudota galimybė pasitelkti akademinį bei privatų sektorius. Geri papildomos kompetencijos pritraukimo pavyzdžiai – kai kurių ministerijų bendradarbiavimas su universitetais. Ar dalyvavimas tarptautinių organizacijų veikloje. Pastebėtina, kad brandesnės organizacijos daugiau pasiekusios, pavyzdžiui, buriasi kompetencijų centrai bendradarbiaujant didžiosioms savivaldybėms su universitetais ir pan.

Informacijos saugumo brandos vertinimo kriterijai ir poreikis. Institucijų situacija.

Šiuo metu nėra aiški institucijų brandos būklė, nors pastebima, kad institucijos pradeda po truputį suprasti pridėtinę jos vertę. Informacijos saugumo patirtis ir kompetencija kyla kartu su branda.

Brandos lygiai turėtų sietis ir su taikymo apimtimi, nebūtina taikyti visų saugumo priemonių, išdėstytų standartuose, šimtu procentų. Kai kurios institucijos yra priverstos tai daryti teisės aktais, tačiau tiesioginis standartų įgyvendinimas sietinas ir su nemažu lėšų poreikiu. Naujai įsigalioję teisės aktai (Valstybės informacinių išteklių valdymo įstatymas ir Elektroninės informacijos (kibernetinio saugumo) programa) liečia ir brandos klausimus, tačiau dar per mažai laiko poveikiui vertinti.

Informacijos saugumo funkcijų centralizavimo poreikis ir apimtys.

Valstybė turėtų aiškiai suinventorizuoti turimą turtą ir tada būtų galima spręsti dėl valstybės institucijų valdomos infrastruktūros konsolidavimo, centralizuoto naudojimo. Konsolidavimo užuomazgas sudaro Valstybės informacinių išteklių įstatyme apibrėžiama sveikumo platforma, kuria siekiama išnaudoti esamus išteklius ir paslaugas, nebekurti dar kartą esamų funkcionalumų.

Kita funkcijų centralizavimo sritis galėtų būti mokymų vykdymas ar bent organizavimas; informacijos saugumo kompetencijos trūkumas ir konsultacijų poreikis pastebimas visuose lygiuose. Galėtų būti svarstomas centralizuotas rizikos analizės ir vertinimo, saugos ir valdymo audito vykdymas. Labai naudinga būtų vienoda metodika ir palyginami kriterijai, esami įrankiai jau nebeatitinka realybės. Taip pat galėtų būti apibrėžti taikytini informacijos saugumo sertifikatai auditoriams ir institucijoms, išorinio audito tvarka, galbūt jis irgi galėtų būti vykdomas (užsakomas) centralizuotai.

Informacijos saugumo stebėsenos ir kontrolės sistemos kūrimas ir vertinimo kriterijai.

Tokios sistemos kūrimas numatytas, girdėti Vidaus reikalų ministerijos ketinimai tokią sistemą kurti. Šis įrankis galėtų padėti apibrėžti ir stebėti tą pačią institucijų brandą, atitiktį teisės aktuose įtvirtintiems reikalavimams, auditų, rizikos analizių rezultatus, spręsti apie institucijų kompetenciją ir pagalbos joms poreikį.

9 Priedas. EKSPERTŲ INTERVIU APIBENDRINAMOJI LENTELĖ

Tema	Citata	Eksperto Nr.
Informacijos saugumo valdymo objektas ir tikslai	„Europos Sąjungoje nėra bendros nuomonės, kas turėtų būti informacijos saugumo objektu“.	Ekspertas Nr. 1
	„<...> galvojama apie Europos Sąjungos Interneto saugumo programą, manoma, kad Kibernetinio saugumo strategija skamba per daug techniškai, ypač aukščiausio lygio vadovybei, todėl sunku atkreipti vadovų dėmesį į saugumo problemas“.	Ekspertas Nr. 1
	„Lietuvoje informacijos saugumo objektu, priėmus naują įstatymą, tapo informacijos ištekliai“.	Ekspertas Nr. 1
	„Saugant informaciją, tikslais pagal prioritetus galėtų būti įvardinti – CIA, tinklus – AIC“.	Ekspertas Nr. 1
	„<...> tikslai nėra tiesiogiai deklaruoti, tačiau vertinant <...> visumą, galima juos įžvelgti“.	Ekspertas Nr. 1
	„<...> institucijų požiūris į saugumo prioritetus <...> nėra tirtas, būtų įdomu išsiaiškinti jų požiūrį“.	Ekspertas Nr. 1
	„Informacijos saugumo objektu valstybės institucijose susiklostė informacinės sistemos“.	Ekspertas Nr. 2
	„<...> derėtų apmąstyti saugumo objekto plėtimą, galbūt sujungiant informacines sistemas ir ryšių tinklus <...> svarstytinas klausimas dėl informacijos kaip bendrinio saugos objekto apibrėžimo“.	Ekspertas Nr. 2
	„Iškyla opus klausimas – kaip apsaugoti informaciją, kai ji perduodama iš sistemos į sistemą“.	Ekspertas Nr. 2
	„<...> įtvirtinti saugumo tikslai, apimantys konfidencialumą“.	Ekspertas Nr. 2
	„<...> formalizuotas vientisumo užtikrinimo poreikis“.	Ekspertas Nr. 2
	„Prieinamumo klausimai taip pat svarbūs, <...> galbūt nėra aiškiai ir formaliai deklaruoti, tačiau galima įžvelgti šio tikslo siekimą“.	Ekspertas Nr. 2
	„<...> anksčiau objektas buvo registrai ir informacinės sistemos, įsigaliojus Valstybės informacinių išteklių valdymo įstatymui, objektu tapo informaciniai ištekliai“.	Ekspertas Nr. 3
	„Galbūt vertėtų mažinti objektų skaičių, informacijos saugumo reglamentavimą galima būti sieti su organizacija“.	Ekspertas Nr. 3
	„Tai aktualu daugiau išteklių valdančioms institucijoms“.	Ekspertas Nr. 3
	„<...> pirmos kategorijos (svarbiausioms) sistemoms neproporcingai sureikšmintas informacijos prieinamumo reikalavimas – sistemos atstatymas per 15 min. nepasiekiamas net ir institucijoms, valdančioms kritinės svarbos sistemas“.	Ekspertas Nr. 3
	„<...> reikalavimas įgyvendinamas tik formaliai, tinkamas jo realizavimas pareikalautų labai daug finansinių resursų“.	Ekspertas Nr. 3

Tema	Citata	Eksperto Nr.
	„Reikalavimai turėtų būti labiau detalizuojami pagal duomenų svarbumą“.	Ekspertas Nr. 3
	„<...> istoriškai susiklosčiusią situaciją labai sudėtinga pakeisti, tam reikėtų labai daug resursų ir pastangų“.	Ekspertas Nr. 4
	„Institucijoms turėtų būti labiau leidžiama pasirinkti joms aktualius saugumo tikslus ir atitinkamai jų siekimo priemones, tačiau procesas turi būti gerai apgalvotas, nepamatuoti keitimai gali sukurti daug bereikalingo biurokratinio darbo ir neatnešti jokios papildomos naudos saugumui“.	Ekspertas Nr. 4
	„Tarp saugos specialistų nuolat kyla diskusijų dėl informacijos saugumo objekto – sistemos ar tinklai“.	Ekspertas Nr. 5
	„<...> pagrindas yra informacija ir duomenys, juos ir reikėtų saugoti“.	Ekspertas Nr. 5
	„Nuo seno Lietuvoje susiklostė informacinės sistemos kaip saugumo objektas“.	Ekspertas Nr. 5
	„<...> buvo didelė spraga vertinant bendrą institucijose valdomos informacijos kiekį, kuriam saugumo reikalavimai nebuvo taikomi“.	Ekspertas Nr. 5
	„Naujasis Valstybės informacinių išteklių valdymo įstatymas apėmė daug didesnį išteklių skaičių ir praktiškai dengia visas informacijos valdymo formas institucijose”.	Ekspertas Nr. 5
	„<...> sudaro kaip niekad geras prielaidas informacijos saugai užtikrinti“.	Ekspertas Nr. 5
	„<...> situacija, suvienodinusi visas institucijas prioritetų klausimu, tikrai nėra pati tinkamiausia. Brandžios institucijos turėtų turėti galimybę pačios pasirinkti“.	Ekspertas Nr. 5
	„Informacijos saugumo objektas turėtų būti informacija, kaip vienetas, tiesiogiai nesiejant nei su informacinėmis sistemomis ar ištekliais, nei su ryšių tinklais“.	Ekspertas Nr. 6
	„Šiuo metu yra tarpinis laikotarpis <...> Valstybės informacinių išteklių valdymo įstatymas jau galioja, <...> tačiau teisės aktai, kurių reikia šiam įstatymui įgyvendinti, dar tik planuojami“.	Ekspertas Nr. 6
	„<...> šie metai yra rinkiminiai, todėl sunku prognozuoti, ar planuojami teisės aktai laiku ir tinkamai bus priimti“.	Ekspertas Nr. 6
	„Saugumo tikslai, taikomos saugos priemonės turėtų remtis informacijos klasifikavimu“.	Ekspertas Nr. 6
	„<...> galioja kiek komplikuotas informacijos klasifikavimas, anksčiau buvo keturios kategorijos, įsigaliojęs įstatymas numato kiek kitokią klasifikaciją“.	Ekspertas Nr. 6
	„Asmens duomenų apsaugai taikomi specializuoti reikalavimai. Galėtų būti ieškoma bendrumų tarp šių kategorijų ir tik esant išskirtiems ypatumams taikomi specializuoti reikalavimai“.	Ekspertas Nr. 6

Tema	Citata	Eksperto Nr.
Informacijos saugumo valdymo organizavimas, kompetencijos ir atsakomybės	„Tarpinstitucinę koordinacinę funkciją Lietuvoje vykdo <...> koordinavimo komisija“.	Ekspertas Nr. 1
	„<...> koordinatore paskirta Vidaus reikalų ministerija“.	Ekspertas Nr. 1
	„<...> atsakomybe dalinasi visa eilė institucijų“.	Ekspertas Nr. 1
	„<...> trūksta resursų saugos funkcijoms vykdyti <...> trūksta tiek etatų, tiek kompetencijos, tiek ir finansų“.	Ekspertas Nr. 1
	„Lietuvoje vėliausia susirūpinta kritinės infrastruktūros saugumo funkcijomis“.	Ekspertas Nr. 1
	„Privalumas būtų veikianti idėjų generavimo, konsultacinė struktūra“ .	Ekspertas Nr. 1
	„<...> būtų galima pasimokyti iš Estijos, kurioje labai sėkmingai veikia savanoriška organizacija – Saugumo lyga, pavyzdžio“.	Ekspertas Nr. 1
	„<...> šiuo pavyzdžiu ketina sekti ir kaimynai latviai, susidomėjimą išreiškė ir kitos šalys“.	Ekspertas Nr. 1
	„<...> koordinavimo klausimai deleguoti tarpinstitucinei komisijai, konsultavimo klausimai – konsultacinei tarybai, deja, šiuo metu ji dar nesudaryta“.	Ekspertas Nr. 2
	„Galima pastebėti tiek verslo, tiek ir akademinio sluoksnių pageidavimus dalyvauti platesnio pobūdžio konsultaciniame procese“.	Ekspertas Nr. 2
	„Formaliai institucijoms išdalintos atsakomybės sritys“.	Ekspertas Nr. 2
	„<...> pastebima gana aiški valstybiniam sektoriui būdinga tendencija – kompetentingų specialistų, finansų ir kitų resursų trūkumas. Dažnai saugos prioritetai pasimeta tarp kitų institucijų funkcijų“.	Ekspertas Nr. 2
	„<...> kritinės infrastruktūros klausimai nėra tinkamai sprendžiami – neturime ne tik vienareikšmiškai atsakingos institucijos, bet net ir šios infrastruktūros apibrėžimo“.	Ekspertas Nr. 2
	„Bendra tendencija – kompetencijos trūkumas ir žmonių stoka. Su esamu etatų skaičiumi iš atsakingų institucijų sunku tikėtis proveržio ar didelių darbų. Jau kurį laiką galima stebėti lėtą reikalingų teisės aktų rengimą, užtrunkantį nuostatų ir kitų saugos dokumentų derinimą.“	Ekspertas Nr. 3
	„Galima tikėtis, komisija pradės koordinuoti darbus“.	Ekspertas Nr. 4
	„<...> koordinatorių daug, o realius darbus dirbti nėra kam“.	Ekspertas Nr. 4
	„<...> po kelis žmones institucijose, ypač vertinant biurokratinio darbo mastus, tikrai negali nuveikti didelių darbų“.	Ekspertas Nr. 4
	„Su šia valdžia iki naujų rinkimų mažai tikėtinas koks nors proveržis“.	Ekspertas Nr. 4
	„Saugumo valdymo organizavimas tikrai neblogas formaliąja prasme“.	Ekspertas Nr. 5

Tema	Citata	Eksperto Nr.
	„<...>paskutiniu metu atsakingų institucijų, gal išskyrus Ryšių reguliavimo tarnybą, kompetencija saugos srityje pastebimai sumenko“.	Ekspertas Nr. 5
	„Vidaus reikalų ministerija, turėjusi dedikuotus padalinius saugos problemoms koordinuoti ir spręsti, krizės metu visai išbarstė kompetenciją“	Ekspertas Nr. 5
	„<...> saugos atsakomybės išdalintos po truputį daugelyje institucijų“.	Ekspertas Nr. 5
	„<...> kolegialią instituciją galėtų pastiprinti viešojo ir privataus sektorių bendradarbiavimo pagrindu veikiantis kompetencijos centras, kuris galėtų jungti ir akademinio sluoksnio specialistus“.	Ekspertas Nr. 5
	„<...> daugiau tvarkos padėtų įnešti ir Valstybės kontrolės aktyvesnė veikla analizuojant saugos įgyvendinimą institucijose“.	Ekspertas Nr. 5
	„Institucijų kompetencijos gana aiškios“.	Ekspertas Nr. 6
	„<...> neatsakytų klausimų išlieka dėl kritinės infrastruktūros identifikavimo ir apsaugos“.	Ekspertas Nr. 6
	„<...> išsiskiria institucijų nuomonės dėl tolesnio (platesnio) informacijos saugumo reglamentavimo <...> specialiu saugos įstatymu“.	Ekspertas Nr. 6
	„<...> galima modernizuoti saugumo reglamentavimą esamo <...> įstatymo bazėje“.	Ekspertas Nr. 6
	„<...> galėtų būti pasisemta patirties, kaip tokie dariniai veikia užsienio šalyse, ir išnaudota galimybė pasitelkti akademinį bei privatų sektorius“.	Ekspertas Nr. 6
	„Geri papildomos kompetencijos pritraukimo pavyzdžiai – kai kurių ministerijų bendradarbiavimas su universitetais. Ar dalyvavimas tarptautinių organizacijų veikloje.“.	Ekspertas Nr. 6
	„<...> buriasi kompetencijų centrai bendradarbiaujant didžiosioms savivaldybėms su universitetais ir pan.“.	Ekspertas Nr. 6
Informacijos saugumo brandos vertinimo kriterijai ir poreikis. Institucijų situacija	„<...> numatytas brandos stebėjimas, tačiau kol kas nėra bendros metodikos brandai vertinti, nebuvo vykdyti platūs tyrimai“.	Ekspertas Nr. 1
	„<...> metodika galėtų remtis COBIT, ITIL ar kitos tarptautinės metodikos principais)“.	Ekspertas Nr. 1
	„Iš pavienių tyrimų galima numanyti, kad maždaug du trečdaliai Lietuvos institucijų atitinka maždaug pirmą, trečdalis antrą brandos lygį (iš penkių), galbūt su labai retomis išimtimis“.	Ekspertas Nr. 1
	„<...> galėtų būti siejamas su institucijų valdomų informacinių išteklių svarba (kategorija). Kuo svarbesnius išteklius valdo institucija, tuo aukštesnio brandos lygio ji turėtų siekti“.	Ekspertas Nr. 1
	„<...> institucijų branda yra labai įvairi, tikrai yra institucijų, smarkiai pažengusių, tačiau kas darosi, pavyzdžiui, savivaldybių lygmenyje, labai sunku pasakyti“.	Ekspertas Nr. 2
	„Tyrimai šiame kontekste nedaryti ir tikrai būtų aktualūs“.	Ekspertas Nr. 2

Tema	Citata	Eksperto Nr.
	„Institucijų branda ir saugumo reikšmės supratimas tikrai įvairus“.	Ekspertas Nr. 3
	„<...> jau dabar atitinka saugumo valdymo standartus“.	Ekspertas Nr. 3
	„Institucijos paliktos savieigai, stipresnės juda, silpnesnės – labai sunkiai“.	Ekspertas Nr. 4
	„Vertinimai labiau proginės veiklos nei sistema“.	Ekspertas Nr. 4
	„Net ir didelės institucijos, investavusios ženklias sumas į sistemas ir saugą, nesugeba išvengti incidentų. Taip neturėtų būti“.	Ekspertas Nr. 4
	„Neteko girdėti apie platesnius brandos vertinimus“.	Ekspertas Nr. 5
	„<...> galima numanyti „mažąsias“ institucijas esant nuliniame ar pirmajame lygyje“.	Ekspertas Nr. 5
	„Tikrai vertėtų sukurti brandos vertinimo sistemą valstybės institucijoms, kad ir COBIT ar panašios metodikos pagrindu“.	Ekspertas Nr. 5
	„<...> nėra aiški institucijų brandos būklė, nors pastebima, kad institucijos pradeda po truputį suprasti pridėtinę jos vertę“.	Ekspertas Nr. 6
	„Brandos lygiai turėtų sietis ir su taikymo apimtimi, nebūtina taikyti visų saugumo priemonių, išdėstytų standartuose, šimtu procentų“.	Ekspertas Nr. 6
	„<...> tiesioginis standartų įgyvendinimas sietinas ir su nemažu lėšų poreikiu“.	Ekspertas Nr. 6
Informacijos saugumo funkcijų centralizavimo poreikis ir apimtys	„Funkcijos galėtų būti centralizuojamos įvairiais lygmenimis, pavyzdžiui, „vyriausybės debesis“ (*angl. Government Cloud*), kolektyvinės ryšių gynybos sistemos ar kitos infrastruktūrinės priemonės“.	Ekspertas Nr. 1
	„<...> rengiamos vienodos metodikos, daromos rizikos analizės ar intervenciniai auditai“.	Ekspertas Nr. 1
	„Tai leistų taupyti finansinius išteklius, lengviau palyginti institucijų situaciją“.	Ekspertas Nr. 1
	„<...> brandžios institucijos galbūt gali „savimi pasirūpinti“, tačiau mažiau brandžioms tikrai praverstų centralizuota pagalba – kompetencijos kėlimo, audito, rizikos analizės klausimais“.	Ekspertas Nr. 2
	„<...> net ir brandžioms institucijoms vertinga gali būti išorės audito nuomonė „iš šalies“.	Ekspertas Nr. 2
	„Verta būtų svarstyti <...> finansinių resursų paieškos klausimų centralizuotą paskyrimą kokiai nors institucijai“.	Ekspertas Nr. 2
	„Galėtų būti centralizuojamos funkcijos apimant valdomas sistemas pagal veiklos sritis. Ministerijos galėtų centralizuotai vykdyti mokymus, saugos vertinimą, tipinių teisės aktų rengimą visoms savo pavaldžioms institucijoms“.	Ekspertas Nr. 3
	„<...> būtų sveikintinas dalykas – infrastruktūros centralizavimas <...> institucijoms tai leistų mažiau rūpintis su tiesiogine veikla nesusijusiomis funkcijomis, lengviau atitikti iškeltus saugos reikalavimus“.	Ekspertas Nr. 3

Tema	Citata	Eksperto Nr.
	„Centralizuoti funkcijas tikrai yra poreikis“.	Ekspertas Nr. 4
	„Esant tokiai kompetencijos situacijai valstybės sektoriuje, tikrai reikia galvoti apie kompetencijų centrus, institucijos nesugebės kiekviena sau išlaikyti profesionalių specialistų“.	Ekspertas Nr. 4
	„Kompetencijos centrai galėtų būti ir pagal funkcines sritis“.	Ekspertas Nr. 4
	„Centralizavimas tikrai praverstų techninės infrastruktūros lygmenyje“.	Ekspertas Nr. 5
	„<...> svarbus veiksnys – stipri koordinuojanti institucija, turinti pakankamai kompetencijos koordinuoti darbus, organizuoti centralizuotus saugos vertinimus, auditus, rizikos analizes, metodinius dokumentus, mokymus ir pan.“.	Ekspertas Nr. 5
	„Valstybė turėtų aiškiai suinventorizuoti turimą turtą ir tada būtų galima spręsti dėl valstybės institucijų valdomos infrastruktūros konsolidavimo, centralizuoto naudojimo“.	Ekspertas Nr. 6
	„<...> nebekurti dar kartą esamų funkcionalumų“.	Ekspertas Nr. 6
	„<...> funkcijų centralizavimo sritis galėtų būti mokymų vykdymas ar bent organizavimas; informacijos saugumo kompetencijos trūkumas ir konsultacijų poreikis pastebimas visuose lygiuose“.	Ekspertas Nr. 6
	„Galėtų būti svarstomas centralizuotas rizikos analizės ir vertinimo, saugos ir valdymo audito vykdymas. Labai naudinga būtų vienoda metodika ir palyginami kriterijai“.	Ekspertas Nr. 6
	„<...> galėtų būti apibrėžti taikytini informacijos saugumo sertifikatai auditoriams ir institucijoms, išorinio audito tvarka, galbūt jis irgi galėtų būti vykdomas (užsakomas) centralizuotai“.	Ekspertas Nr. 6
Informacijos saugumo stebėsenos ir kontrolės sistemos kūrimas ir vertinimo kriterijai	„Tokia sistema leistų stebėti institucijų atitiktį saugos reikalavimams, dokumentų savalaikį parengimą ir atnaujinimą“.	Ekspertas Nr. 1
	„Galėtų būti stebimas ir organizacijų brandos lygis ir jo kitimas“.	Ekspertas Nr. 1
	„<...> egzistuoja rimta automatizuota incidentų ir anomalijų tinkluose stebėsenos sistema“.	Ekspertas Nr. 2
	„Stebėsenos <...> priemonių <...> trūksta“.	Ekspertas Nr. 2
	„Su esama kompetencija ir resursais sunkiai tikėtina reikšminga stebėsena ir kontrolė“.	Ekspertas Nr. 3
	„<...> tokios sistemos poreikis yra“.	Ekspertas Nr. 4
	„Tokia sistema turėtų būti esminis koordinuojančios institucijos darbo įrankis“.	Ekspertas Nr. 5
	„<...> įrankis galėtų padėti apibrėžti ir stebėti tą pačią institucijų brandą, atitiktį teisės aktuose įtvirtintiems reikalavimams, auditų, rizikos analizių rezultatus, spręsti apie institucijų kompetenciją ir pagalbos joms poreikį“.	Ekspertas Nr. 6

10 Priedas. KIEKYBINIO TYRIMO ANKETA

Informacijos saugumo Lietuvos valstybės institucijose tyrimo

ANKETA

Šio tyrimo tikslas – įvertinti esamą situaciją Lietuvos valstybės institucijose valdant informacijos saugumą. Tyrimas padės identifikuoti valstybės institucijų valdomus informacijos išteklius, informacijos saugumo prioritetus, taikomus informacijos saugumo valdymo įrankius bei iššūkius, su kuriais susiduria valstybės institucijos.

Tyrimo rezultatai bus naudojami Lietuvos Respublikos vidaus reikalų ministerijos vykdant pavestas funkcijas, apibendrinti duomenys – Vilniaus Universiteto Komunikacijos moksliniame tyrime.

Anketa pildoma viena visai organizacijai. Anketos priedas (Valstybės informacinio ištekliaus kortelė) pildomas kiekvienam organizacijos valdomam ištekliui atskirai.

Dėkojame už skirtą laiką.

1. Apie organizaciją

1.1. Jūsų institucijos ar įstaigos (toliau – organizacija) pilnas pavadinimas:

Įrašykite

1.2. Kiek darbuotojų dirba Jūsų organizacijoje?

Iki 50 ☐ 50-100 ☐ 100-200 ☐ Per 200 ☐

Pažymėkite tinkamą variantą

1.3. Jūsų organizacijoje už informacinių technologijų (IT) priežiūrą atsakingas:

Dedikuotas darbuotojas (-ai)	☐			
Specialus organizacijos padalinys, *kuriame dirba*	Iki 10 ☐	10-50 ☐	50-100 ☐	per 100 ☐
Išorinis pavaldumo ryšiais susijęs padalinys, *kuriame dirba*	Iki 10 ☐	10-50 ☐	50-100 ☐	per 100 ☐
Pasamdyta bendrovė (-ės)	☐			
Kita (įrašyti)				

Pažymėkite (įrašykite) visus tinkamus variantus

1.4. Jūsų organizacijoje už informacijos saugumą atsakingas:

Dedikuotas informacijos saugumo darbuotojas (-ai)	☐			
Už IT priežiūrą atsakingas padalinys	☐			
Specialus organizacijos informacijos saugumo padalinys, kuriame dirba	Iki 5 ☐	5-10 ☐	10-50 ☐	per 50 ☐
Išorinis pavaldumo ryšiais susijęs padalinys, kuriame dirba	Iki 5 ☐	5-10 ☐	10-50 ☐	per 50 ☐
Kita (įrašyti)				

Pažymėkite (įrašykite) visus tinkamus variantus

2. Valdomi valstybės informaciniai ištekliai

2.1. Kokius valstybės informacinius išteklius valdo Jūsų organizacija?

Išteklių rūšis	Išteklių skaičius
Valstybės registrą (-us)	
Žinybinį registrą (-us)	
Valstybės informacinę sistemą (-as)	
Vidaus administravimo informacinę sistemą (-as)	
Kita (įrašyti)	

Įrašykite valdomų išteklių skaičių

3. Informacijos saugumo valdymas

3.1. Kokie informacijos saugumo tikslai (prioritetai) aktualūs Jūsų organizacijai?

Prioritetai	Neaktualu				Labai aktualu
Informacijos konfidencialumas *(informacija turi būti prieinama tik tiems, kas turi tokią teisę)*	1	2	3	4	5
Informacijos vientisumas *(informacija turi būti autentiška, apsaugota nuo tyčinio ar netyčinio nesankcionuoto pakeitimo)*	1	2	3	4	5
Informacijos prieinamumas *(informacija turi būti pasiekiama, kai jos reikia)*	1	2	3	4	5

Apibraukite (paryškinkite) kiekvieno prioriteto aktualumą

3.2. Jūsų organizacija informacijos saugumui užtikrinti taiko (visos organizacijos mastu):

Bendruosius elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimus (Patvirtinti LR Vyriausybės)	
Informacijos saugumo valdymo ISO 27000 šeimos standartus	
Informacinių technologijų metodiką ITIL	
Informacinių technologijų metodiką COBIT	
Kita (įrašyti)	

Pažymėkite (įrašykite) visas taikomas priemones

3.3. Organizacijos saugos įgaliotinis

Ar Jūsų organizacija turi oficialiai paskirtą saugos įgaliotinį? Taip ☐ Ne ☐

Pažymėkite vieną tinkamą variantą, jei atsakymas „Ne“, eiti prie 3.4. klausimo

Ar saugos įgaliotinis tiesiogiai pavaldus organizacijos vadovui? Taip ☐ Ne ☐

Pažymėkite vieną tinkamą variantą

Organizacijos saugos įgaliotinis yra (jei paskirti keli, koordinuojantis):

Specializuoto (informacijos) saugumo padalinio	Vadovas ☐	Darbuotojas ☐
Vidaus audito padalinio	Vadovas ☐	Darbuotojas ☐
IT padalinio	Vadovas ☐	Darbuotojas ☐
Kita (įrašyti)		

Pažymėkite ar įrašykite vieną tinkamą variantą

3.4. Ar Jūsų organizacijoje vykdoma rizikų analizė (visos organizacijos mastu)?

Rizikos analizę atliko organizacijos darbuotojai:

Pastaraisiais metais ☐ Prieš 2–3 metus ☐ Seniau nei prieš 3 metus ☐ Niekada ☐

Rizikos analizę atliko išorinės organizacijos:

Pastaraisiais metais ☐ Prieš 2–3 metus ☐ Seniau nei prieš 3 metus ☐ Niekada ☐

Ar buvo parengtas nustatytų rizikų valdymo planas?

Taip ☐ Ne ☐

Pažymėkite visus tinkamus variantus (pvz.: jei rizikų analizė daroma kasmet, visus 3 pirmus langelius ir pan.)

3.5. Ar jūsų organizacijoje vykdomas informacijos saugumo auditas (visos organizacijos mastu)?

Informacijos saugumo auditą atliko organizacijos darbuotojai:

Pastaraisiais metais ☐ Prieš 2–3 metus ☐ Seniau nei prieš 3 metus ☐ Niekada ☐

Informacijos saugumo auditą atliko išorinės organizacijos:

Pastaraisiais metais ☐ Prieš 2–3 metus ☐ Seniau nei prieš 3 metus ☐ Niekada ☐

Ar buvo pateiktos audito rezultatais pagrįstos rekomendacijos?

Taip ☐ Ne ☐

Ar buvo parengtas audito metu pastebėtų trūkumų šalinimo planas?

Taip ☐ Ne ☐

Pažymėkite visus tinkamus variantus (pvz.: jei auditas daromas kasmet, visus 3 pirmus langelius ir pan.)

3.6. Ar Jūsų organizacijoje vykdomi imitaciniai įsilaužimų testavimai?

Imitacinius įsilaužimų testus vykdo organizacijos darbuotojai:

Dažniau nei kartą per metus ☐ Kasmet ☐ Rečiau nei kartą per metus ☐ Niekada ☐

Imitacinius įsilaužimų testus vykdo išorinės organizacijos:

Dažniau nei kartą per metus ☐ Kasmet ☐ Rečiau nei kartą per metus ☐ Niekada ☐

Pažymėkite visus tinkamus variantus

3.7. Ar Jūsų organizacija turi formalizuotą informacijos saugumo strategijos dokumentą?

Turi, atitinkantį realią situaciją ☐ Turi, bet neatitinkantį realios situacijos ☐ Neturi ☐

Pažymėkite vieną tinkamą variantą

3.8. Ar Jūsų organizacija yra atlikusi kibernetinių grėsmių analizę?

Taip, atliko organizacijos darbuotojai ☐ Taip, atliko išorės organizacija ☐ Neatliko ☐

Pažymėkite vieną tinkamą variantą

3.9. Ar Jūsų institucijoje vyksta specializuoti informacijos saugumo mokymai:

Organizacijos vadovams:

Dažniau nei kartą per metus ☐ Kasmet ☐ Rečiau nei kartą per metus ☐ Niekada ☐

Visiems organizacijos darbuotojams:

Dažniau nei kartą per metus ☐ Kasmet ☐ Rečiau nei kartą per metus ☐ Niekada ☐

IT personalui:

Dažniau nei kartą per metus ☐ Kasmet ☐ Rečiau nei kartą per metus ☐ Niekada ☐

Informacijos saugumo personalui:

Dažniau nei kartą per metus ☐ Kasmet ☐ Rečiau nei kartą per metus ☐ Niekada ☐

Pažymėkite visus tinkamus variantus

3.10. Su kokiais iššūkiais susiduria Jūsų organizacija, užtikrindama informacijos saugumą:

Iššūkis	Nesutinku				Sutinku
Informacijos saugumas organizacijai nėra prioritetas	1	2	3	4	5
Organizacijos darbuotojams trūksta kompiuterinio raštingumo žinių	1	2	3	4	5
Organizacijos darbuotojams trūksta informacijos saugumo žinių	1	2	3	4	5
Trūksta informacijos saugumo darbuotojų	1	2	3	4	5
Informacijos saugumo darbuotojai dažna keičiasi	1	2	3	4	5
Per daug sudėtingi informacijos saugumo reikalavimai	1	2	3	4	5
Trūksta centralizuoto vadovavimo ir veiksmų koordinavimo	1	2	3	4	5
Trūksta lėšų informacijos saugumo priemonėms įsigyti	1	2	3	4	5
Kita (įrašyti)					

Apibraukite (paryškinkite) kiekvieno iššūkio aktualumą

3.11. Pagrindinės saugumo problemos, su kuriomis susiduria Jūsų organizacija:

Problema	Neaktualu				Labai aktualu
Virusai	1	2	3	4	5
Šnipinėjančios programos	1	2	3	4	5
Įsilaužimai į sistemas	1	2	3	4	5
Konfidencialios informacijos nutekėjimas	1	2	3	4	5
Duomenų praradimas (sunaikinimas, sugadinimas)	1	2	3	4	5
Neveikiančios (nepasiekiamos) sistemos	1	2	3	4	5
Techninės įrangos gedimai	1	2	3	4	5
Elektros tiekimo trikdžiai	1	2	3	4	5
Kita (įrašyti)					

Apibraukite (paryškinkite) problemos aktualumą

3.12. Jūsų nuomone, šios funkcijos turėtų būti organizuojamos:

Funkcija	Centralizuotai	Organizacijos
Informacijos saugumo dokumentų rengimas		
Organizacijos vadovų informacijos saugumo mokymai		
Organizacijos darbuotojų informacijos saugumo mokymai		
IT personalo informacijos saugumo mokymai		
Informacijos saugumo auditas		
Rizikos analizė		
Imitacinis įsilaužimų testavimas		
Informacijos saugumo techninės ir programinės įrangos įsigijimas		
Įspėjimai apie aktualias grėsmes		
Saugumo priemonių taikymas (pvz., tinklo apsaugos, įsilaužimų)		
Konsultacijos informacijos saugumo klausimais		
Kita:		

Pažymėkite (įrašykite) nuomonę apie funkcijas; funkcijos gali būti vykdomos ir centralizuotai, ir organizacijos

Anketą užpildė:

Vardas Pavardė	*Telefono numeris*	*El. pašto adresas*

VALSTYBĖS INFORMACINIO IŠTEKLIAUS KORTELĖ

Ši kortelė pildoma atskirai kiekvienam organizacijos valdomam valstybės informaciniam ištekliui.

Jūsų institucijos ar įstaigos (toliau – organizacija) pilnas pavadinimas:

Įrašykite

1. Apie Valstybės informacinį išteklių

1.1. Jūsų organizacijos valdomo Valstybės informacinio ištekliaus pavadinimas:

Įrašykite

1.2. Šis Valstybės informacinis išteklius yra:

Valstybės registras ☐ Žinybinis registras ☐

Valstybės informacinė sistema ☐ Vidaus administravimo informacinė sistema ☐

Kita (įrašyti)	

Pažymėkite (įrašykite) vieną tinkamą variantą

1.3. Šio Valstybės informacinio ištekliaus kategorija yra:

1	2	3	4	Nepriskirta

Pažymėkite (paryškinkite) tinkamą variantą

1.5. Ar patvirtinti šio Valstybės informacinio ištekliaus nuostatai? Taip ☐ Ne ☐

Kita (įrašyti)	

Pažymėkite (įrašykite) tinkamą variantą

1.6. Ar šiam Valstybės informaciniam ištekliui taikoma (atlikta):

Rizikos analizė ☐ Vidinis informacijos saugumo auditas ☐ Išorinis informacijos saugumo auditas ☐

ISO 27000 ☐ ITIL ☐ COBIT ☐

Kita (įrašyti)	

Pažymėkite (įrašykite) tinkamą variantą

2. Valstybės informacinio ištekliaus saugos dokumentai

2.1. Ar šis išteklius turi pavirtintus duomenų saugos nuostatus?

Taip ☐ Taikomi bendri organizacijos saugos nuostatai ☐ Ne ☐

Jei atsakymas „Ne“, eiti prie 2.2. klausimo

Ar duomenų saugos nuostatai peržiūrimi kartą per metus? Taip ☐ Ne ☐

Ar duomenų saugos nuostatai buvo keisti per pastaruosius 2 metus? Taip ☐ Ne ☐

Pažymėkite tinkamus variantus

2.2. Ar šis išteklius turi pavirtintas Saugaus elektroninės informacijos tvarkymo taisykles?

Taip ☐ Taikomos bendros organizacijos taisyklės ☐ Ne ☐

Jei atsakymas „Ne“, eiti prie 2.3. klausimo

Ar taisyklės buvo keistos per pastaruosius 2 metus? Taip ☐ Ne ☐

Pažymėkite tinkamus variantus

2.3. Ar šis išteklius turi pavirtintą IS veiklos tęstinumo planą?

Taip ☐ Taikomas bendras organizacijos planas ☐ Ne ☐

Jei atsakymas „Ne“, eiti prie 2.4. klausimo

Ar planas buvo keistas per pastaruosius 2 metus? Taip ☐ Ne ☐

Ar planas buvo išbandytas? Taip ☐ Ne ☐

Pažymėkite tinkamus variantus

2.4. Ar šis išteklius turi pavirtintas IS naudotojų administravimo taisykles?

Taip ☐ Taikomos bendros organizacijos taisyklės ☐ Ne ☐

Jei atsakymas „Ne“, baigti pildyti anketą

Ar taisyklės buvo keistos per pastaruosius 2 metus? Taip ☐ Ne ☐

Pažymėkite tinkamus variantus

Anketą užpildė:

Vardas Pavardė	*Telefono numeris*	*El. pašto adresas*

11 Priedas. LIETUVOS VALSTYBĖS INSTITUCIJŲ SĄRAŠAS

1. Seimo kanceliarija
2. Prezidento kanceliarija
3. Ministro Pirmininko tarnyba
4. Aplinkos ministerija
5. Energetikos ministerija
6. Finansų ministerija
7. Krašto apsaugos ministerija
8. Kultūros ministerija
9. Socialinės apsaugos ir darbo ministerija
10. Susisiekimo ministerija
11. Sveikatos apsaugos ministerija
12. Švietimo ir mokslo ministerija
13. Teisingumo ministerija
14. Užsienio reikalų ministerija
15. Ūkio ministerija
16. Vidaus reikalų ministerija
17. Žemės ūkio ministerija
18. Lietuvos vyriausiojo archyvaro tarnyba
19. Kūno kultūros ir sporto departamentas prie LRV
20. Narkotikų, tabako ir alkoholio kontrolės departamentas prie LRV
21. Statistikos departamentas prie LRV
22. Valstybinė atominės energetikos saugos inspekcija
23. Valstybinė maisto ir veterinarijos tarnyba
24. Ryšių reguliavimo tarnyba
25. Valstybės kontrolė
26. Seimo kontrolierių įstaiga
27. Specialiųjų tyrimų tarnyba
28. Lietuvos standartizacijos departamentas prie AM
29. Lietuvos geologijos tarnyba prie AM
30. Nacionalinis akreditacijos biuras prie AM
31. Valstybinė mokesčių inspekcija prie FM
32. Muitinės departamentas prie FM
33. Valstybės dokumentų technologinės apsaugos tarnyba prie FM
34. Kultūros paveldo departamentas prie KM
35. Socialinių paslaugų priežiūros departamentas prie SADM
36. Valstybinio socialinio draudimo fondo valdyba prie SADM
37. Neįgalumo ir darbingumo nustatymo tarnyba prie SADM
38. Lietuvos darbo birža prie SADM
39. LR Valstybinė darbo inspekcija
40. Valstybinė kelių transporto inspekcija prie SM
41. Valstybinė geležinkelio inspekcija prie SM
42. Informacinės visuomenės plėtros komitetas prie SM
43. Lietuvos automobilių kelių direkcija prie SM
44. Valstybinė ligonių kasa prie SAM
45. Valstybinė vaistų kontrolės tarnyba prie SAM
46. Valstybinė akreditavimo sveikatos priežiūros veiklai tarnyba prie SAM
47. Radiacinės saugos centras
48. Registrų centras
49. Ekstremalių sveikatai situacijų centras
50. Centrinė hipotekos įstaiga
51. Kalėjimų departamentas prie LR teisingumo ministerijos
52. Valstybinė duomenų apsaugos inspekcija
53. Įmonių bankroto valdymo departamentas prie ŪM
54. Valstybinis turizmo departamentas prie ŪM
55. Valstybinė ne maisto produktų inspekcija prie ŪM
56. Viešųjų pirkimų tarnyba
57. Lošimų priežiūros tarnyba prie FM
58. Valstybinė metrologijos tarnyba
59. Lietuvos metrologijos inspekcija
60. Valstybinė teritorijų planavimo ir statybos inspekcija prie AM
61. Asmens dokumentų išrašymo centras prie VRM
62. Finansinių nusikaltimų tyrimo tarnyba prie VRM
63. Gyventojų registro tarnyba prie VRM
64. Policijos departamentas prie VRM
65. Informatikos ir ryšių departamentas prie VRM
66. Migracijos departamentas prie VRM
67. Priešgaisrinės apsaugos ir gelbėjimo departamentas prie VRM
68. Vadovybės apsaugos departamentas prie VRM
69. Valstybės sienos apsaugos tarnyba
70. Valstybės tarnybos departamentas prie VRM
71. Valstybinis studijų fondas
72. Transporto investicijų direkcija
73. Civilinės aviacijos administracija
74. Pasienio kontrolės punktų direkcija prie SM
75. Ginklų fondas prie VRM
76. Nacionalinė žemės tarnyba prie ŽŪM
77. Nacionalinė mokėjimo agentūra prie ŽŪM
78. Valstybinė augalininkystės tarnyba prie ŽŪM
79. Žuvininkystės tarnyba prie ŽŪM
80. Lietuvos saugios laivybos administracija

81. Vilniaus miesto savivaldybės administracija
82. Alytaus miesto savivaldybės administracija
83. Birštono miesto savivaldybės administracija
84. Druskininkų miesto savivaldybės administracija
85. Kauno miesto savivaldybės administracija
86. Klaipėdos miesto savivaldybės administracija
87. Marijampolės miesto savivaldybės administracija
88. Neringos miesto savivaldybės administracija
89. Palangos miesto savivaldybės administracija
90. Panevėžio miesto savivaldybės administracija
91. Šiaulių miesto savivaldybės administracija
92. Visagino miesto savivaldybės administracija
93. Akmenės rajono savivaldybės administracija
94. Alytaus rajono savivaldybės administracija
95. Anykščių rajono savivaldybės administracija
96. Biržų rajono savivaldybės administracija
97. Ignalinos rajono savivaldybės administracija
98. Jonavos rajono savivaldybės administracija
99. Joniškio rajono savivaldybės administracija
100. Jurbarko rajono savivaldybės administracija
101. Kaišiadorių rajono savivaldybės administracija
102. Kauno rajono savivaldybės administracija
103. Kėdainių rajono savivaldybės administracija
104. Kelmės rajono savivaldybės administracija
105. Klaipėdos rajono savivaldybės administracija
106. Kretingos rajono savivaldybės administracija
107. Kupiškio rajono savivaldybės administracija
108. Lazdijų rajono savivaldybės administracija
109. Mažeikių rajono savivaldybės administracija
110. Molėtų rajono savivaldybės administracija
111. Pakruojo rajono savivaldybės administracija
112. Panevėžio rajono savivaldybės administracija
113. Pasvalio rajono savivaldybės administracija
114. Plungės rajono savivaldybės administracija
115. Prienų rajono savivaldybės administracija
116. Radviliškio rajono savivaldybės administracija
117. Raseinių rajono savivaldybės administracija
118. Rokiškio rajono savivaldybės administracija
119. Skuodo rajono savivaldybės administracija
120. Šakių rajono savivaldybės administracija
121. Šalčininkų rajono savivaldybės administracija
122. Šiaulių rajono savivaldybės administracija
123. Šilalės rajono savivaldybės administracija
124. Šilutės rajono savivaldybės administracija
125. Širvintų rajono savivaldybės administracija
126. Švenčionių rajono savivaldybės administracija
127. Tauragės rajono savivaldybės administracija
128. Telšių rajono savivaldybės administracija
129. Trakų rajono savivaldybės administracija
130. Ukmergės rajono savivaldybės administracija
131. Utenos rajono savivaldybės administracija
132. Varėnos rajono savivaldybės administracija
133. Vilkaviškio rajono savivaldybės administracija
134. Vilniaus rajono savivaldybės administracija
135. Zarasų rajono savivaldybės administracija
136. Elektrėnų savivaldybės administracija
137. Kalvarijos savivaldybės administracija
138. Kazlų Rūdos savivaldybės administracija
139. Pagėgių savivaldybės administracija
140. Rietavo savivaldybės administracija