ISSN 1392-6195

JURISPRUDENCIJA
Mokslo darbai
2007 2(92); 37–45

VALSTYBĖS ELEKTRONINĖS INFORMACIJOS SAUGOS STRATEGIJA – VIENAS IŠ PAGRINDINIŲ ELEKTRONINĖS INFORMACIJOS SAUGOS REGULIAVIMO INSTRUMENTŲ: LYGINAMOJI ANALIZĖ

Darius Štitilis *
Žydrūnas Paškauskas **

Mykolo Romerio universiteto Ekonomikos ir finansų valdymo fakulteto Informatikos ir statistikos katedra
Ateities g. 20, LT-08303 Vilnius
Telefonas 234 75 76
Elektroninis paštas infdep@mruni.lt

Pateikta 2006 m. rugsėjo 25 d., parengta spausdinti 2007 m. sausio 26 d.

Santrauka. Straipsnyje nagrinėjamos elektroninės informacijos saugos reguliavimo srityje lyderiaujančių Europos valstybių elektroninės informacijos saugos strategijos lyginant jas su naująja Lietuvos elektroninės informacijos saugos strategija.

Straipsnio objektas – elektroninės informacijos saugos reguliavimas, kurio vienas iš pagrindinių elementų – elektroninės informacijos saugos strategija. Straipsnio tikslas – lyginamuoju aspektu išnagrinėti kai kurias pažangiausias Europos valstybių valstybines elektroninės informacijos saugos strategijas bei pateikti Lietuvos elektroninės informacijos saugos strategijos lyginamąjį įvertinimą, taip pat atitinkamus pasiūlymus dėl elektroninės informacijos saugos reguliavimo. Straipsnyje taikomas lyginamasis, analizės ir kiti metodai. Analizuojant ES valstybių elektroninės informacijos saugos strategijas naudojamasi užsienio valstybių teisinių dokumentų duomenų bazėmis bei periodine literatūra.

Straipsnį sudaro dvi dalys. Pirmoje dalyje lyginamuoju aspektu nagrinėjamos Norvegijos, Suomijos bei Čekijos informacijos saugos strategijos, antroje lyginamuoju aspektu analizuojama naujoji Lietuvos elektroninės informacijos saugos strategija, keliamos egzistuojančios elektroninės informacijos saugos reguliavimo Lietuvoje problemos. Atlikta analizė leidžia teigti, kad naujoji Lietuvos elektroninės informacijos saugos strategija, nors priimta 2006 m., ne visiškai atspindi kai kuriuos pagrindinius elektroninės informacijos saugos reguliavimo principus ir yra tobulintina. Straipsnyje pateikiamos Lietuvos elektroninės informacijos saugos strategijos tobulinimo kryptys, priemonės, taip pat pasiūlymai dėl elektroninės informacijos saugos reguliavimo Lietuvoje tobulinimo.

Pagrindinės sąvokos: elektroninės informacijos saugos reguliavimas, elektroninės informacijos saugos strategija.

ĮVADAS

Šiandien informacinių technologijų ir tinklų plėtrą lemia rinkos poreikiai. Egzistuoja daugybė veiksnių, kurie lyg ir leidžia teigti, kad šalių vyriausybės turi teisę aktyviai veikti šioje visuomeninių santykių srityje, tačiau kartu egzistuoja tam tikri vyriausybės veiksmų ribų apribojimai. Todėl, autorių nuomone, vyriausybės politika turi būti labai gerai sukurta ir gebėti įsisavinti esmines nacionalines bei tarptautines iniciatyvas šioje visuomeninių santykių srityje per pastaruosius kelerius metus.

Valstybės elektroninės informacijos saugos strategija, priskirtina informacijos saugos politikos dokumentams, gali būti išskirta kaip vienas iš pagrindinių elektroninės informacijos saugos reguliavimo teisinių dokumentų [1, p. 36]. Šis dokumentas ne tik įvardija pagrindines elektroninės informacijos saugos problemas, bet ir numato svarbiausias elektroninės informacijos saugos užtikrinimo kryptis bei būdus. Elektroninės informacijos saugos strategijos dažniausiai būna įtvirtinamos nacionalinių valstybių teisės aktais, šios strategijos taip pat

* Mykolo Romerio universiteto Ekonomikos ir finansų valdymo fakulteto Informatikos ir statistikos katedros docentas.
** Mykolo Romerio universiteto Ekonomikos ir finansų valdymo fakulteto Informatikos ir statistikos katedros doktorantas.

turi tiesioginę įtaką kuriant naujus ir tobulinant jau priimtus elektroninės informacijos saugą reglamentuojančius teisės aktus. Remiantis elektroninės informacijos saugos strategijomis atskirose valstybėse įgyvendinama bendroji elektroninės informacijos saugos reguliavimo politika, kuri tampa vis svarbesne šiuolaikinės žinių visuomenės kontekste.

Kai kurios Europos valstybės elektroninės informacijos saugos reguliavimo srityje turi daug didesnę nei Lietuva patirtį. Elektroninės informacijos saugos reguliavimo srityje pažangiausiomis Europos valstybėmis galima įvardyti Suomiją, Norvegiją, Čekiją. Visos šios valstybės turi patvirtintas elektroninės informacijos saugos valstybines strategijas, užtikrinančias elektroninės informacijos saugos reguliavimo tęstinumą. Šiose strategijose perimta ES, Europos bendradarbiavimo ir plėtros organizacijos (toliau – EBPO) ir kita informacijos saugos reguliavimo patirtis. Todėl šių valstybių patirtis labai svarbi Lietuvoje gerinant elektroninės informacijos saugos reguliavimą ir kartu saugos užtikrinimą.

Lietuva elektroninės informacijos saugos reguliavimo prasme neturi tokių senų tradicijų kaip minėtos Europos valstybės. Lietuvoje naujoji elektroninės informacijos saugos strategija priimta tik 2006 m. Toliau einanti kai kurių valstybių strategijų lyginamoji analizė padės konstruktyviau, objektyviau įvertinti Lietuvos informacijos saugos valstybės institucijų informacinėse sistemose strategiją bei numatyti šios strategijos tobulinimo būdus ir priemones. Nors Lietuva neturi visas sritis apimančios informacijos saugos strategijos, o nagrinėtina strategija skirta tik valstybės institucijų sektoriui, minėtų strategijų analizė padės įvertinti ir bendrosios Lietuvos informacijos saugos strategijos reikalingumą.

1. KAI KURIŲ EUROPOS VALSTYBIŲ ELEKTRONINĖS INFORMACIJOS SAUGOS STRATEGIJOS – LYGINAMASIS ASPEKTAS

1.1. Norvegijos nacionalinė informacijos saugos strategija

Norvegijos nacionalinė informacijos saugos strategija (toliau – Norvegijos strategija) priimta 2003 m. birželį [2]. Bendrasis Norvegijos strategijos tikslas – sumažinti informacinių sistemų pažeidžiamumą ir padidinti elektroninių komunikacijų bei informacinių technologijų konfidencialumą [3, p. 17]. Pagrindiniai Norvegijos strategijos tikslai:

1. užtikrinti vienodą požiūrio į informacijos saugą, kuri yra tolesnės darnios politikos kūrimo pagrindas, formavimą;
2. skatinti, kontroliuoti ir koordinuoti valstybės institucijų, dalyvaujančių kuriant valstybės politiką šioje srityje, veiksmus.

Pagrindinės Norvegijos strategijos veiklos kryptys: mažinti kritiškai svarbios infrastruktūros (kaip, beje, ir visų informacinių technologijų (toliau – IT)) pažeidžiamumą bei lengvinti saugaus e. verslo tarp viešojo ir privataus sektoriaus bei saugių ir patikimų e. valdžios paslaugų plėtrą.

Norvegijos vyriausybė išskyrė 4 pagrindinius objektus, reikšmingus visuomenei informacijos saugos srityje:

1. Kritiškai svarbi keitimosi informacija infrastruktūra turi būti saugi, dinamiška ir atspari jai gresiančioms grėsmėms. Kritiškai svarbios informacinės sistemos turi būti saugios iki tokios lygio, kad atsižvelgiant į joms gresiančius informacijos saugos incidentus žala neviršytų „prieinamos rizikos“.
2. Saugos kultūra turi būti kuriama atsižvelgiant į ypatumus, pagal kuriuos projektuojamos ir plėtojamos informacinės sistemos ir keičiamasi elektronine informacija Norvegijoje. IT sauga turi būti pagrindinis veiksnys, kai kalbama apie IT naudojimą Norvegijos versle ir tarp vartotojų.
3. Turi būti plačiai prieinamos elektroninio parašo, elektroninių ryšių partnerių autentifikavimo ir „jautrios“ informacijos perdavimo infrastruktūros.
4. Reguliavimas informacijos saugos srityje turi būti įgyvendinamas ir toliau plėtojamas koordinuotai, atvirai ir suprantamai.

Norvegijos vyriausybės nuomone, šie įgyvendinti veiksniai informacijos saugos srityje lems didesnį, o kartu ir saugesnį interaktyvių paslaugų plitimą ir naudojimą. O tai savo ruožtu vėl skatins imtis priemonių kritiškai svarbiai infrastruktūrai apsaugoti.

Norvegijos strategijoje pabrėžiama, kad vyriausybė yra pagrindinis ir svarbiausias veiksnys kuriant tokią aplinką, tačiau atsakomybe turi dalintis ir kitos šalys ypatingais klausimais, susijusiais su IT saugos klausimų skleidimu ir supratimu. Vyriausybė taip pat turi inicijuoti dialogą su privačiu sektoriumi.

Kaip teigiama Norvegijos strategijoje, privalu atsižvelgti į specialius reikalavimus, keliamus duomenims bei juos apdorojančioms informacinėms sistemoms. Kiekvienu tokiu atveju turi būti aiški „prieinama rizika“. IT sistemos ir jose tvarkoma informacija turi būti skirstomos atsižvelgiant į gresiančių grėsmių veiksnį ir į tai, kokios svarbos sistema ir joje tvarkoma informacija yra asmenims, įstaigai, visai visuomenei arba valstybei. Todėl kritiškai svarbios valstybės informacinės sistemos turi būti apsaugotos tik valstybės sertifikuotais saugos sprendimais. Tokios sistemos bei jose tvarkoma informacija turi būti klasifikuojamos atsižvelgiant į tai, kiek sistema arba informacija yra kritiškai svarbi organizacijai ar visuomenei, ir į egzistuojančias grėsmes. IT sistemos ir infrastruktūra gali būti pripažinta kritiškai svarbia visuomenei, jei tos pačios visuomenės, atskirų valstybės įstaigų, organizacijų ar asmenų veikla gali būti pažeidžiama sutrikus tokios sistemos normaliam darbui. Tokiu atveju ypač svarbu nustatyti tokias sistemas ir įvertinti jų patikimumą pagal kritiškumo skalę. Organizacijose saugos priemonės turi būti naudojamos atitinkamai pagal nustatytus ir įvertintus rizikos veiksnius. Organizacijos sauga turi apimti ir fizinius, ir loginius, administracinius, ir teisinius lygius bei priemones. Turbūt tinkamomis priemonėmis reikėtų laikyti geros praktikos kodeksų pritaikymą organizacijos veikloje siekiant

užtikrinti kritiškai svarbios informacijos ir infrastruktūros patikimumą, atsparumą ir apsaugą. Šiuo tikslu, vadovaujantis tarptautinėmis metodikomis, geraja praktika ir standartais, turi būti kuriami nacionaliniai IT sistemų ir informacijos klasifikavimo standartai, IT sistemų ir informacijos kategorijų schemos, taikytinos ir viešajam, ir privačiam sektoriams.

Norvegijoje šiai strategijai prižiūrėti ir įgyvendinti prie Gynybos ministerijos įsteigta Norvegijos nacionalinė saugos valdyba. Ši valdyba patvirtino nacionalinių saugos produktų akreditavimo tvarką pagal SERTIT schemą, kuri parengta vadovaujantis Bendraisiais reikalavimais, keliamais IT saugai (angl. *Common Information Technology Security Evaluation Criteria*).

Norvegijos strategijoje numatyta sukurti Informacijos saugos centro bandomąjį projektą, skirtą visapusiškam pažinimui apie IT, informacijos saugos grėsmes, kontrpriemones bei ryšių su užsienio valstybėmis užmezgimu ir bendradarbiavimu.

Atkreiptinas dėmesys, kad Norvegijos strategija yra sukurta atsižvelgiant į EBPO 2002 m. EBPO Informacinių sistemų ir tinklų saugumo gaires [4]. Ši rekomendacija nustato pagrindinius tolesnės informacinių sistemų plėtros principus, rekomenduoja valstybėms narėms imtis tam tikrų priemonių, procedūrų, kad būtų įgyvendinti informacinių sistemų saugos principai.

2005 m. priimtame teisės akte „e. Norvegija 2005“[1] išdėstyta pozicija, kad vyriausybė, siekdama nustatyti saugumo nuostatų įgyvendinimą ne tik valstybiniame, bet ir privačiame sektoriuje, turi peržiūrėti teisės aktus (įskaitant ir strategiją) [3, p. 15]. Todėl galima įžvelgti tendenciją, jog elektroninės informacijos sauga tam tikra prasme pradedama reguliuoti ir privačiame sektoriuje, kuris, beje, darosi vis labiau susijęs su valstybės informacinėmis sistemomis.

1.2. Suomijos nacionalinė informacijos saugos strategija

Suomijos nacionalinė informacijos saugos strategija (toliau – Suomijos strategija) priimta 2003 m. rugsėjo 4 d. [5]. Pasiūlymus dėl šiaos strategijos suformulavo Informacijos saugos patariamoji valdyba (angl. *Information Security Advisory Board*), kuri buvo tam specialiai sukurta 2001–2003 m. Suomijos strategijos projektas parengtas Transporto ir Komunikacijų ministerijos. Suomijos strategija sulaukė dėmesio ne tik Suomijoje, bet ir tarptautiniu mastu [6, p. 4]. Todėl Suomijos valstybė rekomenduoja ES valstybėms narėms pasirinkti jos informacijos saugos koordinavimo modelį kaip pavyzdinį [7].

Suomijos strategija skatina ir prisideda prie saugios informacinės visuomenės kūrimo Suomijoje. Pagrindiniai Suomijos strategijos numatyti tikslai, uždaviniai ir įgyvendintinos priemonės, susijusios su elektroninės informacijos saugos reguliavimu:

1. *Skatinti bendradarbiavimą IT saugos klausimais nacionaliniu ir tarptautiniu lygiu*. Suomijos strategijoje numatyta patvirtinti nuolatinę Nacionalinę informacijos saugos patarėjų tarybą (angl. *Information Security Advisory Board*) (toliau – Taryba), kuri padės derinti ir įgyvendinti Suomijos strategijoje numatytas priemones, prižiūrės, kaip Suomijos strategija įgyvendinama, bei teiks pasiūlymus Vyriausybei dėl Suomijos strategijos keitimo arba atnaujinimo. Pasiūlymuose Suomijos strategijai priimti buvo numatyta ir išplėstinės Tarybos funkcijos bei įgaliojimai (pasiūlymai dėl šios strategijos buvo priimti Suomijos vyriausybės sudaryto Informacijos saugos patarėjų komiteto 2002 m. lapkričio 25 d.) [8]. Kadangi vyriausybė, Suomijos strategijos leidėja, yra atsakinga už joje numatytų tikslų ir priemonių įgyvendinimą, Taryba privalo periodiškai atsiskaityti vyriausybei. Ji veikia kaip plataus masto forumas, skirtas pačių įvairiausių subjektų IT saugos srityje bendradarbiavimui užtikrinti ir pagerinti. Taryba taip pat gali steigti darbo grupes atskiriems projektams, darbams ar tyrimams vykdyti. Tam, kad Suomijos strategijoje numatytos priemonės būtų įgyvendintos, rekomenduojama, kad Taryba galėtų tęsti savo darbą nepriklausomai nuo politinių pokyčių Parlamente ir Vyriausybėje, t. y. daugiau nei vieną politinę kadenciją. Labai svarbus aspektas vykdant informacijos technologijų saugą – Suomijos strategijos įgyvendinimo kontrolė. Suomijos strategijoje numatytos informacijos technologijų saugos užtikrinimo ir gerinimo priemonės turi būti įgyvendinamos laiku ir tinkamai. Taryba kontroliuoja Suomijos strategijos įgyvendinimo terminų laikymąsi, vykdo Suomijos strategijos įgyvendinimo kokybės kontrolę. Vykdydama tokią kontrolę Taryba pagal savo kompetenciją gali operatyviai reaguoti ir teikti pasiūlymus bei rekomendacijas tiek dėl Suomijos strategijos įgyvendinimo terminų, tiek dėl kokybės. Tokia Suomijos strategijos įgyvendinimo kontrolė įvardijama kaip vienas iš pagrindinių Tarybos uždavinių.

2. *Gerinti ir užtikrinti informacijos saugos rizikos valdymą.* Kaip viena iš prioritetinių priemonių Suomijos strategijoje yra numatyta rizikos valdymas. Jis vykdomas siekiant įsigilinti į faktinę aplinką, o tai galima tik reguliariai atliekant tam tikrus kontrolės veiksmus, ir kartu mažinti galimus rizikos pasireiškimo veiksnius bei jų įtaką, žalą, saugoti kritiškai svarbią infrastruktūrą. Šiuo tikslu kuriama nacionalinė informacijos saugos rizikos valdymo sistema, valdoma FICOROS[2], bei užtikrinamas nuolatinis pagrindinių veikėjų dalyvavimas atnaujinant informaciją (Transporto ir komunikacijų, Vidaus reikalų, Finansų, Pramonės ir prekybos, Gynybos ministerijos, Valstybės saugumo padalinys bei kiti subjektai, susiję su informacijos sauga). Bendradarbiavimo tikslu numatyta sukurti darbo grupę, sudarytą iš pagrindinių veikėjų, atsakingų už kritiškai svarbios infrastruktūros apsaugą.

[1] „e. Norvegija 2005“ yra Norvegijos strateginis dokumentas, susijęs su valstybės politika elektroninės erdvės ir elektroninės informacijos kontekste.

[2] FICORA yra institucija, atsakinga už Suomijos elektroninių ryšių operatorių ir elektroninių ryšių paslaugų teikėjų veiklos reguliavimą bei priežiūrą.

3. Užtikrinti pagrindinių žmogaus ir piliečio teisių, laisvių ir teisėtų interesų bei nacionalinio žinių potencialo apsaugą. Suomijos strategijoje taip pat pabrėžiama privataus sektoriaus ir savivaldos dalyvavimo šiame procese svarba, pažyminti būtinumą saugoti verslo ir komercines paslaptis, turtines ir neturtines autorių teises bei klientų (asmens) duomenis. Dauguma institucijų, kurios pagal savo kompetenciją atsakingos už informacijos saugos politikos formavimą, bendradarbiauja su privačiu sektoriumi siekdamos perteikti geriausią praktiką ne tik valstybinėms institucijoms, bet ir privačiam verslui. Tik nuoseklus ir tolygus informacinių technologijų ir informacijos saugos užtikrinimas ne tik viešajame, bet ir privačiame sektoriuje, Suomijos vyriausybės nuomone, leidžia sukurti saugią informacinės visuomenės aplinką. Šiuo tikslu numatyta įvertinti esamą teisinę aplinką verslo ir komercinių paslapčių, autorių teisių bei duomenų apsaugos srityse ir pateikti atitinkamų valdžios institucijų pasiūlymus, kaip tobulinti esamą reguliavimą.

Atkreiptinas dėmesys, kad ir Suomijos strategija yra sukurta atsižvelgiant į 2002 m. EBPO „Informacinių sistemų ir tinklų saugumo gaires“ ir įgyvendina gairėse nurodytus principus.

1.3. Čekijos informacijos saugos strategija

Čekijos nacionalinė informacijos saugos strategija [9] (toliau – Čekijos strategija) buvo priimta 2006 m. ir laikoma pagrindiniu dokumentu Čekijos informacijos saugos politikos srityje [10]. Teigiama, kad Čekijos strategijoje yra įgyvendinami informacijos saugos principai, išdėstyti 2002 m. EBPO Informacinių sistemų ir tinklų saugumo gairėse. Atskiras Čekijos strategijos priedas – priedas Nr. 1, skirtas informacijos saugai viešojo administravimo srityje. Svarbu paminėti, jog Čekijos strategijoje numatytas strategijos ryšys su kitais Čekijos ir ES strateginiais dokumentais. Čekijos strategijoje nurodoma, kad šį dokumentą buvo numatyta priimti Čekijos vyriausybės patvirtintoje „Valstybės informacijos ir komunikacijos strategijoje: e. Čekija 2006“ [11] bei „Čekijos saugumo strategijoje“.

Už Čekijos strategijos įgyvendinimą, atnaujinimą bei tikslų pasiekimo įvertinimą atsakinga Čekijos informatikos ministerija. Ši ministerija turi sudaryti informacijos saugos komitetą, kuris dalyvaujant viešojo administravimo subjektų atstovams atliktų informacijos saugos koordinavimo funkciją.

Čekijos strategija numato šiuos pagrindinius tikslus, susijusius su elektroninės informacijos saugos reguliavimu:

1) *Gerinti informacijos saugos ir rizikos valdymą*. Šiuo tikslu siekiama plėtoti bei gerinti informacijos valdymo sistemų kokybę ir įtraukti šias sistemas į bendrą organizacijos valdymą. Šios sistemos turi užtikrinti visų informacijos formų saugumą įskaitant ir informaciją elektronine forma. Turi būti įgyvendinamos tokios priemonės kaip:

- vykdyti nuolatinę grėsmių stebėseną;
- vykdyti pasiūlytų kontrpriemonių efektyvumo stebėseną;
- užtikrinti valstybės kritinės informacijos infrastruktūros apsaugą;
- gerinti viešojo administravimo subjektų informacijos saugumą.

2) *Palaikyti tarptautinį bei nacionalinį bendradarbiavimą informacijos saugos srityje*. Siekiama paskatinti dalyvauti įvairiose ES bendradarbiavimo programose, EBPO veikloje ir pan. Šiam tikslui pasiekti numatomos priemonės:

- įgyvendinti veiksmingą bendradarbiavimą ir koordinavimą nacionaliniu mastu;
- įgyvendinti aktyvų tarptautinį bendradarbiavimą;
- įgyvendinti bendradarbiavimą nacionalinės gynybos srityje prieš grėsmes informacijos saugumui (pvz., įgyvendinti kritinę informacijos infrastruktūrą valdančių tarnybų bendradarbiavimą).

3) *Gerbti žmogaus teises ir laisves*. Siekiant šio tikslo būtina plėtoti teisinę bazę, saugančią žmogaus teises ir pagrindines laisves (pvz., užtikrinti, kad konstitucinės normos, tokios kaip privatumą saugančios normos, būtų detalizuojamos įstatymuose ir poįstatyminiuose aktuose);

4) *Palaikyti Čekijos ekonomiką bei konkurencingumą*. Šis tikslas apima tokias priemones kaip:

- vykdyti teisės aktų stebėseną ir juos įvertinti;
- panaikinti tam tikras kliūtis (pvz., panaikinti kliūtis laisvai pasirinkti ir diegti kompiuterių programas) ir kt.

Čekijos strategijos priedas Nr. 1 dėl informacijos saugos viešojo administravimo srityje skirtas viešojo administravimo subjektų bei organizacijų informacijos saugai. Atkreiptinas dėmesys, kad priede labai aiškiai atskirtos įvairių organizacijų bei institucijų funkcijos, pareigos bei kompetencija informacijos saugos užtikrinimo srityje. Pavyzdžiui, informacijos saugos komitetas privalo įkurti informacijos saugos forumą, kuriame dalyvautų informacijos saugos srities (plačiąja prasme) ekspertai, taip pat užtikrinti privataus ir viešojo sektoriaus bendradarbiavimą [12]. Aiškiai išskirta bei detalizuojama tokių institucijų/organizacijų kompetencija informacijos saugos srityje kaip: Informatikos ministerijos, Nacionalinio saugumo biuro, Informacijos saugumo tarnybos, Vidaus reikalų ministerijos, Policijos, Gynybos ministerijos, Prekybos ministerijos, Teisingumo ministerijos, Asmens duomenų apsaugos inspekcijos, Statistikos departamento ir kt. Be to, atskiras priedo skirsnis skirtas informacijos saugai užtikrinti vietos savivaldoje.

1.4. Nagrinėjamų informacijos saugos strategijų apibendrinantys lyginamieji aspektai

Visos analizuotos strategijos nacionaliniu lygiu įtvirtina pagrindinius tolesnės informacinių sistemų plėtros principus, numatytus 2002 m. EBPO Informacinių sistemų ir tinklų saugumo gairėse.

Remiantis atlikta elektroninės informacijos saugos strategijų analize galima išskirti šiuos elektroninės informacijos saugos reguliavimo aspektus:

1) visos nagrinėtos strategijos numato, kad būtina nacionaliniu lygiu kompleksiškai reguliuoti elektroninės informacijos saugos procesus;

2) analizuotų valstybinių elektroninės informacijos saugos strategijų reguliavimo apimtis – visa nacionalinė elektroninės informacijos infrastruktūra, apimanti tiek privataus, tiek ir viešojo (taip pat ir valstybinio) sektorių elektroninę informaciją;

3) visose nagrinėtose strategijose ganėtinai nuosekliai ir išsamiai išdėstytos ir apibūdintos užsibrėžtų pagrindinių tikslų ir priemonių, kuriomis jie įgyvendinami, nuostatos. Atsižvelgiant į strategijas įgyvendinančių institucijų turimas galimybes numatomi realūs sėkmingo strategijų užsibrėžtų tikslų įgyvendinimo terminai. Visos analizuotos saugos strategijos sutampa visais esminiais užsibrėžtais pasiekti tikslais, tokiais kaip *turi būti kuriama ir puoselėjama saugos kultūra, užtikrinamas vienodo požiūrio į informacijos saugą formavimas, gerinamas informacijos saugos ir rizikos valdymas, užtikrinama pagrindinių žmogaus teisių, laisvių ir teisėtų interesų apsauga, daugiau dėmesio turi būti skiriama kritiškai svarbių valstybei informacinių sistemų apsaugai, skatinamas bendradarbiavimas saugos klausimais nacionaliniu ir tarptautiniu lygiu ir pan.* Skiriasi tik šių tikslų pasiekimo priemonės, kurios priklauso nuo nacionalinių šalies infrastruktūros, teisinės sistemos ir kitų ypatumų;

4) strategijose išskirti du elektroninės informacijos saugos institucinės sistemos lygiai: elektroninės informacijos saugos politikos formavimo lygis ir elektroninės informacijos saugos kontrolės lygis;

5) kai kurios iš nagrinėtų strategijų įgyvendina naudingas elektroninės informacijos saugos reguliavimo praktikas: nurodo strategijų ryšį su kitais elektroninės informacijos saugą reglamentuojančiais teisės aktais, tam tikrų institucijų funkcijas (kompetenciją) arba kelia institucijų reikalingumo/atsakomybės klausimus;

6) Suomijos ir Čekijos elektroninės informacijos saugos strategijos nemažai dėmesio skiria savivaldos elektroninės informacijos saugai reguliuoti.

Autorių nuomone, straipsnyje išnagrinėtus pagrindinius minėtų Europos valstybių informacinių sistemų ir elektroninės informacijos saugos įgyvendinimo principus, priemones bei turimą šių valstybių patirtį turėtų panaudoti kompetentingos valstybės institucijos, įgyvendindamos ir koordinuodamos elektroninės informacijos saugos užtikrinimo procesus nacionaliniu lygiu.

2. ELEKTRONINĖS INFORMACIJOS SAUGOS REGULIAVIMAS LIETUVOJE – LIETUVOS ELEKTRONINĖS INFORMACIJOS SAUGOS VALSTYBĖS INSTITUCIJŲ INFORMACINĖSE SISTEMOSE VALSTYBINĖ STRATEGIJA

Lietuvos elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinė strategija iki 2008 m. (toliau – Valstybinė strategija) ir jos įgyvendinimo priemonių planas [13] Lietuvos Respublikos Vyriausybės nutarimu Nr. 601 patvirtintas 2006 m. birželio 19 d. Jau iš strategijos pavadinimo aišku, kad Valstybinė strategija skirta išimtinai valstybės institucijų sektoriui – taip susiaurinta informacijos saugos reguliavimo sritis. Tokia tendencija formuojama ir kai kuriuose kituose Lietuvos Respublikos teisės aktuose. Pavyzdžiui, Elektroninės valdžios koncepcijos [14] IX skyriuje, skirtame informacijos saugumui, kalbama tik apie valstybės informacinių sistemų saugumą ir neužsimenama apie elektroninės valdžios dalyvių – asmenų informacinių sistemų saugumą. Ši tendencija kelia tam tikrą nerimą, nes informacijos saugumas negali būti veiksmingai užtikrinamas reguliuojant tik valstybės institucijų sektorių ir paliekant nuošalyje privatų sektorių. Informacijos sauga yra procesas, kai informacijos saugumą turi užtikrinti visos procese dalyvaujančios šalys. Kaip išimtį galima paminėti teiginį, kad daugiau turėtų būti rūpinamasi saugumo užtikrinimu ne tik viešojo administravimo sektoriuje, bet ir platesniu mastu [15].

Pagrindiniai valstybinės strategijos tikslai yra:

- tobulinti elektroninės informacijos saugos koordinavimą ir priežiūrą. Šiam tikslui pasiekti numatyti tokie uždaviniai: užtikrinti elektroninės informacijos saugos koordinavimą; sukurti veiksmingą kovos su nusikalstamomis veikomis, vykdomomis elektroninės informacijos perdavimo aplinkoje, sistemą;
- teisės aktais reguliuoti elektroninės informacijos saugą. Šiam tikslui pasiekti numatyti tokie uždaviniai: priimti teisės aktus, reguliuojančius elektroninės informacijos saugą; elektroninės informacijos saugą nustatyti saugos dokumentuose;
- kelti elektroninės informacijos saugos kultūrą. Šiam tikslui pasiekti numatyti tokie uždaviniai: mokyti elektroninės informacijos saugos valstybės tarnautojus ir darbuotojus, dirbančius pagal darbo sutartis; skatinti elektroninės informacijos saugos svarbos suvokimą;
- tobulinti elektroninės informacijos perdavimo infrastruktūros saugą. Šiam tikslui pasiekti numatytas uždavinys – tobulinti saugiame valstybiniame duomenų perdavimo tinkle saugomos ir perduodamos elektroninės informacijos saugą;
- skatinti elektroninės informacijos saugos užtikrinimo projektų įgyvendinimą. Šiam tikslui pasiekti numatytas uždavinys – naudotis privataus sektoriaus patirtimi įgyvendinant elektroninės informacijos saugos projektus.

Pažymėtina, kad nepaisant šioje strategijoje užsibrėžtų tikslų uždavinių, skirtų šiems tikslams pasiekti, formuluotės yra ganėtinai deklaratyvios, abstrakčios ir nekonkrečios. Autorių nuomone, atsižvelgiant į anksčiau minėtų Suomijos, Norvegijos bei Čekijos valstybių patirtį būtų tikslinga siektinus tikslus formalizuoti konkrečiais užsibrėžtais įgyvendinti veiksmais. Dabartiniame Valstybinės strategijos variante šios priemonės pateikiamos atskirai patvirtintame šios strategijos įgyvendinimo priemonių plane, šių priemonių nekonkretinant.

Taip pat būtina pažymėti ir tai, kad Valstybinė strategija, kitaip nei Čekijos, Norvegijos bei Suomijos valstybių praktika, tam tikrais aspektais neformuoja darnios elektroninės informacijos saugos politikos Lietuvos Respublikoje. Toliau bus aptariami, autorių nuomone, Lietuvos valstybinės strategijos trūkumai bei teikiami pasiūlymai dėl Valstybinės strategijos tobulinimo, taip pat dėl atitinkamo elektroninės informacijos saugos reguliavimo Lietuvoje tobulinimo.

Pirmiausia Valstybinės strategijos reguliavimo neapima Lietuvos Respublikos savivaldybių informacinės sistemos. Kaip rodo Čekijos bei Suomijos valstybės saugos informacinėse sistemose reguliavimo praktika, savivaldybės yra gana svarbi valstybinio sektoriaus dalis, kuriai turėtų būti skiriamas deramas dėmesys reguliuojant elektroninės informacijos saugą. Šiuo metu Lietuvoje elektroninės informacijos sauga savivaldybėse iš viso nereguliuojama – taip savivaldybių informacinės sistemos paliekamos likimo valiai šiuolaikinių informacijos saugumo grėsmių akivaizdoje.

Valstybinė strategija išimtinai taikoma tik valstybiniam sektoriui (viešas nevalstybinis ir privatus lieka nereguliuojami), tačiau tokių valstybinių įmonių (kaip VĮ „Regitra“, VĮ „Infostruktūra“, VĮ „Registrų centras“ ir kt.) informacinių sistemų šios strategijos reguliavimo sritis neapima. Šių įmonių informacinės sistemos vaidina kritiškai svarbų vaidmenį mūsų valstybės informacinėje infrastruktūroje, tačiau šios strategijos nuostatos (jeigu skaitytume teisės akto tekstą) joms nėra privalomos. Reikia atkreipti dėmesį, kad šioms įmonėms net nėra rekomenduojama vadovautis šiuo dokumentu. Taigi dalis valstybinio sektoriaus visiškai „iškrenta“ iš Valstybinės strategijos reguliavimo srities. Todėl galima tik įsivaizduoti, kas įvyktų, jeigu VĮ „Regitra“, VĮ „Infostruktūra“ arba VĮ „Registrų centras“ informacinių sistemų sauga nebūtų reglamentuota saugos politiką numatančiais dokumentais ir kiekvienas administratorius arba vartotojas elgtųsi kaip tinkamas. Atsižvelgiant į elektroninės informacijos saugos reguliavimo srityje lyderiaujančių užsienio valstybių patirtį ne tik pageidautina išplėsti Valstybinės strategijos taikymo sritį viešajam nevalstybiniame sektoriui, tačiau svarstytina ir bendrosios valstybinės strategijos, apimančios ne tik valstybės institucijų sektorių, bet ir privatų sektorių, galimybė.

Grįžtant prie Valstybinės strategijos pažymėtina, kad joje išskiriama atskirų valstybės institucijų, valstybės informacinių sistemų valdytojų kompetencija, ypač atsakomybė elektroninės informacijos saugos srityje. Tai viena iš pagrindinių Valstybinės strategijos problemų, praktikoje suponuojanti situaciją, kai valstybės institucijoms iki galo neaišku, kokias funkcijas turi (turėtų) vykdyti informacijos saugos srityje. Kaip pavyzdį galima pateikti nelaukto komercinio pašto (angl. *Spam*) kontrolės problemą. Paminėtinos kelios institucijos – Ryšių reguliavimo tarnyba, Valstybinę duomenų apsaugos inspekcija, Vartotojų teisių gynimo taryba – kurių veikla ir funkcijos iš dalies susijusios ir su šiuo neigiamu reiškiniu. Tačiau šių institucijų funkcijos nėra aiškiai atribotos ir tai lemia kovos su minimu neigiamu reiškiniu efektyvumo stoką.

Valstybinės strategijos reguliavimo sritis – valstybės institucijų informacinių sistemų sauga (pavadinimas turėtų būti tikslintinas atsižvelgiant į 2004 m. Lietuvos Respublikos Vyriausybės nutarimą Nr. 451, kuriuo įvestas valstybės informacinių sistemų terminas) – savo ruožtu neapima valstybės ir žinybiniuose registruose tvarkomos elektroninės informacijos, užimančios didesnę dalį valstybinio sektoriaus infrastruktūros. Manome, kad Valstybinės strategijos įgyvendinimo stebėsenai atlikti būtina įtraukti ir informaciją apie valstybės ir žinybinių registrų veiklą.

Valstybinėje strategijoje nėra nulemtas ryšio su kitais teisės aktais klausimas (Valstybės registrų integralios sistemos kūrimo strategija, Elektroninės valdžios koncepcija, Informacinės visuomenės plėtros strateginis planas ir kt.), o dėl to taip pat sunku kalbėti apie nuoseklios valstybės politikos šioje srityje egzistavimą.

Išnagrinėjus Valstybinės strategijos priemonių planą nustatyta, kad elektroninės informacijos saugos koordinavimas ir priežiūra bus įgyvendinami steigiant Elektroninės informacijos saugos koordinavimo komisiją (toliau – Komisija). Ją formuos Lietuvos Respublikos Vyriausybė. Komisijos įgaliojimai, matyt, būtų išdėstyti jos nuostatuose. Tačiau būtina pabrėžti, kad strategijoje visiškai neužsimenama apie Komisijos įgaliojimus.

Autorių nuomone, Komisija turėtų skatinti ir lemti Valstybinėje strategijoje numatytų tikslų ir priemonių praktinį įgyvendinimą vykdydama Lietuvos Respublikos Vyriausybės deleguotas koordinavimo funkcijas įgyvendinant šios srities valstybės politiką. Vykdydama tokį koordinavimą Komisija pagal savo kompetenciją galėtų operatyviai reaguoti ir teikti pasiūlymus ir rekomendacijas dėl Valstybinės strategijos įgyvendinimo terminų arba kokybės. Komisija prireikus teiktų pasiūlymus Valstybinei strategijai atnaujinti. Tam, kad Valstybinėje strategijoje numatytos priemonės būtų įgyvendintos, rekomenduojama, kad Komisija galėtų tęsti savo darbą nepriklausomai nuo politinių pokyčių Parlamente ir Vyriausybėje, t. y. daugiau nei vieną politinę kadenciją. Vyriausybė, būdama Valstybinės strategijos leidėja, atsakinga ir už joje numatytų tikslų ir priemonių įgyvendinimą. Komisija šiuo atveju ir būtų tas įrankis, kuris padėtų derinti šiuos procesus. Komisija privalėtų periodiškai atsiskaityti Vyriausybei. Ji turėtų veikti kaip plataus masto forumas, skirtas pačių įvairiausių subjektų bendradarbiavimui dėl elektroninės informacijos valstybės institucijų informacinėse sistemose saugos užtikrinti ir gerinti.

Pažymėtina, kad elektroninės informacijos saugos politikos formavimo lygis (ne tik valstybės institucijų sektoriuje) šiuo metu Lietuvoje kelia nemažą susirūpinimą. Manoma, kad už informacijos saugos politikos formavimą turi būti atsakinga viena institucija [16, p. 33]. Šiuo metu Lietuvoje nėra nepriklausomos institucijos, kuriai būtų pavesta formuoti informacijos saugos politiką Lietuvos mastu.

Institucinės kontrolės klausimu, autorių nuomone, siekiant aiškios ir veiksmingos elektroninės informacijos valstybės institucijų informacinėse sistemose saugos

kontrolės turi būti įgyvendinami du skirtini institucinės kontrolės lygiai:

1. politikos formavimo elektroninės informacijos valstybės institucijų informacinėse sistemose saugos kontrolės lygis;
2. nustatytų elektroninės informacijos valstybės institucijų informacinėse sistemose saugos reikalavimų laikymosi kontrolės lygis.

Turėtų būti ypač stiprinamas antrasis kontrolės lygis, nes šiuo metu esanti elektroninės informacijos valstybės institucijų informacinėse sistemose saugos reikalavimų laikymosi kontrolė yra per silpna. Į šio lygio įgyvendinimą turėtų aktyviai įsitraukti Valstybės kontrolė, kuri iki šiol atlikdavo valstybės informacinių sistemų auditą tik kaip kitų įstatymuose numatytų auditų rūšių (veiklos, finansinio audito) dalį. Todėl reikėtų įvertinti įstatymų nustatytas Valstybės kontrolės funkcijas atliekant valstybės informacinių sistemų auditą bei aiškiau suformuluoti Valstybės kontrolės uždavinius užtikrinant antrąjį informacijos technologijų saugos valstybiniame sektoriuje lygį. Tam tikros antrojo lygio kontrolės funkcijos turėtų būti suteikiamos Lietuvos Respublikos vidaus reikalų ministerijai, kurios sudėtyje yra Informacinės politikos departamentas. Šio departamento darbuotojai turėtų turėti galimybę esant pagrindui atlikti valstybės informacinėse sistemose užtikrinamos informacijos technologijų saugos patikrinimą. Tokie patikrinimai turėtų būti įmanomi ir pasitelkiant trečiuosius asmenis, pavyzdžiui, sertifikuotas audito įstaigas arba nepriklausomus ekspertus. Institucinė valstybės institucijų informacijos technologijų saugos kontrolė turėtų būti derinama ir su Komisijos vykdoma veikla.

Autorių nuomone, siekiant veiksmingai reglamentuoti valstybinių institucijų informacinių sistemų veiklą būtina suformuoti nuoseklią informacijos saugos politiką. Todėl tikslinga Valstybinės strategijos užsibrėžtą įgyvendinti tikslą „teisės aktais reguliuoti elektroninės informacijos saugą“ išplėsti nuostatomis, numatančiomis, kad kiekviena institucija, informacinių sistemų ir informacijos saugumo srityje formuodama savo informacijos saugos politiką, privalo parengti teisinę bazę, kuri būtų veiksmingai taikoma konkrečios institucijos informacinei sistemai arba informacinėms sistemoms. Valstybė gali nustatyti tik pagrindines gaires, kurių turėtų būti laikomasi. Autorių nuomone, tikslinga atsisakyti šiuo metu galiojančių patvirtintų Tipinių duomenų saugos nuostatų [17] kai kurias jų nuostatas perkeliant į Bendruosius duomenų saugos reikalavimus [18] ir nustatyti, kurie teisės aktai, pavyzdžiui, informacijos saugumo koncepcija, informacijos saugumo nuostatai, informacijos tvarkymo taisyklės, informacinės sistemos nuostatai, saugaus darbo su duomenimis taisyklės, nenumatytų situacijų valdymo planas bei vartotojų administravimo taisyklės, turi sudaryti kiekvienos institucijos informacijos saugumo politiką.

Atsižvelgiant į minėtas sritis pati institucija turi nuspręsti, kaip geriausiai užtikrinti valstybės nustatytus informacinių sistemų ir informacijos saugos reikalavimus. Formuojant saugią politiką turi būti taikomas savireguliacijos principas. Užtikrinant informacinių sistemų ir informacijos saugą svarbu atsižvelgti į tai, kad kiekviena institucija naudoja skirtingas technologijas, todėl laikydamosi technologinio neutralumo principo jos pačios turi nuspręsti, kurios technologijos geriausiai užtikrina informacinių sistemų ir informacijos saugą; kiekviena institucija turi skirtingą organizacinę struktūrą; kiekvienai institucijai būdingi skirtingi uždaviniai; ne visos institucijos turi vienodus finansinius išteklius; taip pat svarbu atsižvelgti, kokio turinio informaciją valdo informacinių sistemų valdytojas. Pačios institucijos gali priimti veiksmingiausią sprendimą.

Norint užtikrinti adekvatų elektroninės informacijos valstybės institucijų informacinėse sistemose saugą, informacinės sistemos ir jose tvarkoma informacija turi būti klasifikuojamos atsižvelgiant į gresiančių grėsmių veiksnį ir į tai, kokios svarbos sistema ir joje tvarkoma informacija yra asmenims, įstaigai, visai visuomenei arba valstybei. Kritiškai svarbios informacinės sistemos ir infrastruktūra turi būti saugomos tik sertifikuotais saugos sprendimais. Informacinės sistemos ir infrastruktūra gali būti pripažinta kritiškai svarbia visuomenei, jei tos pačios visuomenės, atskirų valstybės įstaigų, organizacijų ar asmenų veikla gali būti pažeidžiama sutrikus normaliam tokios sistemos darbui. Tokiu atveju ypač svarbu nustatyti tokias sistemas ir įvertinti jų patikimumą pagal kritiškumo skalę. Visoms kitoms valstybės informacinėms sistemoms turėtų būti taikomi bendrieji saugos reikalavimai. Organizacijose saugos priemonės turi būti naudojamos atitinkamai pagal nustatytus ir įvertintus rizikos veiksnius. Sauga organizacijoje turi apimti tiek fizinius, tiek loginius, administracinius, tiek ir teisinius lygius ir priemones. Tinkamomis priemonėmis turbūt reikėtų laikyti geros praktikos kodeksų taikymą organizacijos veikloje siekiant užtikrinti kritiškai svarbios informacijos ir infrastruktūros patikimumą, atsparumą ir apsaugą. Šiuo tikslu Lietuvos Respublikoje turi būti patvirtintas sąrašas reikalavimų, kuriais vadovaujantis būtų galima nustatyti kritiškai svarbias sistemas ir infrastruktūrą. Šis sąrašas turėtų būti sudaromas įvertinant rizikos ir patikimumo nustatymo metodus bei jų santykį, taip pat priemones, kuriomis būtų galima patikrinti informacinių sistemų konfidencialumą, vientisumą bei tinkamumą eksploatuoti. Šiuo tikslu, vadovaujantis tarptautinėmis metodikomis, gerąja praktika ir standartais, turi būti kuriami nacionaliniai informacinių sistemų ir informacijos klasifikavimo standartai, IT sistemų ir informacijos kategorijų schemos, taikytinos ir viešajam, ir privačiam sektoriams. Išimtis turėtų būti taikoma informacinėms sistemoms ir infrastruktūrai, apdorojančioms įslaptintą informaciją. Jų saugumo lygis nustatomas vadovaujantis Valstybės ir tarnybos paslapčių įstatymo nuostatomis, reglamentuojančiomis įslaptintos informacijos klasifikavimą ir žymėjimą.

Daugiau dėmesio turi būti skiriama saugos įgaliotiniui. Siekiant tinkamai įgyvendinti informacijos saugos politiką kiekvienoje valstybinėje institucijoje turi būti nustatytos saugos įgaliotinio funkcijos, uždaviniai bei atsakomybė. Taip pat turi būti apibrėžti reikalavimai, būtini šioms pareigoms užimti.

Siekiant sukurti saugią informacinės visuomenės aplinką būtina nuosekliai ir tolygiai užtikrinti informacinių sistemų ir informacijos saugumą ne tik viešajame (valstybiniame), bet ir privačiame sektoriuose. Todėl tikslinga išplėsti Valstybinės strategijos taikymo sritį įtraukiant nuostatas, kad valstybinės institucijos, kurios pagal savo kompetenciją atsakingos už informacijos saugumo politikos formavimą, turi bendradarbiauti su privačiu sektoriumi siekdamos perteikti geriausią praktiką ne tik valstybinėms institucijoms, bet ir privačiam verslui. Privataus ir viešojo sektoriaus bendradarbiavimas gali būti sėkmingai įgyvendinamas apmokant informacinių sistemų ir informacijos saugos specialistus. Būtina atkreipti dėmesį ir į grįžtamojo ryšio problemą. Turima omenyje, kad valstybės institucijos taip pat gali ir turi pritaikyti privataus sektoriaus sprendimus ir praktiką savo veikloje.

Atsižvelgiant į užsienio valstybių patirtį tikslinga Valstybinės strategijos strategijos, taip pat kitas elektroninės informacijos saugos reguliavimo nuostatas sukonkretinti autorių teikiamais pasiūlymais. Autorių nuomone, šie pasiūlymai leistų užpildyti nagrinėtas esamo elektroninės informacijos saugos reguliavimo spragas.

IŠVADOS

1. Nagrinėtose Europos valstybių (Norvegijos, Čekijos, Suomijos) strategijose sistemiškai reguliuojama informacijos saugos informacinėse sistemose sritis:
   - strategijos taikomos ne tik valstybės institucijoms, bet ir privačiam sektoriui;
   - aiškiai įvardijamos institucijų kompetencijos informacijos saugos srityje ribos;
   - daug dėmesio skiriama informacijos saugos informacinėse sistemose politikai bei kontrolei koordinuoti;
   - privatus ir valstybinis sektoriai skatinami visapusiškai bendradarbiauti diegiant tam tikrą elektroninės informacijos saugos reguliavimą.

2. Lietuvos valstybinėje strategijoje nėra numatyta svarbių elektroninės informacijos saugos užtikrinimo būdų bei priemonių, kurias galima aptikti šiuolaikinėse užsienio valstybių elektroninės informacijos saugos strategijose. Dabartinės Valstybinės strategijos nuostatos yra gana deklaratyvios, abstrakčios ir nekonkrečios. Valstybinėje strategijoje nėra apspręstas ryšio su kitais teisės aktais klausimas (Valstybės registrų integralios sistemos kūrimo strategija, Elektroninės valdžios koncepcija, Informacinės visuomenės plėtros strateginis planas ir kt.), o tai savo ruožtu leidžia teigti, kad ši Valstybinė strategija tam tikrais aspektais formuoja nuoseklią elektroninės informacijos saugos politiką Lietuvos Respublikoje.

3. Valstybinės strategijos reguliavimo sritis taip pat neapima valstybės ir žinybiniuose registruose tvarkomos elektroninės informacijos, apimančios didelę dalį valstybinio sektoriaus infrastruktūros. Manome, kad Valstybinės strategijos įgyvendinimo stebėsenai atlikti būtina įtraukti ir informaciją apie valstybės ir žinybinių registrų veiklą.

4. Elektroninės informacijos saugos politikos formavimo lygis kelia nemažą susirūpinimą. Lietuvoje galima paminėti kelias institucijas – Ryšių reguliavimo tarnybą, Valstybinę duomenų apsaugos inspekciją, Vidaus reikalų ministeriją, Informacinės visuomenės plėtros komitetą prie Lietuvos Respublikos Vyriausybės – jos dalyvauja formuojant ir vykdant elektroninės informacijos valstybės informacinėse sistemose saugos politiką. Tačiau šių institucijų funkcijos ir atsakomybė elektroninės informacijos saugos srityje nėra aiškiai atribotos. Autorių nuomone, Valstybinėje strategijoje turėtų būti įtvirtinta už informacijos saugos politikos formavimą atsakinga nepriklausoma institucija.

5. Siekiant sukurti saugią žinių visuomenės aplinką būtina nuosekliai ir tolygiai užtikrinti informacinių sistemų ir informacijos saugumą ne tik viešajame (valstybiniame), bet ir privačiame sektoriuose. Atkreiptinas dėmesys į tai, kad Valstybinės strategijos reguliavimo sritis neapima Lietuvos Respublikos savivaldybių informacinės sistemos. Autorių nuomone, atsižvelgiant į Suomijos, Norvegijos bei Čekijos valstybių patirtį būtų tikslinga Valstybinės strategijos formuluotes išplėsti konkrečiais užsibrėžtais įgyvendinti veiksmais. Dabartinėje Valstybinės strategijos redakcijoje šios nesukonkretintos priemonės pateikiamos atskirai patvirtintame šios strategijos įgyvendinimo priemonių plane.

6. Lietuvoje turėtų būti tobulinamas elektroninės informacijos saugos reguliavimas atitinkamais teisės aktais užtikrinant: straipsnyje siūlomą elektroninės informacijos valstybės institucijų informacinėse sistemose klasifikavimą, elektroninės informacijos saugos politikos formavimo ir institucinės kontrolės sistemos atskyrimą bei elektroninės informacijos saugos įgaliotinio instituto detalizavimą.

LITERATŪRA

1. **Mitrakas A**. Information Security Law in Europe: Risks Checked // Information & Communications Technology Law. 2006. Vol. 15. No. 1.
2. **National Strategy** for Information Security Challenges, Priorities and Measures. Norway, 2003 // http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf/viewHtml/index/$FILE/Norway_Nat%20strat%20info%20security.pdf.
3. **eNorway 2005** // http://odin.dep.no/archive/nhdvedlegg/01/03/eNorw040.pdf.
4. **OECD Guidelines** for the Security of Information Systems and Networks: Towards a Culture of Security. 2002 // http://www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html.
5. **Government Resolution** on National Information Security Strategy. Ministry of Transport and Communications of Finland // http://webdomino1.oecd.org/COMNET/STI/ IccpSecu.nsf/viewHtml/index/$FILE/Finland%20 Government%20resolution%20on%20national%20information%20%20security%20strategy.pdf.
6. **Creating a Safer** Information Society: National Information Security Advisory Board report, submitted to the Government on 14 December 2004. – Vammalan Kirjapaino Oy, 2005. ISSN 1457-747X; // http://www.tekes.fi/ julkaisut/lvm_tietoyht_e_mr.pdf.

7. **Finland Promotes** It's Secure Information Society Model to EU Countries // http://e.finland.fi/netcomm/news/showarticle.asp?intNWSAID=35824.
8. **National information** security strategy proposal. November 25, 2002 Proposal of the Advisory Committee for Information Security // http://www.ficora.fi/englanti/ document/infos.pdf#search=%22National%20Information%20Security%20Strategy%20proposal%22.
9. **Czech Republic** National Strategy for Information Security, 2006 // http://micr.cz/scripts/detail.php?id=3189.
10. **Security Strategy** of Czech Rebublic: Introduction of the Prime Ministre of Czech republic // http://www. czechembassy.org/wwwo/mzv/default.asp?id=24118&ido=7567&idj=2.
11. **State Information** and Communications Policy e-Czech 2006 // http://www.micr.cz/files/1288/ENG-SIKP.pdf.
12. **Czech Republic** National Strategy for Information Security - Annex No. 1 (Information Security for Public Administration Bodies) // http://www.micr.cz/files/3189/AJ_P__loha_1_k_NSIB.pdf.
13. **Lietuvos Respublikos** Vyriausybės 2006 m. birželio 19 d. nutarimas Nr. 601 „Dėl elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinės strategijos iki 2008 metų ir jos įgyvendinimo priemonių plano patvirtinimo“ // Žin. 2006. Nr. 70-2575.
14. **Lietuvos Respublikos** Vyriausybės 2002 m. gruodžio 31 d. nutarimas Nr. 2115 „Dėl elektroninės valdžios koncepcijos patvirtinimo“ // Žin. 2003. Nr. 2-54.
15. **Lietuvos informacinės** visuomenės plėtros strategija, patvirtinta 2005 m. birželio 8 d. Lietuvos Respublikos Vyriausybės nutarimu Nr. 625 // Žin. 2005. Nr. 73-2649.
16. **Esterle A., Ranck H., Schmitt B**. Information Security: A New Challenge for EU. – Institute for Security Studies, Paris, 2005.
17. **Vidaus** reikalų ministro 2003 m. liepos 16 d. įsakymas Nr. 1V-272 „Dėl tipinių duomenų saugos nuostatų patvirtinimo“ // Žin. 2003. Nr. 76-3511.
18. **Lietuvos Respublikos** Vyriausybės 1997 m. rugsėjo 4 d. nutarimas Nr. 952 „Dėl bendrųjų duomenų saugos reikalavimų patvirtinimo“ // Žin. 1997. Nr. 83-2075; 2003. Nr. 2-45.
19. **OECD Reviews** of Risk Management Policies: Norway - Information Security // http://www.oecd.org/document/31/0,2340,en_2649_201185_36792031_1_1_1_1,00.htm (paskutinį kartą prieita 2006 m. rugpjūčio 9 d.).
20. **The Finnish Government** Information Security Development Plan // http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf/viewHtml/index/$FILE/Finland%20Security%20Plan.pdf. (paskutinį kartą prieita 2006 m. rugpjūčio 9 d.).

STATE`S ELECTRONICS INFORMATION SECURITY STRATEGY – ONE OF KEY ELECTRONIC INFORMATION SECURITY REGULATORY INSTRUMENTS: COMPARATIVE ANALYSIS

Darius Štitilis [*]
Žydrūnas Paškauskas [**]
Mykolas Romeris University

S u m m a r y

In the light of the analysis of the security of electronic information, Lithuania ranks one of the last positions as far as it concerns the level of the security of electronic information across the EU. Therefore, it is possible to maintain that Lithuania needs special measures (including statutory instruments) with a view of substantially improving the security of electronic information. In 2006 Lithuania adopted a new strategy for the security of electronic information; however, bearing in mind the statistics related to the security of electronic information, it is doubtful whether all key methods and measures for ensuring the security of electronic information have been reckoned with. Some EU Member States and other countries have a more profound experience in the field of ensuring the security of electronic information (e.g. Finland, Czech Republic, Norway). The best practice of these countries is essential for improving the legal basis for the security of electronic information as well as ensuring the enforcement of such security. The article deals with strategies for the security of electronic information in several European countries in comparison to the new Lithuanian strategy for the security of electronic information. The subject of this article relates to regulation of the security of electronic information taking into account the fact that the strategy for the security of electronic information is one of its key elements. The purpose of this article is to compare and analyze the most advanced strategies of the security of electronic information which are available in some EU Member States and other countries (Finland, Czech Republic, Norway) and provide an assessment of the Lithuanian strategy for the security of electronic information as well as appropriate proposals how to improve the strategy. The methods of comparison and analysis as well as some others have been applied in the article. Databases of legal instruments in foreign countries as well as periodicals have been referred to in order to analyze the strategies for the security of electronic information in the above-referred countries.

The analysis made in the article makes it possible to assert that, notwithstanding the recent adoption (2006), the new Lithuanian strategy for the security of electronic information fails to include some key principles of regulation of the *security* of electronic information and needs improvements. To this end, different ways and measures how to improve the Lithuanian strategy for the *security* of electronic information have been specified in this article.

Keywords: regulation of electronic information security, electronic information security strategy.

[*] Doctor of Social Science, Associated Professor of Department of Informatics and Statistics of Faculty of Economics and Finance Management of Mykolas Romeris University.

[**] Doctoral Candidate of Department of Informatics and Statistics of Faculty of Economics and Finansc Management of Mykolas Romeris University.