INFORMACIJOS VADYBA

Informacijos saugumo valdymas Lietuvos viešajame sektoriuje

Saulius Jastiuginas
Vilniaus universiteto Komunikacijos fakulteto
Informacijos ir komunikacijos katedros doktorantas
Departament of Information and Communication,
Faculty of Communication, Vilnius University,
Doctoral student
Saulėtekio al. 9, LT-10222 Vilnius
Tel. (8 5) 236 61 19, faks. (8 5) 236 61 04
El. paštas: *saulius.jastiuginas@kf.vu.lt*

Informacijos saugumas tampa vis aktualesnis šiuolaikinėje visuomenėje. Dažniausiai informacijos saugumo problematika išryškėja įvykus informacijos saugumo incidentams ar pažeidimams, todėl suprantama, kad visame pasaulyje augantis informacijos saugumo pažeidimų skaičius ir dėl jų patiriamų nuostolių mastai įvardijami kaip vienas iš pagrindinių informacijos saugumo problemų egzistavimo rodiklių. Vertinant nuolatinį šių problemų pobūdį, galima daryti prielaidą, kad trūksta sisteminio požiūrio į informacijos saugumo valdymą. Užsienio šalių mokslininkai informacijos saugumo valdymo problematiką nagrinėja įvairiais strateginio, žmogiškojo veiksnio bei technologinio požiūrio aspektais; išskiriamas problematikos specifiškumas organizacijų, valstybės bei tarptautiniu lygmeniu, tačiau Lietuvoje informacijos saugumo valdymo mokslinis ištirtumas tebėra menkas. Siekiant išryškinti informacijos saugumo valdymo formavimosi Lietuvoje ypatumus tarptautiniame kontekste, straipsnyje teorinės užsienio ir Lietuvos mokslininkų informacijos saugumo valdymo paradigmos jungiamos į sisteminę informacijos saugumo valdymo koncepciją, o atliktas tyrimas leido įvertinti Lietuvos viešojo sektoriaus informacijos saugumo valdymo būklę ir suformuoti tolimesnių mokslinių tyrimų prielaidas.

Pagrindiniai žodžiai: *informacijos saugumas, informacijos saugumo valdymas, informacijos saugumo valdymo koncepcija, saugumo standartai, saugumo reikalavimai, informacinės sistemos, valstybės registrai, valstybės institucijos, viešasis sektorius.*

Įvadas

Informacijos saugumo problematika sena kaip pati informacija, informacijos saugumo aktualumas išryškėjo atsiradus poreikiui saugoti, perduoti ir kitaip tvarkyti informaciją. Dar Julijaus Cezario laikais saugiam informacijos perdavimui buvo naudojami slapti kodai, kurie davė pradžią kriptologijai (Denning, 1999; Rusell, Gangemi, 1991).

Šiuolaikinis supratimas apie informacijos saugumą pradėjo formuotis atsiradus kompiuteriams ir poreikiui valdyti informaciją ir žinias antroje XX a. pusėje. Visuomenei tampant vis labiau priklausomai nuo patikimo informaciją apdorojančių

technologijų veikimo, šių jos individų, organizacijų ar net visos visuomenės gyvenimą nuolat veikia technologijų veiklos sutrikimai, pavyzdžiui, nepageidaujami laiškai, virusai, interneto svetainių sutrikimai, tapatybės pasisavinimas, slaptos informacijos nutekėjimas (pvz., Wikileaks) ar Tūkstantmečio klaidos (Y2K) sukeltas ažiotažas visame pasaulyje (Amaral, 2007; Atkočiūnienė, 2009; Kuttschreuter, Gutteling, 2004).

Daugėjant informacijos saugumo pažeidimų (žr. iliustraciją), kyla poreikis valdyti informacijos saugumo problemas valstybių lygmeniu, tačiau kibernetinės erdvės ir interneto infrastruktūros globalus pobūdis reikalauja dar platesnio požiūrio. Pasaulinei interneto infrastruktūrai priskiriami didžiausi elektroninių ryšių paslaugų teikėjai, interneto srautų skirstymo įranga, vardų sričių saugyklos ir kita milijonus vartotojų bei milijardus užklausų aptarnaujanti įranga; šios įrangos sutrikimai ar tikslingos atakos gali smarkiai sulėtinti tarptautinių duomenų srautą, atkirsti pavienius tinklus ar jų grupes bei kitus išteklius nuo kitų vartotojų (Ryan, 2007). Tokių atakų realumą ir žalą parodė įvykiai Estijoje perkeliant „bronzinio kario skulptūrą“, kai dėl organizuoto informacinio puolimo prieš šią šalį buvo atkirstos visos valstybės galimybės susisiekti su pasauliu, gauti ar pranešti informaciją apie šalyje vykstančius procesus, paralyžuotas valstybės institucijų darbas ir galimybė tvarkyti verslo ar kasdieninio gyvenimo poreikius elektroninėje erdvėje. Šis įvykis sukėlė plačią tarptautinę diskusiją dėl tokio masto pažeidžiamumo ir kolektyvinių veiksmų tokiais atvejais būtinybės. Diskusijoje dalyvavo ir NATO bei Europos Sąjungos atitinkamos institucijos (Janeliūnas, 2007; Lorents, Rain, Rikk, 2009).

Iliustracija: Augantys informacijos saugumo pažeidimų atvejai:

- ✓ Jungtinėse Amerikos Valstijose per ketverius pastaruosius metus kompiuterinių incidentų skaičius išaugo daugiau nei 400 procentų (GAO ataskaita, 2010).
- ✓ Didžiojoje Britanijoje 92 proc. didžiųjų bendrovių praneša apie rimtus saugumo incidentus, patirtus 2009 metais (palyginimui 2008 metais – 72 proc.) ir išaugusius vidutinius didžiausio incidento atneštus nuostolius, kurie apytiksliai nuo 90–170 tūkst. svarų sterlingų išaugo iki 280–690 tūkst. svarų sterlingų (Infosecurity Europe, 2010).
- ✓ 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).

Įvertinus informacijos saugumo incidentų mastą, galima teigti, kad individų ir organizacijų netinkamas pasirengimas valdyti informacijos saugumo incidentus gali lemti visos valstybės ir net pasaulines problemas, todėl gebėjimas valdyti informacijos saugumą turi tapti strateginiu tiek organizacijų, tiek valstybių tikslu. Akivaizdu, kad tik valstybės, suvaldžiusios informacijos saugumo problematiką savo viduje, gali tinkamai prisidėti prie tarptautinio lygmens rizikos valdymo (CIO, CSO ir PwC tyrimas, 2010; Ernst & Young's 12th Annual Global Information Security Survey; NATO, 2010).

Vertinat situaciją Lietuvoje, galima pažymėti, kad nors mūsų šaliai taip pat aktualios globalios problemos – esame susidū-

rę su internetinės bankininkystės sistemų sutrikimais, registrų ir valstybės informacinių sistemų duomenų nepasiekiamumu, asmens duomenų nutekėjimu iš valstybės institucijų, plataus atgarsio sulaukė 2008 metų birželį įvykdytas įsilaužimas į privataus ryšių paslaugų tiekėjo serverius, dėl kurio nukentėjo keli šimtai privačių bendrovių ir kelių valstybės institucijų interneto svetainės, buvo sutrikdytas jų darbas (Gamulis, Kiškina, 2009; Janeliūnas, 2007; RRT, 2010; iliustracija), – tačiau atsižvelgiant į menką mokslinį informacijos saugumo valdymo ištirtumą Lietuvoje, sudėtinga argumentuotai vertinti Lietuvos pasirengimą globalioms rizikoms.

Straipsnio tikslas – tarptautinio informacijos saugumo valdymo kontekste įvertinti situaciją Lietuvos viešajame sektoriuje. 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 įspraustas į aiškius rėmus ir negali laisvai rinktis, kaip reaguoti į informacijos saugumo rizikas, todėl Lietuvos valstybės institucijų informacijos saugumas tiesiogiai priklauso nuo galiojančių informacijos saugumo valdymo reikalavimų, vadinasi, šie reikalavimai turi būti tinkamai pagrįsti.

Tikslui įgyvendinti iškelti šie uždaviniai: 1) apibrėžti informacijos saugumo valdymo turinį, kad būtų išanalizuoti tarptautiniame lygmenyje vyraujantys požiūriai į informacijos saugumo valdymą ir, juos apibendrinus, suformuluota informacijos saugumo valdymo koncepcija; 2) išskirti plačiausiai taikomas informacijos saugumo valdymo priemones, leidžiančias įgyvendinti informacijos saugumo valdymo koncepciją; 3) atsižvelgiant į tarptautines tendencijas, atlikti Lietuvos viešajam sektoriui galiojančių informacijos saugumo valdymo reikalavimų ir jų taikymo analizę.

Tyrimo metodai: mokslinės literatūros ir teisės aktų turinio analizės, informacijos sisteminimo, lyginimo ir apibendrinimo metodai, teorinis dokumentinis tyrimas.

Informacijos saugumo valdymo sąvokos ir koncepcija

Informacijos saugumo valdymo sąvokos apibrėžimą pirmiausia komplikuoja *informacijos saugumo* apibrėžtis, todėl svarbu nuosekliai aptarti *informacijos saugumo*, *informacijos saugumo valdymo,* kitas susijusias sąvokas, jų genezę bei tarpusavio ryšius, o *informacijos saugumo valdymo koncepciją* suformuluoti kaip holistinį požiūrį į informacijos saugumo valdymą.

Dauguma *informacijos saugumo* apibrėžimų remiasi Donno B. Parkerio apibrėžtais informacijos saugumo tikslais. Anot Parkerio, *informacijos saugumo* tikslas – užtikrinti informacijos *konfidencialumą*, *vientisumą* ir *prieinamumą*. *Konfidencialumas* suprantamas kaip informacijos slaptumą, t. y. informacija turi būti prieinama tik tiems, kam ji skirta; *vientisumas* apima pradinės informacijos tikrumą, patikimumą ir autentiškumą, t. y. informacija turi būti apsaugota nuo klaidingo ar nesankcionuoto pakeitimo; *prieinamumas* – užtikrinta galimybė pasinaudoti informacija, t. y. sankcionuoti vartotojai turi turėti galimybę pasiekti informaciją, kai jos jiems reikia (Parker, 1981).

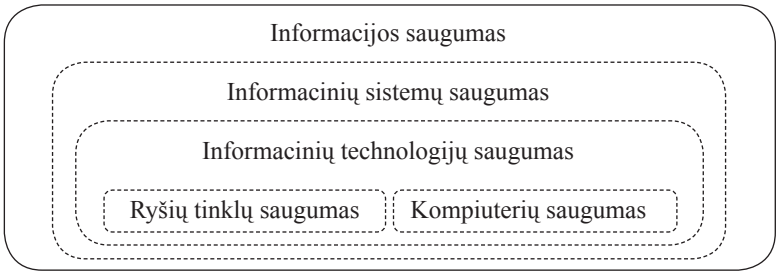
Informacijos saugumo srityje vartojami įvairūs terminai: *informacijos, duomenų, kompiuterių, ryšių tinklų, informacijos technologijų, informacinių sistemų saugumas (apsauga),* ir nors šie terminai skiriasi savo objektu ir turiniu, literatūroje dažna sinonimiška jų vartosena. Techniškiausiems ir siauriausiems terminams priskirtini *kompiuterių saugumas* ir *ryšių tinklų saugumas*, kurie apibrėžiami kaip visuma priemonių, skirtų apsaugoti informacijai, tvarkomai kompiuteryje ar perduodamai ryšių tinklais, nuo atsitiktinių ar tyčinių grėsmių. Sąvokos *informacijos technologijų saugumas* ir *informacinių sistemų saugumas* taip pat dažnai vartojamos sinonimiškai, tačiau reikėtų pasakyti, kad *informacinių technologijų saugumas* apima daugiau technologinius aspektus, o *informacinių sistemų saugumas* – dar ir žmogiškąjį veiksnį (von Solms, 2000; Trcek, 2006; Mikalauskienė, Brazaitis, 2010). Šių sąvokų sąsajos pavaizduotos 1 paveiksle.

Minėti autoriai sutaria, kad informacija yra didžiausias turtas ir svarbiausias saugumo objektas, tačiau reikėtų pažymėti, kad Lietuvoje nėra griežtai nusistovėjęs šiame kontekste anglų kalboje vartojamo termino *security* vertimas – *saugumas, sauga, apsauga.* Šiuo metu terminas *apsauga* dažniausiai pasitaiko asmens duomenų teisinės apsaugos, privatumo kontekste (Asmens duomenų..., 2008), *sauga* – valstybės registrų ir informacinių sistemų kontekste (Valstybės registrų įstatymas, 2009), *saugumas* vartojamas plačiausiai, kaip apimantis visus išvardytus aspektus, todėl *informacijos saugumo* sąvoka labiausiai tinka siekiant atskleisti įvairialypį informacijos saugumo valdymo kontekstą.

Vertinant *informacijos saugumo* sąvokos genezę, galima teigti, kad požiūris į informacijos saugumą nuo pirmųjų kompiuterių pasirodymo iki šių dienų iš esmės evoliucionavo – nuo siauro informacijos saugumo supratimo kaip tik grynai technologinės problemos iki plačios informacijos saugumo valdymo suvokties (Denning, 1999; Dlamini, Eloff, Eloff, 2009; Rusell, Gangemi, 1991).

Šiuos organizacijų lygmens pokyčius detaliai analizavo Johanesburgo universiteto profesorius Basie von Somsas, kuris savo mokslinėse publikacijose išskyrė tris *saugumo bangas*, o vėliau pristatė ir ketvirtąją bei penktąją (von Solms, 2000, 2006, 2010; 2 paveikslas).

Pirmoji banga, trukusi iki devintojo dešimtmečio, charakterizuojama kaip *technologinė banga (Technical Wave)* – informacijos saugumo užtikrinimas buvo suprantamas kaip technologijų problema, kuria rūpinosi vien techninis personalas.



1 pav. ***Informacijos saugumo srities sąvokų sąsajos***

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 atsiskaityti apie situaciją ir pažangą užtikrinant saugumą organizacijoje. Ši banga galėtų būti pavadinta *administracine banga (Management Wave);* ji truko maždaug iki dešimtojo dešimtmečio vidurio.

Trečiosios – institucinės bangos (Institutionalization Wave) formavimąsi 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 gerosios praktikos pavyzdžius ir standartus, o pripažinus žmogiškojo veiksnio įtaką saugumui, pradėtas skatinti saugumo kultūros ugdymas.

Ketvirtoji – informacijos saugumo valdymo (Information Security Governance) banga praėjo formuotis po 2000 metų. Didėjantis organizacijų poreikis vertinti ir tarpusavyje lyginti informacijos saugumo situaciją padėjo formuotis praktikai plačiau taikyti informacijos saugumo valdymo standartus (pvz., ISO 27000 standartų grupė), informacinių technologijų valdymo metodikas (pvz., Cobit, ITIL). Šie dokumentai nustato, kad organizacijos turi gebėti 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 diegimą, nuolatinį saugos kultūros skatinimą organizacijoje.

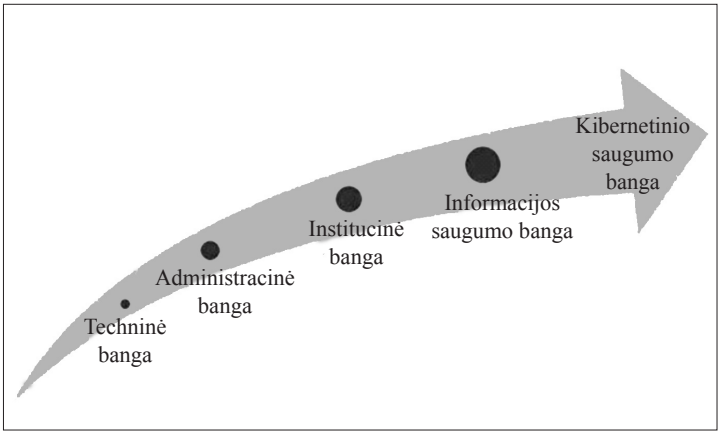
Prie glaudaus valdymo funkcijų integravimo į informacijos saugumo valdymo sąvoką daug prisidėjo informacijos saugumo valdymo reikalavimų įteisinimas atskirų šalių teisės aktais, kurie įtvirtino privalomą saugos standartais ir metodikomis grindžiamų informacijos saugumo valdymo priemonių taikymą bei nustatė asmeninę organizacijos vadovų atsakomybę, pavyzdžiui, 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 patvirtintas SOX (2002), kuris įtvirtino reikalavimus privačiam sektoriui, ir FISMA (2002), kuris apibrėžė privalomus informacijos saugumo valdymo įpareigojimus visam JAV viešajam sektoriui. Saugumo valdymo reikalavimai ilgainiui 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.

Informacijos saugumo bangų skiriamasis bruožas – jų orientacija į organizacijos vidinę veiklą ir valdomą informaciją, tačiau atsižvelgęs į tai, kad organizacijos vis labiau naudoja interneto ir kitas organizacijos tiesiogiai nekontroliuojamas viešojo tinklo technologijas, pavyzdžiui, nuotoliniam darbui, elektroninei komercijai ir kitai veiklai, Basie von Solmsas išskyrė *penktąją – kibernetinio saugumo*

(Cyber Security) bangą. Prie šios bangos susiformavimo prisidėjo ir besikeičiantis rizikos šaltinis; autoriaus teigimu, vis didesnę grėsmę pradeda kelti ne pakankamai gerai apsaugotais organizacijos ištekliais bandantys neteisėtai pasinaudoti asmenys, o paprasti, „naivūs“ vartotojai, kurie kartu yra ir organizacijų elektroninių paslaugų klientai, ar darbuotojai, kurie dirba iš įvairiausių nutolusių kompiuterių, tačiau skiria nepakankamai dėmesio savo asmeninių kompiuterių saugumui ir taip tampa grėsme organizacijų informaciniams ištekliams. Taigi kibernetinio saugumo banga pasižymi dėmesiu ir organizacijos išorinės aplinkos poveikiui (von Solms, 2010).

Informacijos saugumo valdymo sąvokos turinio pokyčius galima įžvelgti nagrinėjant mokslinę literatūrą, kurioje tyrinėjant informacijos saugumo aspektus ir jų tarpusavio sąsajumą išryškinamos pokyčių priežastys.

Analizuojant mokslines publikacijas, skirtas informacijos saugumo valdymo problematikai, galima konstatuoti, kad didžiausias yra įvairių informacijos saugumo valdymo *technologinių aspektų* ištirtumas. Technologinių aspektų tyrimai prasidėjo dar 1970 metais. Mokslininkai daug dėmesio skyrė techninės ir programinės įrangos architektūros tyrimams, kriptografinėms priemonėms, slaptažodžių, biometrijos ir kitų identifikavimo priemonių patikimumui nagrinėti, tinklų topologijos, ugniasienių ir kitoms informacijos saugumo technologijoms analizuoti (D'Archy, Hovav, 2009). Rossas Andersonas ir Tyleris Motore'as taip pat pažymi, kad iki pat 2000 metų informacijos saugumas buvo suprantamas tik kaip technologijų srities disciplina, besiremianti informatikos (*computer science*) ir matematikos mokslais bei naudojanti technologinius įrankius – kriptografiją, tinklų protokolus ir pan. Šie Kembridžo ir Harvardo universitetų mokslininkai 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 (*phishing*), atsiranda informacijos sistemų patikimumo, strateginio planavimo, investicijų valdymo ir kiti ekonominiai aspektai



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

(Anderson, Moore, 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 baigti, paliekant klaidų šalinimą būsimiems programinės įrangos patobulinimams (Anderson, 2001). Mokslininkų manymu, iš esmės pačių informacinių technologijų produktų gamintojų ekonominių veiksnių nulemti sprendimai ir per menkas dėmesys mokslininkų įžvalgoms suformavo dabartinę informacijos saugumo situaciją (Caelli, 2002).

Technologinių, ekonominių veiksnių sąsajumas su psichologiniais ir kitais žmogiškaisiais veiksniais išryškėja nagrinėjant pačių informacijos saugumo valdymo technologijų sudėtingumą. JAV Carnegie Mellon ir Kalifornijos universitetų mokslininkų, vadovaujamų Almos Whitten ir J. D. Tygaro, atlikta studija atskleidė didžiulę properšą tarp saugumo programų kūrėjų lūkesčių ir vartotojų veiksmų – ekspertų sukurtos saugumo programos, skirtos paprastiems vartotojams, yra per sudėtingos, vartotojai nesupranta šių programų galimybių ir naudojimo tikslų, klaidingai jas interpretuodami palieka saugumo spragų, o pačių programų turėjimas vartotojams suformuoja klaidingą jausmą, 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 bei pačių programų kūrėjų netikrumas dėl jų produktų saugumo (Anderson, 1994; Anderson, Moore, 2009).

Šiame kontekste svarbu pabrėžti, kad psichologiniai socialinės inžinerijos instrumentai vis labiau išnaudojami siekiant surinkti jautrią informaciją įvairioms saugumo atakoms ir kitoms nusikalstamoms veikoms. Tam prielaidas sudaro kelios priežastys: 1) žmonės dažnai yra patiklūs ir nori pritapti, o 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) informacijos saugumo ekspertų dialogas su kitais organizacijos nariais yra nepakankamas (Asch, 1952; Ashenden, 2008, Timko, 2008).

Informacijos saugumo valdymo kaip daugiadalykio tyrimų subjekto poziciją išryškina ir Kanados bei Taivano mokslininkai, kurie savo empirinėse studijose taip pat atkreipia dėmesį į tai, kad mokslinėje literatūroje plačiai diskutuojama apie *technologinius veiksnius,* tačiau pabrėžia, kad būtina vertinti organizacijos kultūros ir valdymo principų sąsajas, o efektyvus informacijos saugumo valdymas turi remtis *darniu žmogiškųjų, organizacinių ir technologinių veiksnių* koordinavimu (Chang, Lin, 2007; Parakkattu, Kunnathur, 2010; Werlinger et al, 2009).

Vertinant įvairių informacijos saugumo valdymo aspektų sąsajas svarbios Jano Eloffo ir Mariki Eloff įžvalgos; jie aptarė Demingo rato (planuok – daryk – patikrink – veik) taikymą informacijos saugumo valdymui, išskyrė informacijos saugumo valdymo sistemos kaip proceso ir kaip produkto kūrimo problematiką, akcentavo gerųjų praktikų ir standartų taikymo naudą užtikrinant informacijos saugumo valdymą. Taip pat svarbūs ir Basie von Solmso

apibendrinimai, kur jis, pristatydamas *saugumo bangas* bei pabrėždamas informacijos saugumo daugiadalykiškumą, nagrinėjo *organizacijos valdymo, saugumo politikos, gerųjų praktikų, etikos, sertifikavimo, teisinius, mokymų, vertinimo ir stebėjimo* bei kitus informacijos saugumo valdymui svarbius aspektus (J. Eloff, M. Eloff, 2003; von Solms, 2001).

Autoriui nepavyko aptikti informacijos saugumo valdymo problematiką nagrinėjančių šaltinių Lietuvoje, tačiau moksliniuose darbuose analizuojami aktualūs Lietuvai teisinio reglamentavimo ir reguliavimo (Čėsna, Štitilis, 2000; Štilis, Paškaukas, 2006; Paškauskas, 2007; kiti VU ir MRU mokslininkai), techniniai (Garšva, 2006; Mikučionis ir kt., 2007; Paulauskas, 2009; kiti VU, KTU, VGTU mokslininkai), komunikaciniai (Janeliūnas, 2007), mokymų (Venčkauskas, Krivickienė, Toldinas, 2009) ir kiti informacijos saugumo aspektai.

Remiantis mokslinės literatūros apžvalga, galima pritarti kai kurių autorių (Dlamini, Eloff, Eloff, 2009) išvadoms, kad informacijos saugumo valdymo kontekstas juda strateginio požiūrio kryptimi ir pasireiškia informacijos saugumo administravimo *(information security management)* virtimu informacijos saugumo valdymu *(information security governance)*.

Išanalizavus moksliniuose darbuose tirtus informacijos saugumo valdymo aspektus ir siekiant apibrėžti informacijos saugumo valdymo koncepciją, galima išskirti tris požiūrius (dimensijas):

1) strateginį – apimantį administracinius, organizacinius, valdymo, ekonominius, teisinius, gerųjų praktikų ir pan. aspektus;
2) žmogiškojo veiksnio – apimantį saugumo kultūros, etinius, kompetencijų, mokymų, psichologinius ir pan. aspektus;
3) technologinį – apimantį informacinių technologijų, techninių ir programinių priemonių, matematinius, kriptologinius ir pan. aspektus.

Apibendrinant informacijos saugumo valdymo problematiką tyrinėjusių mokslininkų įžvalgas galima teigti, kad mokslinėse diskusijose nagrinėjami įvairūs informacijos saugumo aspektai, tačiau maždaug nuo 1990 metų lygiagrečiai su siaurais atskirų *informacijos saugumo* aspektų tyrimais buvo plėtojami tarpdalykiniai tyrimai ir pradėjo formuotis *informacijos saugumo valdymo* samprata, kuri integravo strateginį, žmogiškojo veiksnio ir technologinį požiūrius (dimensijas) ir tapo plačia *informacijos saugumo valdymo koncepcija*.

Informacijos saugumo valdymo koncepcijos įgyvendinimo priemonės

Platus informacijos saugumo valdymo koncepcijos turinys inspiravo atitinkamų jos įgyvendinimo priemonių poreikį. Tarptautiniu lygmeniu formavosi reikmė nustatyti palyginamus dydžius, užtikrinti suderinamumą, apibrėžti įvertinimo ir sertifikavimo metodikas, nurodyti vieningas geriausių praktikų įgyvendinimo gaires. Šie poreikiai lėmė standartizavimo būtinybę. Taip pagrindinėmis informacijos saugumo valdymo koncepcijos įgyvendinimo priemonėmis tapo standartai, kurių šaltiniai – verslo šakų kuriamos metodikos, vyriausybių nustatomi reikalavimai bei nacionalinių ir tarptautinių standartizacijos organizacijų tvirtinami standartai (Amaral, 2007; Weise, 2009).

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[1], galima rasti per 350 standartų, susijusių su įvairiais informacijos saugumo valdymo aspektais, tačiau įvertinus jų turinio aprašymus svarbiausiais informacijos saugumo valdymo standartais galima įvardyti ISO 27000 grupės standartus. Šie standartai kilo iš britiškojo standarto BS-7799 ir pakeitė informacijos saugumo valdymo tarptautinį standartą ISO 17799. Šios grupės standartai skirti tiesiogiai informacijos saugumui valdyti, saugumo valdymo sistemai kurti, praktinėms priemonėms diegti, įvertinti ir organizacijai sertifikuoti, jie plačiausiai pripažįstami *de facto* informacijos saugumo valdymo geros praktikos pavyzdžiu (Gorge, 2009).

Valdant ir diegiant informacinių technologijų sprendimus susiklostė geros praktikos pavyzdžiai, kurie ilgainiui tapo plačiai pripažįstamomis, nuolat tobulinamomis metodikomis, o šios – informacijos saugumo valdymo koncepcijos įgyvendinimo priemonėmis. Daugiausia dėmesio sulaukė COBIT ir ITIL metodikos, kurios apima ir informacijos saugumo valdymą.

COBIT (*Control Objectives for Information and Related Technologies*)[2] – pasaulyje pripažintas metodikų rinkinys informacijos ir ryšių technologijų ūkiui valdyti, kuris remiasi rinkos standartais ir geriausia praktika. Šį metodikų rinkinį 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 procesų sutvarkymą apima ir informacijos saugumo valdymą.

ITIL (*Information Technology Infrastructure Library*)[3] – verslo valdymo metodologija, orientuota į darbo optimizavimą bei kokybės užtikrinimą informacinių ir ryšių technologijų bendrovėse ar įmonių informacinių ir ryšių technologijų padaliniuose. ITIL yra kompleksinė informacinių ir ryšių technologijų valdymo metodologija, paremta geriausios praktikos pavyzdžiais. Pagrindinis metodikos vystytojas – Didžiosios Britanijos vyriausybės prekybos rūmai (*Office of Government Commerce – OGC*).

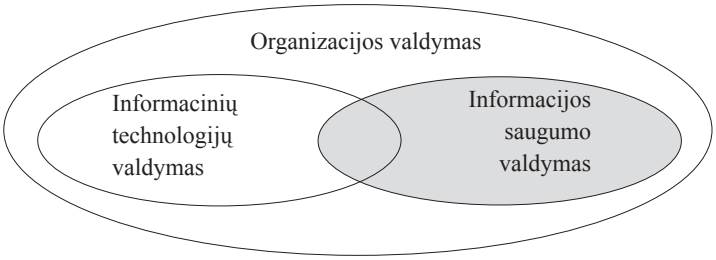
ITIL metodologija taip pat pripažinta Tarptautinės standartizacijos organizacijos standartų – ISO/IEC 20000-1:2005, ISO/IEC 20000-2:2005, ISO/IEC TR 20000-3:2009, ISO/IEC TR 20000-5:2010, kurie šiuo metu peržiūrimi pagal 3-iąją ITIL versiją.

ITIL metodika apima kontrolės priemonių diegimo reikalavimus ir saugumui valdyti, metodikos saugumo valdymo pri-

[1] ISO Catalogue. Prieiga per internetą: http://www.iso.org/iso/iso_catalogue.htm [žiūrėta 2010 m. liepos 16 d.].

[2] COBIT. Prieiga per internetą: http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx [žiūrėta 2011 m. kovo 10 d.].

[3] ITIL. Prieiga per internetą: http://www.itil-officialsite.com [žiūrėta 2011 m. kovo 10 d.].



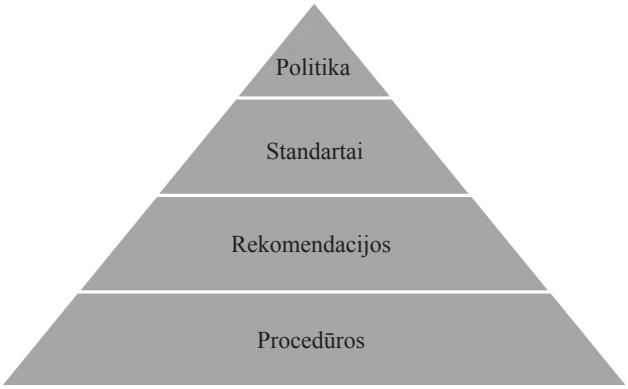
3 pav. ***Organizacijos valdymo sąsajos su IT ir saugumo valdymu***

cipai glaudžiai siejasi su ISO 27000 standartų grupe.

Išanalizavus minėtų informacijos saugumo valdymo standartų ir metodikų turinį, galima teigti, kad šie dokumentai kaip pagrindinį saugumo objektą įvardija informaciją ir pabrėžia informacijos saugumo valdymo sistemiškumą, jo taikymą visos organizacijos mastu, taigi informacijos saugumo valdymas, suderintas su informacinių technologijų valdymu, turi būti integrali visos organizacijos valdymo dalis (3 pav.).

Organizacijos (verslo ar valstybinės), remdamosi pristatytais informacijos saugumo valdymo standartais ir metodikomis, informacijos saugumo valdymo tikslus, uždavinius ir informacijos tvarkymo reikalavimus turėtų nustatyti pagrindiniame organizacijos saugumo valdymo dokumente, vadinamame *informacijos saugumo politikos dokumentu*. Kiekviena organizacija, nusprendusi taikyti savo veikloje šiuos standartus, turi turėti tokį koncepcinį dokumentą, patvirtintą aukščiausios organizacijos vadovybės.

Informacijos saugumo politikos dokumento turinys individualus kiekvienai organizacijai, jame aprašoma siekiama informacijos saugumo būklė, bendrieji saugumo principai, įvardijama saugoma informacija ir ištekliai, nustatomi saugumo prioritetai (ISO 27000 standartų grupė). Informacijos saugumo politika įgyvendinama standartais, procedūromis, rekomendacijomis ir kitais žemesniojo valdymo lygio dokumentais, kurių paskirtis, sąryšiai ir nuorodos į juos taip pat išdėstomi informacijos saugumo politikos dokumente (4 pav.). Šie dokumentai skirti konkrečių paslaugų



4 pav. ***Informacijos saugumo valdymo dokumentų hierarchija***

vartotojams, informacinių technologijų specialistams, sistemų administratoriams.

Apibendrinant galima teigti, kad aptartų informacijos saugumo valdymo standartų ir metodikų turinys išreiškia platų informacijos saugumo valdymo koncepcijos turinį ir jie gali būti laikomi informacijos saugumo koncepcijos įgyvendinimo priemonėmis. Šių priemonių taikymas suteikia organizacijoms tikrumo 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, pripažinto įvertinimo ir sertifikavimo galimybės, atitikties teisiniams reikalavimams bei aplinkai ir nusako, ko galima tikėtis iš organizacijos, įdiegusios konkretų standartą, t. y. sistemiškai įgyvendinti informacijos saugumo valdymo koncepciją strateginiu, žmogiškojo veiksnio ir technologiniu požiūriais.

Informacijos saugumo valdymo Lietuvos viešajame sektoriuje tyrimas

Sisteminant mokslininkų teorinius konceptus, formuluojant informacijos saugumo valdymo koncepciją ir išskiriant jos įgyvendinimo priemones, sukuriamos prielaidos vykdyti informacijos saugumo valdymo tyrimus. Kaip minėta, informacijos saugumo valdymo problematikos specifiškumas pasireiškia organizacijų, valstybės bei tarptautiniu lygmeniu, o valstybės, suvaldžiusios informacijos saugumą savo viduje (t. y. organizacijų lygmenį), gali tinkamai prisidėti prie tarptautinio lygmens informacijos saugumo užtikrinimo.

Vertinant Lietuvos pasirengimą tarptautinio lygmens rizikai valdyti, iškeltas uždavinys įvertinti situaciją Lietuvos viešajame sektoriuje. Šis sektorius, kaip jau minėta, pasirinktas atsižvelgiant į viešosios teisės pricipus: viešajam sektoriui leidžiama tik tai, kas nurodyta, t. y. sektorių įpareigoja aiškūs teisiniai rėmai, kurių sektoriaus subjektai negali peržengti pasirinkdami, kaip reaguoti į globalias rizikas.

Vykdant tyrimą atlikta: 1) dokumentų analizė – įvertintas informacijos saugumo valdymo reikalavimų, įtvirtintų Lietuvos Respublikos teisės aktais, skirtais viešojo sektoriaus organizacijoms, turinys, ieškant sąsajų su išskirtomis informacijos saugumo valdymo koncepcijos įgyvendinimo priemonėmis – tarptautiniais informacijos saugumo valdymo standartais; 2) dokumentinis tyrimas, kaip šių reikalavimų laikomasi pasirinktoje grupėje – Lietuvos Respublikos ministerijose. Šis tyrimas vykdomas apsiribojant strateginiu informacijos saugumo valdymo koncepcijos požiūriu.

Pirmuosius informacijos saugumo reikalavimus Lietuvos Respublikos Vyriausybė patvirtino 1997 metais, siekdama užtikrinti duomenų patikimumą ir apsaugą nuo neteisėto naudojimo (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. Informacijos saugumo valdy-

mas turi būti išdėstytas duomenų saugos nuostatuose (saugumo politikos dokumente), kurį tvirtina informacinės sistemos valdytojas.

2001 metais į informacijos saugumą buvo pažvelgta plačiau ir 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 grupės „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, buvo atnaujinti Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai (toliau – Bendrieji saugumo reikalavimai), kurių 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 grupės „Informacijos technologija. Saugumo metodai“ standartais, apibūdinančiais saugų informacinės sistemos duomenų tvarkymą.

Įgyvendinant antrąją saugos strategiją taip pat buvo patvirtinta: 1) informacinių sistemų klasifikavimo gairės, kurios nustatė informacinių sistemų klasifikavimo kriterijus nuo pirmos (svarbiausių) iki ketvirtos kategorijos; 2) detalūs elektroninės informacijos saugos reikalavimai, kurie detalizavo konkrečios kategorijos informacinių sistemų reikalavimus.

Vertinant registrų reikalavimus, pastebėta: aktuali Valstybės registrų įstatymo redakcija nustato, kad registrų informacijos saugumas taip pat užtikrinamas *vadovaujantis Vyriausybės patvirtintais bendraisiais duomenų saugos reikalavimais* (Valstybės registrų įstatymas, 2009).

Šiuo metu yra rengiamas naujas strateginis dokumentas – Elektroninės informacijos (kibernetinio saugumo) plėtros programa, kurios tikslas – apimti visus, ne tik viešąjį, sektorius, tačiau šis dokumentas dar nepatvirtintas; buvo parengtos kelios redakcijos, vyksta diskusijos dėl jo turinio, todėl šiuo metu nėra galimybių detaliau išanalizuoti ir įvertinti dokumento.

Atlikus Lietuvos viešajam sektoriui galiojančių teisės aktų turinio analizę, galima konstatuoti:

1. Teisės aktais (Bendraisiais saugumo reikalavimais) Lietuvos viešajame sektoriuje yra įteisintas pagrindinis informacijos saugumo valdymo dokumentas – duomenų saugos nuostatai, kurie 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 privalomai Lietuvos standarte LST ISO/IEC 17799:2006 nurodytas technines priemones turi įgyvendinti tik pirmos kategorijos (svarbiausių)

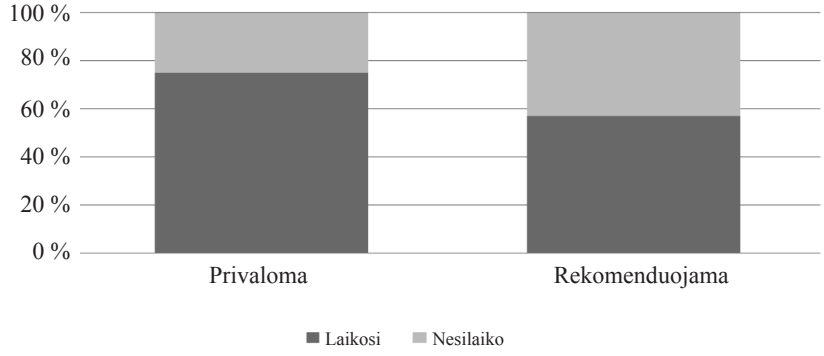
valstybės informacinių sistemų valdytojai. Pažymėtina, kad tik rekomenduojamas standarto taikymas apsunkina informacijos saugos valdymo reikalavimų ir informacijos saugumo valdymo koncepcijos atitikties vertinimą, taip pat kad LST ISO/IEC 17799:2006 standartą jau pakeitė ISO 27000 grupės standartai.

3. Visi teisės aktai, reglamentuojantys informacijos saugumo valdymą, Lietuvos Respublikos Vyriausybės patvirtinti be įstatymų pagrindo (išskyrus valstybės registrų atvejį), o be šio pagrindo pati Vyriausybė neturi galių reguliuoti jai nepavaldžių institucijų veiklos; tai leidžia teigti, kad visi nustatyti informacijos saugumo reikalavimai privalomi tik Lietuvos Respublikos Vyriausybei pavaldžioms institucijoms.

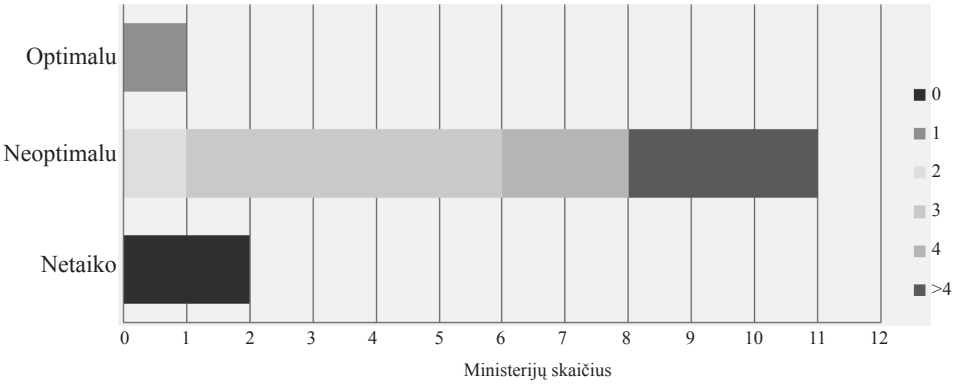
Taigi ir Bendrieji saugumo reikalavimai privalomai taikomi tik valstybės registrų valdytojams ir valstybės informacines sistemas valdančioms Lietuvos Respublikos Vyriausybei pavaldžioms institucijoms (ministerijoms, Vyriausybės įstaigoms, departamentams ir pan.), tačiau institucijos, valdančios informacines sistemas, bet nepavaldžios Lietuvos Respublikos Vyriausybei (teismai, prokuratūra, savivalda ir pan.), saugos reikalavimus gali taikyti savo nuožiūra arba jų iš viso netaikyti.

Įrodyti, kad ši situacija yra rimta saugumo užtikrinimo problema, galima remiantis Valstybės kontrolės išvadomis. Ši institucija turi didžiausią įdirbį vertinant informacijos saugumo valdymo reikalavimus ir jų taikymą Lietuvos viešajame sektoriuje. 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 kaip 40 procentų valstybės institucijų (Aleliūnas, Kindurytė, Kiškina, 2007; 5 pav.).

4. Lietuvos viešajame sektoriuje informacijos saugumo valdymo reikalavimų taikymo objektu istoriškai susiklostė (ir teisės aktais įtvirtinta) informacinės sistemos ir registrai, todėl duomenų saugos nuostatus privalo parengti ir patvirtinti informacinių sistemų ir registrų valdytojai. Ši situacija kelia sunkumų institucijoms, kurios valdo daugiau nei vieną valstybės



5 pav. ***Reikalavimų laikymasis Lietuvos viešojo sektoriaus institucijose***
(pagal Aleliūnas, Kindurytė, Kiškina, 2007)



6 pav. ***Informacijos saugumo politikos dokumentų skaičius ministerijose***

informacinę sistemą ar registrą, o institucijos, kurios nevaldo nė vienos formalizuotos informacinės sistemos ar registro, lieka už informacijos saugumo valdymo reikalavimų taikymo ribų.

Šioms informacijos saugumo valdymo problemoms atskleisti atliktas Vidaus reikalų ministerijos turimų valstybės institucijų, kurios pagal nustatytus Bendruosius saugos reikalavimus teikia ministerijai saugos reikalavimų atitikties informaciją, duomenų tyrimas. Analizuojant Vidaus reikalų ministerijos sukauptuose sąrašuose esamus įrašus apie 14 Lietuvos Respublikos ministerijų, galima rasti net 45 galiojančius duomenų saugos nuostatus (saugumo politikos dokumentus). Šios analizės rezultatai pateikti 6 paveiksle. Pažymėtina, kad tik viena ministerija turi vienus, visas jos valdomas informacijos sistemas apimančius duomenų saugos nuostatus (viršutinis 6 pav. stulpelis), vienuolika ministerijų turi dvejus ir daugiau duomenų saugos nuostatų, kai kurios iš jų turi net po keturis ir daugiau patvirtintų saugos politikos dokumentų atskirai kiekvienai valdomai informacinei sistemai (vidurinis 6 pav. stulpelis), taip pat šiame sąraše galima rasti dvi ministerijas, kurios neturi jokio patvirtinto saugos politikos dokumento (apatinis 6 pav. stulpelis) ir nevaldo jokios teisės aktų nustatyta tvarka įteisintos informacinės sistemos.

Remiantis 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 strateginiu informacijos saugumo koncepcijos įgyvendinimo požiūriu (politikos dokumentų įvertinimu) tik vienoje ministerijoje iš keturiolikos yra optimali informacijos saugumo valdymo situacija, vienuolikoje neoptimali, o dvi ministerijos iš viso netaiko informacijos saugumo valdymo reikalavimų savo veikloje.

Apibendrinant dokumentų analizės rezultatus galima teigti, kad Lietuvos viešajam sektoriui teisės aktai nustato informacijos saugumo valdymo reikalavimus, kurie remiasi informacijos saugumo valdymo koncepcijos įgyvendinimo priemonėmis, tačiau šie reikalavimai neapima visų sektoriaus organizacijų. Informacijos saugumo

valdymo koncepcijos įgyvendinimo kontekste galima išskirti tris pagrindines informacijos saugumo valdymo problemas, kurios susiformavo *visų pirma* dėl to, kad galiojantys informacijos saugumo reikalavimai iš esmės tik rekomenduoja taikyti tarptautinius informacijos saugumo valdymo standartus, dėl to sunku įvertinti pačių reikalavimų turinį be detalios papildomos lyginamosios analizės; *antra,* Lietuvos Respublikos Vyriausybė be teisinio 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, todėl formaliai informacinių sistemų nevaldančios institucijos reikalavimų netaiko, o valdančios kelias sistemas turi papildomų sunkumų derindamos kelis aukščiausio lygio informacijos saugumo politikos dokumentus.

Išvados ir siūlymai

Informacijos saugumo valdymo sąvokos turinys evoliucionavo nuo siauro techninio suvokimo iki plačios informacijos saugumo valdymo koncepcijos, kuri integravo strateginį, žmogiškojo veiksnio ir technologinį požiūrius (dimensijas). Tarptautiniai informacijos saugumo valdymo standartai ir metodikos pagal savo turinį gali būti laikomi informacijos saugumo valdymo koncepcijos įgyvendinimo priemonėmis.

Atliktos dokumentinės analizės rezultatai leidžia teigti, kad informacijos saugumo valdymas Lietuvos viešajame sektoriuje neužtikrina sistemiško informacijos saugumo valdymo koncepcijos įgyvendinimo. Pagrindinės priežastys šios: 1) galiojantys informacijos saugumo valdymo reikalavimai remiasi tik rekomenduojamu informacijos saugumo valdymo koncepcijos 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 sistemiškai įgyvendinti informacijos saugumo valdymo koncepciją Lietuvos viešajame sektoriuje, būtina plėsti informacijos saugumo valdymo reikalavimų taikymo objektą ir subjektus.

Pažymėtina, kad Lietuvoje trūksta mokslinių informacijos saugumo valdymo tyrimų, todėl formuluojant detalius siūlymus, kaip koreguoti Lietuvos viešajam sektoriui galiojančius informacijos saugumo valdymo reikalavimus, straipsnyje pristatyta tyrimų tema turėtų būti tęsiama keliomis kryptimis. Reikėtų įvertinti, kaip Lietuvos viešasis sektorius įgyvendina rekomendaciją taikyti tarptautinius informacijos valdymo standartus ir metodikas, t. y. atlikti detalią viešojo sektoriaus subjektų duomenų saugos nuostatų (saugumo politikos dokumentų), galiojančių informacijos saugumo reikalavimų ir tarptautinių informacijos saugumo valdymo standartų turinio lyginamąją analizę. Taip pat vertėtų plačiau palyginti tyrimų rezultatus su užsienio šalių viešojo sektoriaus analogiška patirtimi.

Tokios analizės rezultatai galėtų išryškinti, ar siekiant sistemiškai įgyvendinti informacijos saugumo valdymo koncepciją pakanka išplėsti Lietuvos viešajam sektoriui galiojančių reikalavimų taikymo objektą ir subjektus, ar reikia esminių šių reikalavimų turinio korekcijų remiantis privalomu tarptautinių standartų taikymu.

LITERATŪRA IR ŠALTINIAI

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>.

ASCH, Sodomon (1952). *Social Psychology*. New York: Prentice-Hall.

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

Asmens duomenų teisinės apsaugos įstatymas (2008) [interaktyvus]. [žiūrėta 2010 m. rugpjūčio 20 d.]. Prieiga per internetą: <http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_ id=314940>.

AMARAL, Paulo (2007). Towards the creation of security ontologism for information technology, communications, information systems, information and knowledge in organizations. In Knop, J.; Salinikov, 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. Amsterdam: IOS Press.

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

ANDERSON, Ross (2001). Why information security is hard – an economic perspective. In *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>

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

ATKOČIŪNIENĖ, Zenona (2009). Informacijos vadyba verslo organizacijos vadybos sistemoje. In Atkočiūnienė, Z.; Janiūnienė, E.; Matkevičienė, R.; Pranaitis, R.; Stonkienė, M. *Informacijos ir žinių vadyba verslo organizacijoje*: monografija. Vilnius: VU leidykla, p. 93–142.

Bendrieji duomenų apsaugos reikalavimai (1997) [interaktyvus]. Lietuvos Respublikos Vyriausybės 1997-09-04 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>.

CAELLI, William (2002). Trusted ... Or ... Trustworthy: The search for a new paradigm for computer and network security. *Computers and Security*, 21(5), p. 413–420.

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.

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-security-survey/pdf/pwcsurvey2010_report.pdf>.

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>.

ČĖSNA, R.; ŠTITILIS D. (2000). *Kompiuterinės informacijos ir elektroninių dokumentų apsauga viešajame administravime*. Vilnius: LTU.

D'ARCY, J.; HOVAV, A. (2009). An Integrative Framework for the Study of Information Security Management Research. In Jatinder, Gupta; and Sushil, Sharma (eds.). *Handbook of Research on Information Security and Assurance*. Idea Group Publishing, p. 55–67.

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

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

Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinė strategija

iki 2008 metų. LR Vyriausybės 2006 m. birželio 19 d. nutarimas Nr. 601 [interaktyvus]. [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=>.

ELOFF, J. H. P; ELOFF, M.M. (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. ISBN 1-58113-774-5.

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>.

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

GAO (2010). United States Government Accountability Office. CYBERSECURITY: Continued attention is needed to protect Federal Information Systems from evolving threats. 2010 m. birželio 16 d. [interaktyvus]. [žiūrėta 2010 m. rugpjūčio 20 d.]. Prieiga per internetą: <http://www.gao.gov/new.items/d10834t.pdf>.

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>.

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

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

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

Informacijos technologijų saugos valstybinė strategija. LR Vyriausybės 2001 m. gruodžio 22 d. 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>.

Infosecurity Europe (2010). Information Security Breaches Survey [interaktyvus]. [žiūrėta 2010 m. liepos 15 d.]. Prieiga per internetą: <http://www.infosec.co.uk/files/isbs_2010 _technical_report_single_pages.pdf>.

JANELIŪNAS, T (2007). *Komunikacinis saugumas*. Vilnius: VU leidykla.

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.

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

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

MIKUČIONIS, M.; TOLDINAS, E.; VENČKAUSKAS, A. (2007). Korporacinių įmonių informacinės saugos architektūrų modeliavimas. *Informacijos mokslai*, t. 42–43, p. 175–181.

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>.

PARAKKATTU, Sindhuja; KUNNATHUR, Anand. S (2010). A Framework for research in information security management. In *Proceedings for the Northeast Region Decision Sciences Institute* (NEDSI), p. 318–323.

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

PAŠKAUSKAS, Žydrūnas (2007). Elektroninės informacijos saugos tarptautinio teisinio reguliavimo analizė: Lietuvos padėtis. *Jurisprudencija,* Nr. 5(83), p. 82–89.

PAULAUSKAS, Nerijus (2009). *Incidentų kompiuterių sistemose tyrimas ir saugumo lygio įvertinimas*: Daktaro disertacija. VGTU. Vilnius: Technika.

PSI (2008). Payment Card Industry Data Security Standard [interaktyvus]. [žiūrėta 2010 m. liepos 15 d.]. Prieiga per internetą: <https://www.

pcisecuritystandards.org/security_ standards/pci_ dss.shtml>.

RYAN, Johnny (2008). Analizė „I.karas“: nauja grėsmė, jos parankumas ir didėjantis mūsų pažeidžiamumas [interaktyvus]. NATO apžvalga [žiūrėta 2011 m. vasario 3 d.]. Prieiga per internetą: <http://www.nato.int/docu/review/2007/issue4/lithuanian/analysis2.html> .

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>.

RUSSELL, Deborah; GANGEMI G. T. (1991). *Computer security basics*. United States of America: O'Reilly & Associates, Inc.

SMITH, Stephen; JAMIESON, Rodger; BUNKER, Deborah; WINCHESTER, Donald (2008). Moving Towards Information System Security Accreditation within Australian State Government Agencies [interaktyvus]. AMCIS 2008 Proceedings. Paper 46 [žiūrėta 2010 m. rugpjūčio 7 d.]. Prieiga per internetą: <http://aisel.aisnet.org/amcis2008/46>.

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

TIMKO, Dan (2008). The Social Engineering Threat. [interaktyvus]. January. ISSA Journal, [žiūrėta 2010 m. liepos 16 d.]. Prieiga per internetą: <https://www.issa.org/Library/Journals/2008/January/Timko-The%20Social%20Engineering%20Threat.pdf>.

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>.

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

SOX (2002). Sarbanes-Oxley Act [interaktyvus]. [žiūrėta 2010 m. liepos 15 d.]. Prieiga per internetą: <http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/content-detail.html/>.

Valstybės registrų įstatymas [interaktyvus]. [žiūrėta 2010 m. rugpjūčio 20 d.]. Prieiga per internetą: <http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=359302>.

VENČKAUSKAS, Algimantas; KRIVICKIENĖ, Vita; TOLDINAS, Eugenijus (2009). Kompiuterių ir operacinių sistemų saugos modulio programos sudarymas. *Informacijos mokslai*, t. 50, p. 187–193.

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>

von SOLMS, Basie (2000). Information Security – The Third Wave. *Computers and Security*, vol. 19(7), p. 615–620.

von SOLMS, Basie (2001). Information security – A multidimensional discipline. *Computers and Security*, vol. 20(6), p. 504–508.

von SOLMS, Basie (2006). Information Security – The Fourth Wave. *Computers and Security*, vol. 25(6), p. 165–168.

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.

WERLINGER, Rodrigo; HAWKEY, Kirstie; BEZNOSOV, Konstantin (2009). An integrated view of human, organizational and technological challenges of IT security management [interaktyvus]. *Information Management & Computer Security*, 17(1), p. 4–19 [žiūrėta 2011 m. sausio 16 d.]. Prieiga per internetą: <http://lersse-dl.ece.ubc.ca/record/153/files/153.pdf>.

WHITTEN, Alma; TYGAR, J. D. (1999). Why Johnny can't encrypt. In *Proc. Eighth USENIX Security Symposium*. Washington, DC, 23–26 August, p. 169–184.

INFORMATION SECURITY MANAGEMENT IN LITHUANIA'S PUBLIC SECTOR

Saulius Jastiuginas

S u m m a r y

Information security is becoming more and more important in modern society. The most common information security issues become apparent when information security incidents or violations occur. Worldwide growth in the number of security breaches and losses are the major indicators showing that there is a lack of systematic approach to information security management.

Solution of practical problems requires the use of scientific approaches. Among academic researchers, a number of studies that focus on various aspects of information security management have emerged in recent years. Scientists are exploring the issues of information security management in various strategic, technological and human factor issues that also deals with the problems of organizations, national and international levels.

Currently, in Lithuania is a lack of information security management research. In order to highlight the information security management characteristics of Lithuania in an international context, this paper combines a theoretical foreign and Lithuanian scientific information security management insights into the systemic information security management concept.

This article also contains the results of the study, which allowed an assessment of the situation in Lithuania's public sector information security management and creates preconditions for further research.