INFORMACIJOS VADYBA

Integralus informacijos saugumo valdymo modelis

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

Saugumo sąvoka yra daugialypė ir nevienareikšmiškai apibrėžiama, saugumas gali būti suprantamas kaip būsena, kuri gali reikšti ir 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) saugu. Analizuojant informacijos saugumo mokslinių tyrimų problematiką, galima daryti prielaidą, kad pagrindinis objektas, kurį siekiama apsaugoti, yra informacija, tačiau neretai saugumo objektu virsta informacinės technologijos ar informacinės sistemos, kuriomis tvarkoma informacija. Darant esminę mokslinę prielaidą, kad svarbiausias informacijos saugumo objektas yra informacija, tikėtina, kad informacijos saugumas turėtų būti tiriamas kaip sudėtinė informacijos vadybos ir kitų gretutinių informacinių koncepcijų (informacijos išteklių vadybos, informacijos sistemų vadybos, informacijos įrašų vadybos) dalis. Straipsnyje aptariamas tyrimas, įrodantis keliamos mokslinės prielaidos pagrįstumą.

Pagrindiniai žodžiai: *informacijos saugumas, informacijos saugumo valdymas, informacijos vadyba, informacijos saugumo valdymo modelis.*

Įvadas

Nagrinėjant teorines mokslininkų įžvalgas ryškėja, kad informacijos saugumo mokslinių tyrimų laukas nuolat plečiasi. Ilgą laiką išskirtinai vyravę techniniai informacijos saugumo klausimai tebėra aktualūs, tačiau pastebima akivaizdi informacijos saugumo mokslinių tyrimų problematikos slinktis link platesnio, vis daugiau aspektų apimančio vadybinio požiūrio. Šiuo metu plačiausiai taikomų informacijos saugumo valdymo priemonių (metodikų, standartų, modelių) raidos analizė leidžia konstatuoti augančią taikomų priemonių turinio asimiliaciją, tačiau stebint nuolat kylančias informacijos saugumo problemas (pavyzdžiui, informacijos saugumo incidentų gausėjimą), aiškėja, kad esamos priemonės nėra pakankamos informacijos saugumui valdyti.

Šios tendencijos formuoja naujų informacijos saugumo valdymo priemonių paieškos mokslinių tyrimų poreikį ir stiprina mokslinę prielaidą, kad informacijos saugumo valdymas iš technologinės tapdamas vadybine disciplina turėtų būti nagrinėjamas kaip sudedamoji informacijos vadybos dalis.

Straipsnio tikslas – sukurti moksliškai pagrįstą integralų informacijos saugumo valdymo modelį, jungiantį informacijos saugumo valdymo ir informacijos vadybos dedamąsias. Straipsnyje keliami uždaviniai: suformuoti informacijos saugumo apibrėžtį; išnagrinėti pagrindinių informacijos vadybos tyrėjų įžvalgas ir identifikuoti saugumo vietą informacijos vadybos mokslų konceptuose; lyginamosios analizės būdu išskirti informacijos vadybos įrankius, kurie potencialiai būtų tinkami informacijos saugumui valdyti; apibendrinant šių teorinių tyrimų rezultatus, suformuoti integralų teorinį informacijos saugumo valdymo modelį.

Straipsnis parengtas remiantis mokslinės literatūros analizės, lyginamosios analizės, loginės analizės, abstrakcijos ir analogijos bei apibendrinimo metodais.

Informacijos saugumo apibrėžtis

Dauguma *informacijos saugumo* apibrėžčių jau daugiau kaip dvidešimt metų remiasi trimis informacijos saugumo tikslais (CIA triada). Pagal CIA triadą įvardijama, kad *informacijos saugumo* tikslas – užtikrinti informacijos konfidencialumą *(confidentiality)*, vientisumą *(integrity)* ir prieinamumą *(availability)*, 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, visi pakeitimai yra žinomi; *prieinamumas* – užtikrinta galimybė pasinaudoti informacija, t. y. sankcionuoti vartotojai turi turėti galimybę pasiekti informaciją, kai jos reikia. Kai kurie autoriai, pavyzdžiui, Donnas Parkeris (1998), pristatydamas savo saugumo heksadą, bandė plėsti informacijos saugumo tikslus pridėdami autentifikavimo, autorizavimo, atskaitomybės, neatsisakymo ir kitus aspektus, tačiau sistemiškai analizuojant informacijos saugumo 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) taip pat yra vientisumo sudedamoji dalis (Parker, 1981, 1998; McCumber, 2005; Trcek, 2006; ISO 27000 standartų grupė ir kiti).

Informacijos saugumo apibrėžties kaitai darė įtaką nemažai mokslinių tyrimų. Tyrinėjant informacijos saugumo problematiką, analizuota informacijos saugumo suvoktis (Parker, 1981; Trcek, 2006; McCumber, 2005; Zafar ir Clark, 2009; Mikalauskienė, Brazaitis, 2010), įvairūs techniniai (Anderson, Moore, 2009), ekonominiai (Gordon, Loeb, 2006 ir kiti), vadybiniai (Chang, Lin 2007; Dlamini, Eloff, Eloff, 2009), standartų taikymo (Weise, 2009), saugos priemonių taikymo (Kazanavičius ir kt., 2012; Japertas, Činčikas, Šestaviskas, 2012), socialinės inžinerijos, psichologiniai ir žmogiškieji (Ashenden, 2008; Bakhshi, Papadaki ir Furnell, 2009), teisinio reglamentavimo ir reguliavimo (Štitilis, Paškauskas, 2007) bei kiti informacijos saugumo aspektai. Analizuojant ir vertinant informacijos saugumo teorijos raidą ir praktinio taikymo patirtį daug prisidėjo F. Bjorckas ir L. Yngstromas (2009),

H. Zafaras ir J. Clarkas (2009), von Solmsas (2001, 2010) ir kiti tyrėjai.

Analizuojant mokslinėse diskusijose nagrinėjamų teorinių įžvalgų visumą, galima konstatuoti aktualių informacijos saugumui aspektų plėtrą. Informacijos saugumo turiniui išryškinti svarbią reikšmę įgyja nuo devintojo dešimtmečio lygiagrečiai su siaurais atskirų informacijos saugumo aspektų tyrimais pradėję vystytis tarpdisciplininiai 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 joms 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.

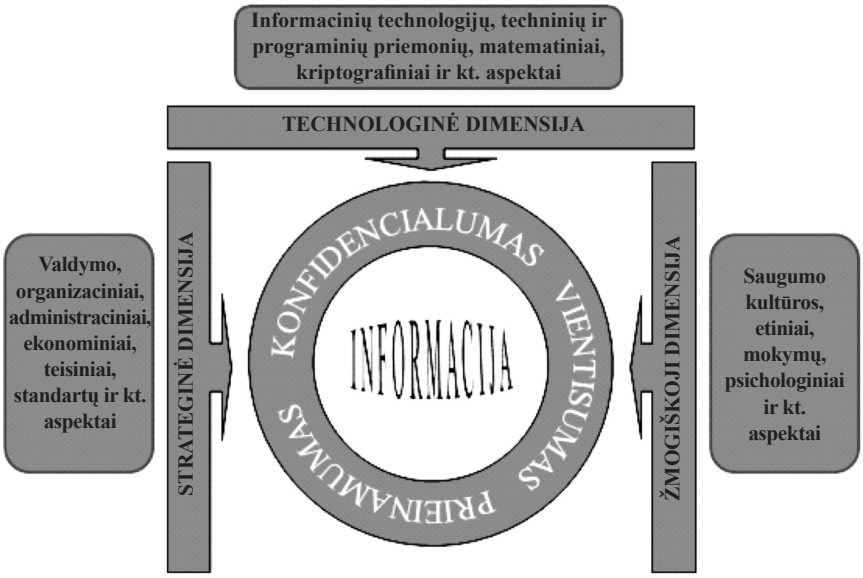
Apibendrinant informacijos saugumo tyrimus ir juose analizuotus informacijos saugumo aspektus, galima konstatuoti, kad informacijos saugumo valdymas apima tris dimensijas – *strateginę, žmogiškąją* ir *technologinę.* Strateginė dimensija jungia administracinius, organizacinius, valdymo, ekonominius, standartų, teisinius, gerųjų praktikų ir pan. aspektus, žmogiškoji – saugumo kultūros, etinius, kompetencijų, mokymų, psichologinius ir pan.; technologinė – informacinių technologijų, techninių ir programinių priemonių, matematinius, kriptografinius ir pan. (Jastiuginas, 2011).

Remiantis Barry Buzano (1997) saugumo studijomis, nagrinėjant saugumo sąvoką, kaip objektyvaus saugumo būseną, kyla poreikis įvardyti ne tik objektą, kas turi būti (tapti) saugu, bet ir sąlygas, kurios leidžia teigti objektą esant (tapus) saugų. Jungiant išryškintas informacijos saugumo valdymo dimensijas, formuojasi visuminis požiūris į informacijos saugumo turinį, aiškėja platus bei nuolat kintantis informacijos saugumo sąlygų kontekstas. Taigi norint 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.

Visuminiam požiūriui į informacijos saugumo valdymo turinį apibrėžti tikslinga jungti informacijos saugumo valdymo objektą, tikslus ir dimensijas. Remiantis aptarta teorine medžiaga pagrindiniu informacijos saugumo valdymo objektu įvardytina informacija, o informacijos saugumo valdymo tikslais – aptarta CIA triada, t. y. 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.

Informacijos saugumo valdymo turinys gali būti apibrėžiamas kaip siekis užtikrinti informacijos konfidencialumą, vientisumą ir prieinamumą derinant strateginę, žmogiškąją ir technologinę dimensijas (1 pav.).

Siekiant valdyti informacijos saugumą nepakanka apibrėžti informacijos saugumo valdymo turinį, tačiau būtina numatyti ir priemones, kuriomis jis galėtų būti valdomas.



1 pav. ***Informacijos saugumo valdymo turinys (sudaryta autoriaus)***

Informacijos saugumo valdymo priemonės

Platus informacijos saugumo turinys lėmė jo įgyvendinimo 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 lėmė formalizuotų informacijos saugumo užtikrinimo priemonių atsiradimo būtinybę. Tokiomis priemonėmis tapo šiame skyrelyje aptariami vyraujantys informacijos saugumo valdymo standartai, metodikos ir modeliai.

Informacijos saugumo valdymo standartai

Analizuojant ISO standartų katalogą[1], galima rasti per 350 standartų, susijusių su įvairiais informacijos saugumo valdymo aspektais, tačiau įvertinus jų turinio aprašymus ir bendrą informacijos saugumo srities standartų aprėptį, galima konstatuoti, kad daugiausia standartų susiję su įvairiomis techninėmis saugumo užtikrinimo priemonėmis. Vertinant informacijos standartų vystymąsi pabrėžtina, kad tik 1995 metais pasirodė pirmasis informacijos saugumo standartas plačiau išryškinęs vadybines dedamąsias, tokiu standartu tapo Jungtinės Karalystės standartizacijos įstaigos patvirtintas standartas BS 7799[2]. Tarptautinėje erdvėje vis labiau ryškėjant suderintam informacijos saugumo valdymo poreikiui, 2000 metais, pripažinus britiškojo standarto pranašumus, jo pagrindu buvo parengtas ISO 17799 standartas, vėliau išsirutuliojęs į atskirą informacijos saugumo valdymo standartų grupę ISO

[1] ISO Catalogue. http://www.iso.org/iso/iso_catalogue.htm [žiūrėta 2012 m. liepos 16 d.].

[2] BSI // http://www.bsigroup.co.uk/ [žiūrėta 2012 m. birželio 1 d.].

27000. Šios grupės standartai skirti tiesioginiam informacijos saugumo valdymui, informacijos saugumo valdymo sistemos kūrimui, praktinių priemonių diegimui, įvertinimui ir organizacijos sertifikavimui. Remiantis J. Weise'o (2009) ir kitų informacijos saugumo valdymo standartų taikymo tyrėjų įžvalgomis pažymėtina, kad ISO 27000 grupės standartai pripažinti *de facto* informacijos saugumo valdymo gerosios praktikos pavyzdžiu.

Informacijos saugumo valdymo metodikos

Valdant ir diegiant informacinių technologijų sprendimus susiklostė gerų praktikų pavyzdžiai, kurie ilgainiui tapo plačiai pripažįstamomis, nuolat tobulinamomis metodikomis, savo turinyje integravusiomis ir informacijos saugumo valdymo priemones. Daugiausia dėmesio sulaukė COBIT ir ITIL metodikos, kurios apima ir informacijos saugumo valdymą.

COBIT (*Control Objectives for Information and Related Technologies*)[3] – pasaulyje pripažintas metodikų rinkinys Informacijos ir ryšių technologijų ūkio valdymui, kuris remiasi rinkos standartais ir geriausiomis praktikomis. Pirmoji metodikų rinkinio versija išleista 1996 metais, jį 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. lapkritį buvo pateiktas COBIT metodikos vertimas ir į lietuvių kalbą[4].

Vertinant COBIT metodikos vystymąsi, galima konstatuoti, kad kiekvienoje versijoje informacijos saugumui valdyti skiriama vis daugiau dėmesio, o informacijos saugumo užtikrinimas vis glaudžiau integruojamas į bendrus informacinių technologijų sėkmingo valdymo procesus. Šią tendenciją tęsia ir šiuo metu baigiama rengti COBIT metodikos 5-oji versija, kurios projekte saugumas išryškinamas kaip vienas svarbiausių uždavinių. Naujos metodikos versijos laukiama pasirodant 2012 metais.

ITIL (*Information Technology Infrastructure Library*)[5] – 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 geriausios praktikos pavyzdžiais. Metodikos pagrindinis vystytojas – Didžiosios Britanijos vyriausybės Prekybos rūmai *(Office of Government Commerce* – OGC). ITIL metodika apima kontrolės priemonių diegimo reikalavimus ir saugumo valdymui, metodikos saugumo valdymo principai glaudžiai siejasi su ISO 27000 standartų grupe.

Informacijos saugumo valdymo modeliai

Informacijos saugumo valdymo tyrėjai, atskiros veiklos šakos ar net įvairių saugu-

[3] COBIT // http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx [žiūrėta 2012 m. kovo 10 d.].

[4] Lietuviška COBIT versija // http://www.cobit.lt/ [žiūrėta 2012 m. balandžio 11 d.].

[5] ITIL // http://www.itil-officialsite.com/ [žiūrėta 2012 m. kovo 10 d.].

mo produktų gamintojai sukūrė ne vieną informacijos saugumo valdymo modelį. Neįvardydami konkrečių priemonių ar įgyvendinimo gairių jie suformulavo apibendrintus informacijos saugumo valdymo principus.

McCumber kubas. 1991 metais Johnas McCumberis sukūrė informacijos saugumo valdymo modelį, kurį sudaro trimačio kubo ląstelės. Trys kubą sudarančios dimensijos yra šios: informacijos charakteristikos (informacijos saugumo tikslai) – konfidencialumas, vientisumas, prieinamumas; informacijos būsena – apdorojimas, saugojimas, perdavimas; informacijos apsaugos priemonės – technologijos, politika ir praktika, žmogiškasis veiksnys (McCumber, 2005).

Modelio autorius pabrėžia šio modelio universalumą ir atsiribojimą nuo technologinio informacijos saugumo požiūrio. J. McCumberio teigimu, modelio unikalumą užtikrina tai, kad informacija gali būti tik trijų būsenų, ir kiekvienu konkrečiu atveju yra arba apdorojama, arba perduodama, arba saugoma, modelyje numatyti apibendrinti saugumo tikslai – vientisumo, konfidencialumo ir prieinamumo užtikrinimas ir apibendrintos visos galimos saugumo užtikrinimo priemonės – politinės, technologinės, žmogiškojo veiksnio.

Analizuojant šio modelio taikymo privalumus, galima pastebėti, kad informacijos saugumo problematika gali būti nagrinėjama bet kuriuo aktualiu pjūviu pasitelkiant bet kurią trimačio kubo dimensijų susikirtimo sudedamąją dalį (ląstelę), pavyzdžiui: pasirenkant informacijos būsenos dimensiją – perduodama informacija, saugumo tikslų dimensiją – konfidencialumas, informacijos saugos priemonių dimensiją – technologijos, galima nagrinėti perduodamos informacijos konfidencialumo užtikrinimo technologijas arba pagal analogiją pasirinkus atitinkamas dimensijas – saugomos 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 (Zeltser 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 maršrutų planavimo ir kitos tinklo srautų skirstymo įrangos stebėjimo priemonės ir kita.

Vertinant šiuolaikinių organizacijų veiklos mastus ir veiklos 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 – įvairiais saugumo metodais ir priemonėmis sulaikyti atakas, kol jos bus pastebėtos ir pašalintos. Šis modelis apima koordinuotą technologijų, personalo ir operacijų elementų saugumą per visą informacinės sistemos gyvavimo ciklą (*Defence in depth*, 2008).

Personalo elementas suprantamas kaip administracinio lygmens problema, kuri sprendžiama suformuojant saugumo politiką ir procedūras, paskirstant pareigas ir at-

sakomybes, 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 elementų suderinimui ir valdymui išskiriamas valdymo elementas, kuris užtikina koordinuotą visų elementų veikimą.

Vertinant Giliosios apsaugos modelio griežtai struktūruotų gynybinių priemonių akcentavimą, jis gali būti plačiai naudojamas statutinėse organizacijose, pavyzdžiui, karinėje 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 vidiniai 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.

Informacijos saugumo valdymo priemonių lyginamoji analizė

Aptarus plačiausiai taikomas informacijos saugumo valdymo priemones, tikslinga atlikti jų lyginamąją analizę siekiant išsiaiškinti, kiek jos atitinka straipsnyje 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 išsamumą 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 straipsnyje aptartų glaudžių jos sąsajų su ISO 27000 standartų šeima), *Perimetro apsaugos* ir *Informacijos srautų saugumo* modeliai (šie modeliai apsiriboja siauresnio pobūdžio konkrečių uždavinių sprendimu). Analizės rezultatai pateikiami 1 lentelėje.

Apibendrinant 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.

1 lentelė. ***Informacijos saugumo įgyvendinimo priemonių palyginimas (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

Lyginant analizės rezultatus su straipsnyje 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 dėmesio skiriama 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 bei

saugos kultūros (informacijos saugumo valdymo turinio žmogiškosios dimensijos sudedamoji dalis) klausimai.

Apibendrinus lyginamosios analizės rezultatus, galima teigti, pagrindinių plačiausiai taikomų informacijos saugumo užtikrinimo priemonių turinys, nors iki neatspindi suformuoto informacijos saugumo valdymo turinio, turi daug bendrumų, o vystantis naujoms šių priemonių kartoms jų turinys dar labiau panašėja.

Saugumas informacijos vadybos moksluose

Siekiant pagrįsti straipsnyje suformuotą esminę mokslinę prielaidą, kad informacijos saugumas turėtų būti tiriamas kaip informacijos vadybos sudedamoji dalis, šioje straipsnio dalyje siekiama atskleisti saugumo teorinį ištirtumą informacijos vadybos mokslų aprėptyje.

Saugumas informacijos vadybos kontekste

Informacijos vadybos apibrėžtis ir reikšmę nagrinėjo daug informacijos vadybos teoretikų: T. Davenportas, T. Wilsonas, D. Chaffey, G. White'as, D. Marchandas, E. Orna, Ch. Schlöglis, S. Woodas, Ch. Choo, Z. Atkočiūnienė, E. Macevičiūtė, A. Augustinaitis, R. Gudauskas, L. Markevičiūtė ir kt.

Remiantis šių tyrėjų atliktomis mokslinėmis įžvalgomis, informacijos vadybos sąvokos raidą galima skirti į tris etapus: 1) šeštojo dešimtmečio antroje pusėje pradėta vartoti 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 įgavo vis daugiau vadybinio konteksto, pabrėžiamas dėmesys pažangiems vadybos sprendimams, efektyviam informacijos apdorojimui, naudojant informacines technologijas, atsiranda organizacinių, kultūrinių, strateginių aspektų. Šiuo metu informacijos vadyboje skiriamos dvi problematikos nagrinėjimo kryptys – informacijos vadyba, orientuota į informacijos technologijas, ir informacijos vadyba, orientuota į turinį (Atkočiūnienė, 2009; 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).

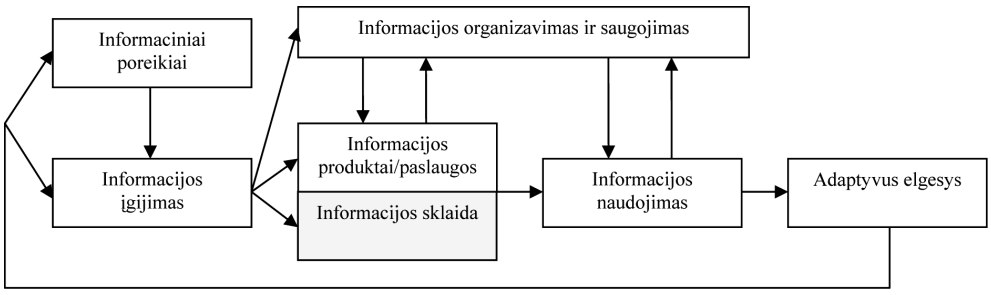
Informacijos vadyboje pabrėžiama informacijos kokybės svarba, jos vertinimo kategorijose taip pat galima rasti informacijos saugumo dedamąją. Informacijos kokybės vertinimo požymiai skirstomi į keturias kategorijas: *esminė kokybės kategorija,* susijusi su tikslumu, objektyvumu, patikimumu ir reputacija; *prieinamumo kokybės kategorija*, apimanti prieinamumo ir saugumo požymius; *kompleksinė kokybės kategorija*, jungianti relevantumą, pridėtinę vertę, atlikimą laiku ir išsamumą; *reprezentatyvumo kokybės kategorija,* pabrėžianti interpretavimo, nuoseklumo, suprantamumo ir glaustumo požymius (Wang, Strong, 1996). Taigi saugumas, vertinamas informacijos kokybės konteks-

te, išskiriamas kaip prieinamumo kokybės kategorijos sudedamoji dalis.

Informacijos saugumas taip pat išskiriama 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 atspindi strateginio požiūrio į informacijos vadybą svarbą – strateginis požiūris į informacijos vadybą leidžia organizacijoms 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 sudedamoji dalis turėtų būti ir informacijos saugumas (Detlor, 2010).

Informacijos saugumo dedamųjų galima aptikti ir analizuojant informacijos vadybos modelius. Kaip pagrindiniai išskirtini šie informacijos vadybos modeliai: Ch. Choo (2002) sudarytas informacijos vadybos procesinis modelis (2 pav.) bei T. Davenporto ir L. Prusako (1997) ekologinis informacijos vadybos modelis. Šių modelių kūrėjai tiesiogiai nepažymi informacijos saugumo kaip informacijos vadybos proceso ar dedamosios, tačiau gretinant Ch. Choo modelio aprašo teorinį konceptą su T. D. Wilsono išsakytų požiūriu, galima išskirti informacijos vadybos procesinio modelio informacijos sklaidos procesą (pažymėta pilka spalva 2 pav.). Šio proceso turinio apibrėžčiai Ch. Choo ir T. D. Wilsonas ryškina informacijos pateikimo reikiamam asmeniui, reikiama forma, reikiamu laiku svarbą, kas suponuoja būtinybę nustatyti tinkamus informacijos saugumo lygius konkrečiai informacijai bei užtikrinti atitinkamų prieigos teisių nustatymą ir valdymą (Choo 2002; Wilson 1997). Prieigos valdymas priskiriamas prie pagrindinių informacijos saugumo užtikrinimo priemonių, o informacijos saugumo tikslų (konfidencialumo, vientisumo ir prieinamumo) kontekste prieigos valdymas aktualiausias užtikrinant informacijos konfidencialumą, iš dalies ir vientisumą. Konfidencialumas itin svarbus, kad tik sankcionuoti (turintys leidimus) vartotojai galėtų prieiti prie informacijos. Vientisumas svarbus, kiek tai susiję su informacijos vartotojų teisių (pvz., informacijos



2 pav. ***Informacijos vadybos procesinis modelis (Choo, 2002)***

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.

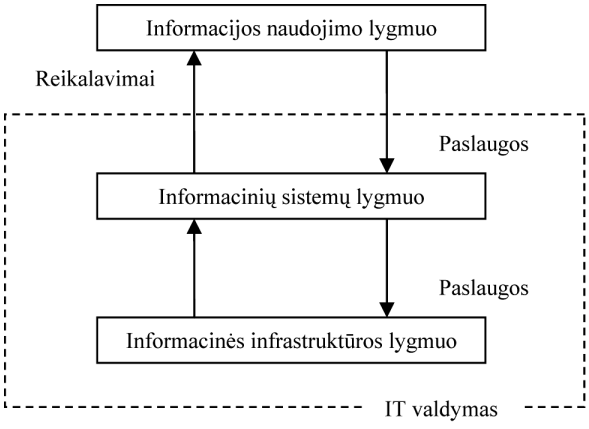
Apibendrinant saugumo paieškas informacijos vadybos teorinėse įžvalgose, galima teigti, kad nors ir fragmentiškai, tačiau saugumas tyrinėjamas kaip viena iš informacijos vadybos dalių. Informacijos vadybos teoretikai saugumą tiesiogiai įvardija kaip vieną iš informacijos vadybos tyrimo objektų, saugumas nagrinėjamas kaip sudėtinė informacijos kokybės, informacinės veiklos kompetencijos sudedamųjų dalių, labiausiai saugumas išryškinamas informacijos skaidos procesuose tyrinėjant, kaip naudojamos prieigos valdymo priemonės.

Vertinant mokslines diskusijas apie informacijos vadybos turinį, tikslinga išplėsti informacijos saugumo dedamosios paieškas į gimininga informacines vadybines koncepcijas – įrašų vadybą, informacinių išteklių vadybą, informacinių technologijų vadybą, duomenų vadybą, informacijos sistemų vadybą ir kt. Šiai tyrimo plėtotei vertinga pasiremti M. Wollniko sudarytu trijų lygių modeliu, susisteminusiu požiūrius į informacijos vadybą (3 pav.). Jame išskiriamas aukščiausias – informacijos vadybos lygmuo, vidurinysis – informacinių sistemų valdymo lygmuo ir žemiausias – informacinės infrastruktūros valdymo lygmuo, apimantis technologinį pagrindą (platformą), reikalingą aukštesniems lygmenims (Wollnik, 1988).

Identifikavus saugumo ir informacijos vadybos tarpusavio ryšį bei išryškinus informacijos saugumo tyrimų tendencijas (kaip aptarta straipsnyje, didžiausias techninių informacijos saugumo aspektų ištirtumas), tikėtina žemesniuose (labiau techniniuose) informacijos vadybos lygiuose rasti dar glaudesnių saugumo ir informacijos vadybos sąsajų.

Saugumas informacijos išteklių vadybos kontekste

Informacijos išteklių vadybos apibrėžtis nagrinėjo ir modelius sukūrė C. Burkas, D. Marchandas, F. Hortonas, N. Willard,



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

D. Skyrme'as, J. Hovenas, Z. Atkočiūnienė, L. Markevičiūtė ir kiti.

Kaip teigia A. Atkočiūnienė, tikslios ir vienareikšmiškos informacijos išteklių apibrėžties nėra, o išskiriant kokybinius informacijos apdorojimo lygmenis „duomenys–informacija–žinios", išteklius kaip informacija gali būti bet kuris iš jų (Atkočiūnienė, 2009). D. Marchando ir F. Hortono 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 valdyba remiasi informacijos vadyba (Marchand ir Horton, 1986).

Analizuojant saugumo vietą informacijos išteklių vadyboje, tikslinga ištirti pagrindinius informacijos išteklių vadybos modelius, taip pat analizei pasitelkti ir Lietuvos tyrėjų suformuotą bendrąjį informacijos išteklių vadybos modelį.

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

N. Willardas 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 informacijos ištekliais (Willard, 1993; 2003). Pastarasis rizikos elementas gali būti siejamas su saugumu ir yra aktualiausias jo kontekste.

Siekdamas efektyviai valdyti informacijos išteklius nemažai principų suformulavo D. Skyrme'as. 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 išorinės ir vidinės veiklos stebėseną, vertinti išteklius, kurie yra svarbūs organizacijos veiklai; pasirinkti tinkamas programines ir technines priemones vidinei ir išorinei 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 informacijos dalijimuisi kultūros kūrimąsi (Skyrme, 1999). Saugumo kontekste aktualiausias šio modelio informacijos valdymo politikos principas, apimantis informacijos vientisumo ir sklaidos aspektus.

J. Hovenas savo darbuose pabrėžia, kad glaudus sąryšis turi sieti organizacijos tikslus ir informacijos išteklių vadybos tikslus ir tai turėtų atsispindėti organizacijos verslo plane. Sėkmingai informacijos išteklių vadybai autorius išskiria šias veiklos sritis:

skatinti duomenų svarbos ir jų valdymo atsakomybės supratimą; siekti, kad visoje organizacijoje dalijantis duomenimis būtų naudojama bendra terminija, apibrėžimai 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.

Z. Atkočiūnienė ir L. Markevičiūtė, apibendrindamos informacijos išteklių teorinius tyrimus, atkreipė dėmesį, kad autoriai dažnai nesiekia apibrėžti viso informacijos išteklių komplekso, o akcentuoja ir analizuoja tik tam tikrus informacijos išteklių valdymo aspektus. Autorės, remdamosi N. Willardo, D. Skyrme'o, C. Burko ir F. Hortono bei 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 įvardijamas informacijos išteklių apsaugos aspektas.

Apibendrinant aptartus informacijos išteklių vadybos modelius informacijos saugumo tikslų – prieinamumo, vientisumo ir konfidencialumo kontekste, galima konstatuoti, kad informacijos išteklių saugumui dėmesio trūksta. C. Burko ir F. Hortono modelyje informacijos išteklių saugumas neminimas, D. Skyrme'as savo modelyje tik iš dalies paliečia informacijos vientisumo problematiką, Z. Atkočiūnienės ir L. Markevičiūtės ir papildytame N. Willardo modelyje minimi konfidencialumo ir prieinamumo aspektai. Galima išskirti J. Hoveno informacijos išteklių valdymo modelį, kuris tiesiogiai pamini visus tris informacijos saugumo aspektus – vientisumą, prieinamumą ir konfidencialumą (2 lentelė).

Vertinant informacijos išteklių vadybą, tikslinga pažymėti įrašų vadybos dedamąją. Įrašų vadybos tikslas yra koordinuoti įrašų valdymą per visą jų gyvavimo ciklą.

2 lentelė. ***Informacijos išteklių sąsajos su informacijos saugumo tikslais (sudaryta autoriaus)***

Informacijos išteklių vadybos modeliai / Informacijos saugumo tikslai	C. Burko ir F. Hortono modelis	N. Willardo modelis	D. Skyrme'o modelis	J. Hoveno modelis	Z. Atkočiūnienės ir L. Markevičiūtės modelis
Prieinamumas	-	+	-	+	+
Vientisumas	-	-	+	+	-
Konfidencialumas	-	+	-	+	+

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).

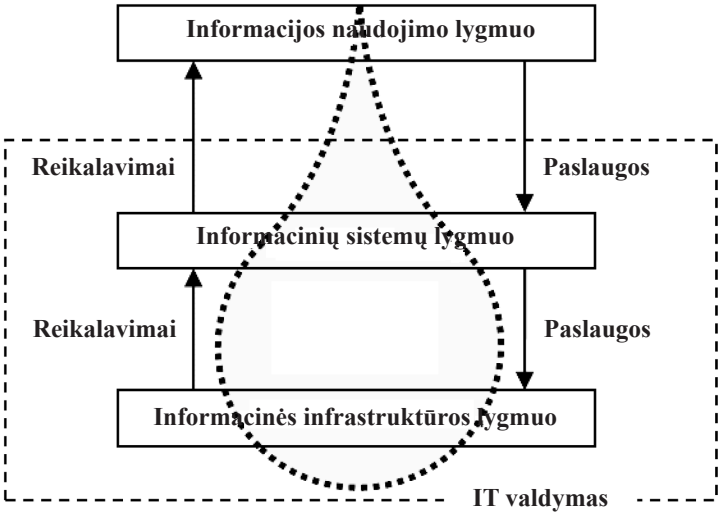
Remiantis A. Willis (2005) įžvalgomis, galima pažymėti, kad įrašų vadyba yra vienas pagrindinių organizacijų vadybos komponentų, ypač svarbus organizacijos atskaitomybei ir kasdieninei veiklai. Pagrįsdamas šiuos teiginius, jis išskyrė šešis įrašų ir informacijos vadybos komponentus, kurie svarbūs sėkmingai organizacijų vadybai – tinkamas procesas, skaidrumas, atskaitomybė, atitikimas, teisėtumas, saugumas. Taigi, organizacijos turi rūpintis visos organizacijos informacijos, kartu ir visų įrašų, tinkama apsauga, tokia funkcija turi būti aiškiai priskirta atsakingiems žmonėms bei užtikrinta tinkama funkcijos vykdymo kontrolė. P. Emery (2003), nagrinėdama įrašų vadybos turinį, pažymėjo, kad įrašų saugumui dažnai naudojamos vaidmenimis grįstos prieigos teisės, taip pat akcentavo saugų įrašų naikinimą jų gyvavimo ciklo pabaigoje. Organizacijos valdomos informacijos netinkamas atskleidimas gali pažeisti privatumo, konfidencialumo ar kitus teisinius reikalavimus, o informacijos praradimas – lemti organizacijos sukauptų žinių, intelektinės nuosavybės ar konkurencinio pranašumo praradimą (Willis, 2005; Lomas, 2010).

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

Saugumas informacijos vadybos mokslų teorinių įžvalgų aprėptyje

Išanalizavus informacijos vadybos, informacijos išteklių vadybos ir gimininga informacijos vadybos mokslų koncepcijas galima teigti, kad šiuo metu daugiausia dėmesio saugumui skiria informacijos vadybos disciplinos ir atitinkami moksliniai tyrimai, kuriuose ryškinamas technologinis informacijos valdymo aspektas, – įrašų vadyba ir informacijos išteklių vadyba. Galima konstatuoti, kad informacijos saugumo prieinamumo ir konfidencialumo tikslai glaudžiai integruoti informacijos įrašų vadyboje, o visi trys informacijos saugumo tikslai ryškinami informacijos išteklių vadybos moksliniuose tyrimuose.

Įvertinus aptartas mokslines įžvalgas, galima daryti išvadą, kad saugumas nėra plačiai tirtas informacijos vadybos mokslų kontekste. Nustatytos saugumo sąsajos su informacijos vadybos tyrimų objektu, informacijos vadybos procesais, informacinėmis technologijomis ir sistemomis bei informacijos vadybos kompetencijomis. Kokybiška informacija taip pat turi atitikti informacijos saugumo valdymo tikslus. Informacijos saugumo sąsajos su M. Wollniko (1988) trijų lygių informacijos vadybos modeliu pavaizduotos 4 paveiksle. 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.



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

Išanalizavus informacijos vadybos teoretikų tyrimus ir konstatavus nepakankamą jų sąsajumą su informacijos saugumo turiniu, galima išryškinti didelę mokslinių tyrimų spragą. Mokslinėse įžvalgose, akcentuojant informaciją kaip kritinį organizacijų išteklių ir esminį konkurencinį pranašumą, menkas informacijos vadybos teoretikų dėmesys šio išteklius saugumui užtikrinti tampa aktualia moksline problema. Moksliškai neįtvirtintas informacijos saugumo valdymas lemia ir praktinio lygmens problemas.

Informacijos vadybos įrankiai informacijos saugumui valdyti

Straipsnyje formuluojant esminę mokslinę prielaidą, kad informacijos saugumas turėtų būti sudedamoji informacijos vadybos dalis, tikėtina, kad informacijos saugumui valdyti turėtų būti pasitelkti ir informacijos vadybos įrankiai. Siekiant pagrįsti šią prielaidą, nagrinėjami pagrindiniai informacijos vadybos įrankiai bei, gretinant jų apibrėžtis su informacijos saugumo valdymo turiniu, teoriniu lygmeniu patikrinama galimybė juos taikyti efektyviam informacijos saugumo valdymui užtikrinti.

Pagrindiniai informacijos vadybos įrankiai

Informacijos vadybos įrankius, jų apibrėžtis ir svarbą nagrinėjo D. Chaffey, S. Wood, C. Schlöglis, Ch. Choo, D. Skyrme'as, M. J. Earl, E. Orna, T. H. Davenportas, T. D. Wilsonas ir kiti. Apibendrinant šių informacijos vadybos mokslininkų įžvalgas pagrindiniais informacijos vadybos įrankiais įvardytina informacijos politika, informacijos strategija, 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, Boon, 2003; Orna, 2004). Informacinių procesų nenutrūkstamas ciklas ir aplinkos komponentų analizė leidžia organizacijai prisitaikyti prie besikeičiančios aplinkos ir koordinuotai įgyvendinti užsibrėžtus tikslus (Choo, 2002; Davenport ir Prusak, 1997), informacijos kokybės valdymas užtikrina, kad organizacija valdo vertingą, organizacijos lūkesčius atitinkančią ir pridėtinę vertę kuriančią informaciją (English, 2004).

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.

Informacijos politika ir strategija

Svarbiausias informacijos politikos tikslas – pateikti pagrindinių principų sąrašą, kuris leistų įvertinti informacijos reikšmę ir vienareikšmiškai ją sieti su organizacijos tikslais ir prioritetais. Informacijos valdymas visų pirma priklauso nuo organizacijoje vyraujančios informacinės politikos modelio (Davenport, Eccles, Prusak, 1992; Davenport ir Prusak, 1997), o pati informacijos politika glaudžiai siejasi su informacijos strategija, kuri užtikrina kryptingą informacijos politikos įgyvendinimą. Remiantis teoriniais tyrimai 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, kontroliavimą, žmonių ir technologijų koordinavimą (Chaffey ir White, 2011).

Vertinant informacijos politikos ir strategijos įrankių reikšmingumą informacijos saugumo valdymo kontekste, galima identifikuoti šių įrankių sąsajas su informacijos saugumo valdymo politika ir jos nustatomais informacijos saugumo tikslais – konfidencialumu, vientisumu ir prieinamumu. Politika, remiantis bendrais organizacijos tikslais, turi apibrėžti 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 padeda koordinuoti organizacijoje vykdomas veiklas, nustatyti politikos įgyvendinimo kryptis, priemones ir atsakomybes.

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 konkre-

taus audito komandą – vidinius ar išorinius auditorius. Nėra visuotinai pripažinto informacijos audito proceso modelio, tačiau remiantis minėtų tyrėjų įžvalgomis galima apibendrintai identifikuoti bendrus informacijos audito proceso etapus: tai 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, šio įrankio taikymas leidžia įvertinti, ar tinkamai funkcionuoja kontrolės sistema, turinti užtikrinti informacijos saugumo strategijoje numatytų priemonių įgyvendinimą, ar pasiekti numatyti rezultatai, ar šie rezultatai siekiami mažiausiomis sąnaudomis. Auditas taip pat leidžia įvertinti, ar tinkamai pasirinkta ir pati informacijos saugumo politikos tikslų įgyvendinimo strategija.

Informacijos procesai ir aplinka

Sėkmingam informacinių procesų vykdymui bei informacijos valdymui atsiranda vis daugiau informacijos valdymo sistemų. Siekiant užtikrinti organizacijos prisitaikymą prie besikeičiančios aplinkos, reikėtų taikyti Ch. Choo (2002) pasiūlytą procesinį informacijos modelį, kuriame pateikiamas nenutrūkstamas ir glaudžiai susijusių veiklų (informacijos poreikių identifikavimas, informacijos įgijimas, informacijos organizavimas ir saugojimas, informacijos produktų ir paslaugų vystymas, informacijos sklaida ir informacijos naudojimas) ciklas, ir T. Davenporto bei L. Prusako (1997) 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 informacinės (strategija, procesai, politika, architektūra, darbuotojai, kultūra ir elgsena) aplinkos komponentai.

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. Akivaizdu, kad siekiant tinkamai valdyti informacijos saugumą, jis turi būti integruotas į visus informacijos vadybos procesus bei informacijos aplinkų dedamąsias.

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, atlikimo laiku, išsamumo, viena-

reikšmiškumo, 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 įvardijami 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 organizacijos informacijos kokybės valdymu.

Aptartų informacijos kokybės ir brandos lygių turinį atskleidžia akivaizdus jų sąsajumas su informacijos saugumo brandos lygiais. Organizacijos brandos lygis lemia tiek informacijos vadybos, tiek informacijos saugumo valdymo kokybę. Vertėtų išryškinti organizacijos brandos lygio ir taikomų vadybos priemonių priklausomybę, t. y. pagal organizacijos brandos lygį turėtų būti parenkami atitinkami vadybos metodai. Aukštesnės brandos organizacijos, kurios supranta ir turi patirtį taikyti tiek informacijos vadybos, tiek ir informacijos saugumo valdymo metodus, gali taikyti vis sudėtingesnius vadybos metodus ir užtikrinti informacijos kokybę, ir priešingai – menkos brandos organizacijoms sudėtingi valdymo metodai numatomos naudos neduos.

Informacijos vadybos įrankių informacijos saugumui valdyti analizės apibendrinimas

Išanalizavus pagrindinių informacijos vadybos įrankių turinį bei sąsajas tarp informacijos vadybos bei informacijos saugumo valdymo problematikos, 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 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 paties audito proceso (planavimo, duomenų rinkimo, duomenų analizės ir įvertinimo, rekomendacijų pateikimo ir jų įgyvendinimo) 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, sykiu ir į informacijos saugumą. Čia galima daryti sąsajas su straipsnyje aptarta įžvalga, kad tik saugi ir patikima informacija gali būti pavadinta kokybiška. Organizacijos branda taip pat sietina su organizacijos sugebėjimu taikyti pažangias valdymo priemones, užtikrinti visų informacijos procesų saugumo valdymą bei nepavėluotą 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 ir yra aukštas informacinės brandos lygis, galima pagrįstai tikėtis, kad bus užtikrintas ir informacijos saugumo valdymas.

Įvertinus informacijos saugumo valdymo objektą, tikslus ir dimensijas, pagrindiniais informacijos saugumo valdymo įrankiais 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 teoriniu ir praktiniu lygmeniu galėtų būti nagrinėjamas kaip pasiūlymai gerinti informacijos saugumo valdymo brandą ir kokybę.

Integralus informacijos saugumo valdymo modelis

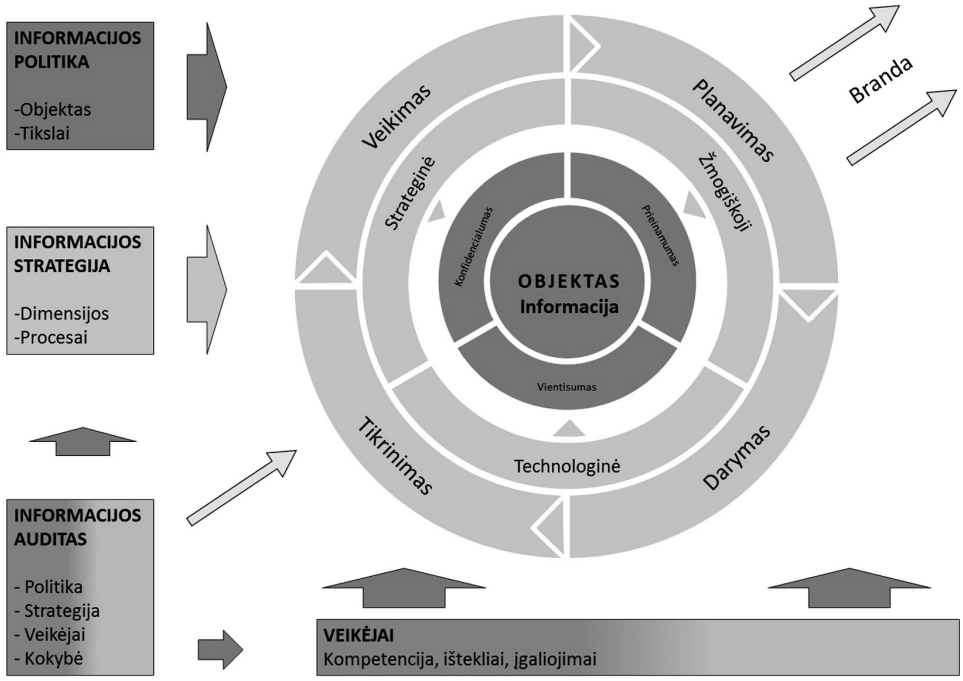
Atlikus informacijos saugumo ir informacijos vadybos diskursų tyrimą, suformuluoti informacijos saugumo valdymo turinio elementai – objektas, tikslai ir dimensijos, bei aptarti pagrindiniai informacijos vadybos įrankiai – informacijos politika, informacijos strategija ir informacijos auditas.

Ištyrus teorinius konceptus ir pagrindus, informacijos saugumo valdymo ir informacijos vadybos sąsajumą, galima gretinti informacijos saugumo valdymo turinio elementus su informacijos vadybos įrankiais. Remiantis atskleista šių abiejų diskursų sudedamųjų dalių apibrėžtimi galima jungti šių diskursų *politikos lygmenį*, kuriame nustatomi tikslai ir pagrindiniai principai, t. y. informacijos saugumo objektas (informacija) ir tikslai (konfidencialumas, vientisumas ir prieinamumas). *Strategijos lygmuo* jungia 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 straipsnyje 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) suteikimas. Kokybės (brandos) kėlimas įvardytinas kaip antrasis procesų tobulinimą įgalinantis veiksnys. *Audito lygmuo* leidžia įvertinti ir šiuos įgalinančius veiksnius.

Integralus teorinis informacijos saugumo valdymo modelis, jungiantis aptartą informacijos valdybos mokslų ir informacijos saugumo valdymo sąsajumą, pateikiamas 5 paveiksle.

Modelio centre pavaizduotas informacijos saugumo objektas – informacija. Pir-



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

masis modelio žiedas iliustruoja informacijos saugumo tikslus. Šias modelio dedamąsias jungia informacijos politikos įrankis ir apibrėžia, *kas* turėtų būti saugoma (modelyje išskirta tamsiai pilka spalva). Antrasis žiedas iliustruoja informacijos saugumo dimensijas, trečiasis – procesus. Šias modelio dedamąsias jungia informacijos strategijos įrankis ir nusako, *kaip* turėtų būti saugoma (modelyje išskirta šviesiai pilka spalva). Informacijos audito įrankis leidžia patikrinti politikos ir strategijos išsamumą bei įvertinti, *ar yra* kitos prielaidos informacijos saugumui valdyti, t. y. ar paskirti veikėjai (suteikti ištekliai ir kompetencijos), ar užtikrinama veiklos kokybė.

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.

Išvados

Vyraujančių informacijos saugumo valdymo priemonių turinys asimiliuojasi, šalia technologinių sprendinių taikymo problematikos ryškėja aktualūs žmogiškieji, ekonominiai ir kiti aspektai, kyla platesnio vadybinio požiūrio poreikis ir tampa akivaizdu, kad esamos informacijos saugumo valdymo priemonės nebėra pakankamos informacijos saugumui valdyti.

Informacinių technologijų svarba informacijos tvarkymui yra neabejotina, tačiau informacijos saugumo valdymo objektu išgryninus informaciją, susidaro prielaidos ieškoti naujų informacijos saugumo valdy-

mo priemonių tarp informacijos vadybos įrankių.

Išanalizavus informacijos vadybos tyrėjų įžvalgas, konstatuota, kad saugumo dedamoji informacijos vadyboje nėra išplėtota. Mokslinėse įžvalgose, akcentuojant informaciją kaip kritinį organizacijų išteklių, menkas informacijos vadybos teoretikų dėmesys šio ištekliaus saugumui užtikrinti tampa aktualia moksline problema, o moksliškai neįtvirtintas informacijos saugumo valdymas lemia ir praktinio lygmens problemas.

Įvertinus pagrindinius informacijos vadybos įrankius informacijos saugumo valdymo kontekste, identifikuota šių įrankių vertė valdant informacijos saugumą. Šios analizės rezultatai leido sumažinti mokslinių tyrimų spragą ir parodyti teorinį mokslinės problemos sprendimą žvelgiant į informacijos saugumo valdymo problemą informacijos vadybos kontekste. Straipsnyje aptartų tyrimų rezultatai sukūrė teorinį pagrindą suformuoti integralų informacijos saugumo valdymo modelį. Šis modelis integruota ir išplėtota saugumo dedamąja praplėtė informacijos vadybos ribas.

Tikėtina, kad teorinis integralus informacijos saugumo valdymo modelis gali būti taikomas tiek teoriniu, tiek praktiniu lygmeniu. Modelio praktiniam pritaikomumui informacijos saugumo valdymui vertinti tikslinga atlikti tolesnius tyrimus, o šių tyrimų rezultatai bus pateikiami kitame straipsnyje.

LITERATŪRA IR ŠALTINIAI

ABELS, Eileen; JONES, Rebecca; LATHAM, John; MAGNONI, Dee; MARSHALL, G. Joanne (2003) Competencies for Information Professionals of the 21st Century [interaktyvus]. [žiūrėta 2012 m. gegužės 14 d.]. Prieiga per internetą: <http://www.sla.org/PDFs/ Competencies2003_revised.pdf>.

ASHENDEN, Debi (2008). *Information Security management:* A human challenge?

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

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

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

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.

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

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

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

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

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

CHOO, Chun Wei (2008). *Information Management* [interaktyvus]. [žiūrėta 2012 m. kovo 5 d.]. Prieiga per internetą: <http://choo.fis.utoronto.ca/Imfaq/>.

CHOO, Chun Wei (2002). *Information management for intelligent organisation: the art of scanning*

the environment. Medford: Information Today, Inc. 325 p.

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>.

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

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

Defence in depth. Summary Report for CIOs and CSO (2008). [interaktyvus]. [žiūrėta 2012 m. gegužės 7 d.]. Prieiga per internetą: <http://tisn.gov.au/www/tisn/content.nsf/Page/ Publications_PublicationsbyTopic>.

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

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

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

EMERY, Priscilla (2003). Document and Records Management: Understanding The Diferences and Embracing Integration [interaktyvus]. [žiūrėta 2012 m. birželio 5 d.]. Prieiga per internetą: <http://www.zylab.com/downloads/whitepapers/White%20Paper%20-%20Document%20 Management%20vs%20Records%20Management.pdf>.

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

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 >.

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

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

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

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

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

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

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

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

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

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

MARCHAND, D., HORTON, F. (1986). *Infotrends*: *Profiting from Your Information Resources*. New York: John Wiley and Sons. 342 p.

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

McLEAN, John. *Security Models and Information Flow* [interaktyvus]. [žiūrėta 2012 m. liepos 15 d.]. Prieiga per internetą: <http://www.cs.cornell.edu/andru/cs711/2003fa/reading/ 1990mclean-sp.pdf>.

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

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

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

PARKER, B. Donn (1998). *Fighting computer crime*: *A new framework for protecting information*. New York, USA: John Wiley & Sons, Inc. 528 p.

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

SKYRME, David (1999). *Information resource management. Insight* [interaktyvus]. [žiūrėta 2012 m. birželio 1 d.]. Prieiga per internetą: <http://www.skyrme.com/insights/8irm.htm>.

ŠTITILIS, Darius, PAŠKAUSKAS, Žydrunas. (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.

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

VODACEK, Leo. *Information Management*: *Concept, Teaching, Applications* [interaktyvus]. [žiūrėta 2012 m. liepos 13 d.]. Prieiga per internetą: <http://www.informationswissenschaft.org/download/isi1998/4_isi98-dv-vodacek-prag.pdf>.

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

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.

WANG, Y. Richard; STRONG, M. Diane (1996). Beyond accuracy: What data means to data customers. *Journal of Management Information Systems*, vol. 2, p. 210–232.

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

WILLARD, Nick (1993). Information Resources Management. *Aslib Information*, vol. 21 (5).

WILLARD, Nick (2003). *The Willard Model of IRM* [interaktyvus]. [žiūrėta 2012 m. birželio 1 d.]. Prieiga per internetą: <http://www.skyrme.com/kmroadmap/willard.htm>.

WILLIS, Anthony (2005). Corporate governance and management of information and records. *Records Management Journal*, vol. 15 (2), p. 86–97.

WILSON, D. Tom (1997). Information management. In *International Encyclopedia of Information and Library Science*. London: Routledge, p. 187–196.

WOLLNIK, Michael (1988). Ein Referenzmodell des Informationsmanagements. *Information Management*, vol. 3, p. 34–43.

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.

ZELTSER, Lenny; KENT, Karen; NORTHCUTT, Stephen; RITCHEY, W. Ronald; WINTERS, Scott (2005). *Perimeter Security Fundamentals* [interaktyvus]. [žiūrėta 2012 m. birželio 28 d.]. Prieiga per internetą: <http://www.informit.com/articles/article.aspx?p=376256>.

XIAOMI, An (2003). An integrated approach to records management. *The Information Management Journal*, vol. 37 (4), p. 24–30.

INTEGRAL INFORMATION SECURITY MANAGEMENT MODEL

Saulius Jastiuginas

S u m m a r y

Analysis of the currently most widely applied means of information security management (methodologies, standards, models) allows finding a growing assimilation of media content, but the frequent information security problems (for example, information security incident growth), show that the existing measures do not provide sufficient information security management.

The analysis of information security research problems shows that the main object is to protect the information, but it often becomes the subject of security information technology or information systems that support information processing.

A substantial scientific assumption is that the primary object of information security is information, it is likely that information security should be studied as an integral part of information management and the other related concepts (information resource management, information systems management, information, records management).

The analysis of the information management has shown that the security component of informa-

tion management is not developed. Scientific insight, emphasizing information as a critical resource organization, poor information management, focus on the resource security becomes a relevant scientific problem and do not provide scientific information security management problems that are apparent on the practical level.

The aim of the study was to create a scientific basis for the integral management of information security model that integrates information security management and information management components.

The paper deals with the basic information management tools and practices of information security management possibilities. The results of the analysis helped to reduce the gap in research and to develop a theoretical basis for the integral form of information security management model.

The proposed theoretical model and the integrated security information management component extend the possibilities of secure information management.

The aim of the article was to create a scientific basis for the integral model of information security management that integrates information security management and information management components.

The paper analyzes the main information management tools and opportunities to use them for information security management. The results of the analysis helped to reduce the gap in scientific research and to develop a theoretical basis for the integral information security management model.