ISSN 2029-7564 (online)
SOCIALINĖS TECHNOLOGIJOS
SOCIAL TECHNOLOGIES
2012, 2(2), p. 441–455

ELEKTRONINĖS INFORMACIJOS SAUGOS REGLAMENTAVIMAS LIETUVOJE IR RUSIJOJE: LYGINAMIEJI ASPEKTAI

Darius Štitilis

Mykolo Romerio universitetas, Lietuva, stitilis@mruni.eu

Valdas Klišauskas

Mykolo Romerio universitetas, Lietuva, v.klisauskas@gmail.com

Abstraktas

Tikslas *– išanalizuoti Lietuvos Respublikos ir Rusijos Federacijos elektroninės informacijos saugos teisinį reguliavimą lyginamuoju aspektu.*

Metodologija *– tyrimui atlikti taikyti keli skirtingi metodai: tiriant Lietuvos ir Rusijos teisinę bazę dėl elektroninės informacijos saugos, autoriai pasitelkė lyginimo metodą. Lietuvoje ir Rusijoje galiojančio elektroninės informacijos saugos teisinio reguliavimo nustatymui taikytas empirinis teisinių dokumentų analizės metodas. Buvo tiriami Lietuvos Respublikos ir Rusijos Federacijos teisės norminiai aktai. Šis metodas leidžia ištyrus oficialius dokumentus tiksliai nustatyti ir aprašyti atitinkamo santykio galiojantį teisinį reguliavimą. Naudodami mokslinės literatūros šaltinius autoriai taikė dedukcijos metodą, leidžiantį daryti pakankamai patikimas išvadas. Sąvokų tyrimui autoriai pasitelkė naujausią mokslinę literatūrą ir žodynus.*

Rezultatai *– tyrimas atskleidė, jog Lietuvos ir Rusijos elektroninės informacijos saugos teisiniame reguliavime yra skirtumų. Šie teisinio reguliavimo skirtumai pateikiami bei komentuojami, įskaitant ir gerosios atitinkamos srities teisinio reguliavimo praktikos pritaikymo galimybes.*

ISSN 2029-7564 (online)
https://www.mruni.eu/lt/mokslo_darbai/st/apie_leidini/
https://www.mruni.eu/en/mokslo_darbai/st/apie_leidini/index.php

Tyrimo ribotumas – *nors elektroninės informacijos saugos teisinio reguliavimo analizė gali būti atliekama lyginant įvairaus lygmens teisės aktus, tačiau tyrimas atliktas lyginant ir komentuojant tik pagrindinius, strateginius teisės aktus – įstatymus, vyriausybės nutarimus. Tyrimo metu taip pat nebuvo detaliai analizuojamas teisės normų elektroninės informacijos saugos srityje įgyvendinimas.*

Praktinė reikšmė – *tyrimo rezultatai gali būti pritaikomi kuriant naujas teisės normas ar atliekant egzistuojančių teisės normų pakeitimus, kiek tai susiję su elektroninės informacijos sauga elektroninėje erdvėje.*

Originalumas/vertingumas – *straipsnyje pristatomas tyrimas yra naujas Lietuvoje. Lietuvos Respublikos ir Rusijos Federacijos teisės aktų, reglamentuojančių informacijos saugumą, analizė ankščiau atlikta nebuvo. Tyrimo rezultatai ir užpildo šią tuštumą.*

Raktažodžiai – *elektroninės informacijos sauga, teisinis reguliavimas.*

Tyrimo tipas – *tyrimo pristatymas, požiūrio pristatymas.*

1. Įvadas

Informacinių technologijų plėtra, informacijos perkėlimas į elektroninę erdvę didina informacinių procesų ir veiklos kokybę, užtikrina geresnį konkurencingumą bei efektyvumą. Tačiau tai sukelia ir neigiamas pasekmes, tokias kaip svarbios elektroninės informacijos praradimas ar net skatina elektroninį nusikalstamumą. Elektroninės informacijos sauga, ypač ekonominėje sferoje – labai svarbi ir specifinė veiklos rūšis, kuri taip pat reikalauja nuoseklaus ir detalaus teisinio reglamentavimo.

Elektroninės informacijos sauga netgi įvardijama kaip kertinis akmuo informacinėje visuomenėje (Schjolberg ir Ghernaouti-Hele, 2011). Elektroninės informacijos sauga gali būti reguliuojama reglamentuojant elektroninės informacijos saugos santykius. Pastaruoju metu visos pasaulio valstybės vis daugiau dėmesio skiria elektroninės informacijos saugai, ne išimtis ir Lietuvos Respublika, ir Rusijos Federacija. Rusijoje elektroninės informacijos saugos užtikrinimui skiriamas didelis dėmesys ir tai atspindi Rusijoje priimti teisės aktai elektroninės informacijos saugai užtikrinti: Rusijos Federacijos informacinės saugos doktrina[1], Federalinis įstatymas „Apie informaciją, informacines technologijas ir apie informacijos apsaugą“[2]. Lietuva elektroninės informacijos saugai užtikrinti taip pat yra priėmusi kelis pagrindinius teisės aktus (vyriausybės nutarimus) reguliuojančius elektroninės informacijos saugą: Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metų programos patvirtinimo[3], Dėl

1 Доктрина информационной безопасности Российской Федерации. Maskva, 2000. Žiūrėta 2012 m. spalio 10 d. Prieiga per internetą: http://www.scrf.gov.ru/documents/5.html.

2 Федеральный закон „Об информации, информационных технологиях и о защите информации“. Žiūrėta 2012 m. vasario 18. Prieiga per internetą: http://www.rg.ru/2006/07/29/informacia-dok.html.

3 Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimas Nr. 796 „Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo“. *Valstybės žinios*. 2011, Nr. 83-4033; 2011, Nr. 106 (atitaisymas).

elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose patvirtinimo[4], Dėl Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepcijos patvirtinimo[5] ir kt. Kaip matome, tiek Lietuvoje, tiek Rusijoje kreipiamas didelis dėmesys šiai problemai spręsti, tačiau Rusija nėra Europos Sąjungos narė ir jos teisei Europos Sąjungos teisė įtakos neturi. Rusijos Federacija elektroninės informacijos saugos teisiniu reglamentavimu susirūpino anksčiau nei Lietuva, nes, kaip matome iš anksčiau pateiktų elektroninės informacijos saugą reglamentuojančių pagrindinių dokumentų, matyti, Rusijos Federacijos informacinės saugos doktrina buvo priimta jau 2000 m., o Federalinis įstatymas „Apie informaciją, informacines technologijas ir apie informacijos apsaugą“ buvo priimtas 2006 m. Taigi, galima teigti, kad Rusija skiria dėmesį grėsmėms, susijusioms su elektroninės informacijos sauga. Vertinant geografinėje kaimynystėje esančios Rusijos Federacijos sukauptą patirtį elektroninės informacijos saugos srityje, manome būtų tikslinga nuodugniau išanalizuoti lyginamuoju aspektu Lietuvos ir Rusijos pagrindinius teisės aktus, reguliuojančius elektroninės informacijos saugą, ir išgryninus Lietuvos teisėkūros spragas padaryti atitinkamas išvadas.

2. Elektroninės informacijos saugos samprata ir teisinio reguliavimo poreikis

Informacijos saugumas (sauga) suprantama kaip informacijos bei sistemos infrastruktūros apsauga nuo atsitiktinio ar tyčinio, natūralaus ar dirbtinio pobūdžio poveikio, galinčio sukelti žalą informacijos ar sistemos infrastruktūros savininkams bei vartotojams (Kiškis et al., 2006). Tuo tarpu, elektroninės informacijos sauga turėtų būti suprantama kaip elektroninės informacijos ir elektroninės informacijos infrastruktūros apsauga. Kitas terminas, apibrėžiantis elektroninį saugumą, – kibernetinis saugumas (ang. *Cybersecurity*). Šiame straipsnyje minimi terminai traktuojami kaip sinonimai.

Informacijos sauga suprantama kaip trijų pagrindinių informacijos savybių – konfidencialumo, vientisumo ir prieinamumo vienybė (Petrauskas et al., 2006). Taigi, skiriami trys elektroninės informacijos saugos aspektai:

1) prieinamumas – galimybė tam tikrą laiką gauti reikalingą informaciją;
2) vientisumas – informacijos svarbums ir neprieštaringumas bei apsauga nuo sunaikinimo ir neteisėto pakeitimo;
3) slaptumas – apsauga nuo neteisėto nuskaitymo.

Labai svarbu paminėti, kad elektroninės informacijos saugos aplinkos klausimus galima skirstyti į keturias pagrindines grupes:

a) normatyvinę – įstatymai, įstatymų įgyvendinamieji teisės aktai ir t. t.;
b) administracinę – organizacijos vadovybės vykdomi bendro pobūdžio veiksmai;

---

4 Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimas Nr. 952. „Dėl duomenų saugos valstybės ir savivaldybių informacinėse sistemose“. *Valstybės žinios*. 2007, Nr. 49-1891.

5 Lietuvos Respublikos Vyriausybės 2006 m. gruodžio 6 d. nutarimas Nr. 1211 „Dėl Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepcijos patvirtinimo“. *Valstybės žinios*. 2006, Nr. 134-5081.

c) procedūrinę – konkretūs su konkrečiais asmeminis susiję saugumo veiksmai;
d) programinį-techninį – vykdomi konkretūs techninio pobūdžio veiksmai (Kiškis et al., 2006).

Šio tyrimo aspektu aktuali pirmoji – normatyvinė – grupė. Veiksminga elektroninės informacijos sauga turėtų būti vienas iš svariausių valstybės informacinės politikos prioritetų (Kiškis et al., 2006). Europos Komisijos pirmininko pavaduotoja Neelie Kroes (2012) teigė, kad „Kibernetinis saugumas yra svarbus Europos gerovės ir konkurencingumo prioritetas. Todėl ypatingai svarbus šio instituto teisinis reguliavimas. Minimo instituto teisinio reguliavimo svarba paminėta tokiuose dokumentuose kaip Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui dėl ypatingos svarbos informacinės infrastruktūros apsaugos „Europos apsauga nuo didelio masto kibernetinių antpuolių ir veiklos sutrukdymo – geresnė parengtis, didesnis saugumas ir atsparumas“[6], Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui dėl ypatingos svarbos informacinės infrastruktūros apsaugos „Visuotinio kibernetinio saugumo užtikrinimas. Laimėjimai ir tolesni veiksmai“[7], Komisijos ataskaita Tarybai, parengta pagal 2005 m. vasario 24 d. Tarybos pamatinio sprendimo dėl atakų prieš informacines sistemas 12 straipsnį[8], 2011 m. birželio 8 d. Europos Parlamento ir Tarybos reglamentas Nr. 580/2011, kuriuo iš dalies keičiamas Reglamentas (EB) Nr. 460/2004, įsteigiantis Europos tinklų ir informacijos apsaugos agentūrą, jos veiklos trukmės atžvilgiu[9]. Šie neprivalomi dokumentai daugiau turėtų veikti Lietuvos teisę, nes Lietuvos Respublika yra ES valstybė narė.

Iš holistinio pobūdžio tarptautinių dokumentų paminėtinos EBPO 2002 m. Informacinių sistemų saugos gairės (OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, 2002). Iki šių dienų tai bene vienintelis tarptautinės prigimties dokumentas elektroninės informacijos saugos srityje. Tačiau pažymėtina, kad tai neprivalomojo pobūdžio dokumentas. Vis dėlto EBPO priimtos direktyvos vertintinos kaip specifinę reikšmę turintys dokumentai, kurie nurodo

---

6 Europos Komisijos 2009 m. kovo 30 d. komunikatas COM/2009/149 Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui dėl ypatingos svarbos informacinės infrastruktūros apsaugos „Europos apsauga nuo didelio masto kibernetinių antpuolių ir veiklos sutrukdymo – geresnė parengtis, didesnis saugumas ir atsparumas“. Žiūrėta 2012 m. spalio 10 d. Prieiga per internetą:http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:LT:HTML.

7 Europos Komisijos 2011 m. kovo 31 d. komunikatas COM/2011/163 Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui dėl ypatingos svarbos informacinės infrastruktūros apsaugos „Visuotinio kibernetinio saugumo užtikrinimas. Laimėjimai ir tolesni veiksmai“. Žiūrėta 2012 m. spalio 10 d. Prieiga per internetą: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:LT:HTML.

8 Europos Komisijos 2008 m. liepos 14 d. ataskaita COM/2008/448 Tarybai parengta pagal 2005 m. vasario 24 d. Tarybos pamatinio sprendimo dėl atakų prieš informacines sistemas 12 straipsnį. Žiūrėta 2012 m. spalio 10 d. Prieiga per internetą: http://eur-law.eu/LT/Komisijos-ataskaita-Tarybai-parengta-2005-m-vasario-24,480987,d.

9 Europos Parlamento ir Tarybos 2011 m. birželio 8 d. reglamentas 2011/580/ES, kuriuo iš dalies keičiamas Reglamentas 2004/460/EB, įsteigiantis Europos tinklų ir informacijos apsaugos agentūrą, jos veiklos trukmės atžvilgiu. Žiūrėta 2012 m. spalio 10 d. Prieiga per internetą: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:165:0003:0004:LT:PDF.

valstybėms narėms pagrindines veiklos kryptis atitinkamoje reglamentavimo srityje (Kiškis et al., 2006). Europos Sąjungoje elektroninės informacijos sauga kol kas reguliuojama fragmentiškai (Štitilis et al., 2011). Paminėtina, kad nei Lietuva, nei Rusija nėra EBPO narės (List of OECD Member countries – Ratification of the Convention on the OECD, 1960), tad šių valstybių teisės aktus elektroninės informacijos saugos srityje minėtos 2002 m. gairės formaliai neturėtų veikti.

3. Strateginiai dokumentai, reguliuojantys elektroninės informacijos saugą Lietuvoje ir Rusijoje

Šioje dalyje aptarsime pamatinį teisinį visuomeninių santykių elektroninės informacijos saugos srityje reguliavimą Lietuvoje ir Rusijoje (strateginius dokumentus ir pagrindinius įstatymus), nes būtent nuo jo priklauso visos detalesnės teisinės bazės kūrimas. Atsižvelgiant į šio darbo tikslą, atitinkamus teisės aktus nagrinėsime lyginamuoju aspektu.

Elektroninės informacijos saugos strategija yra vienas iš pagrindinių elektroninės informacijos saugos reguliavimo instrumentų (Štitilis ir Paškauskas, 2007). Lietuvoje pirmoji elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinė strategija buvo patvirtinta tik 2006 m. ir galiojo iki 2008 m.[10] Šiuo metu galiojanti elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programa (toliau – Lietuvos programa) buvo patvirtinta 2011 m. birželio 29 d. Vyriausybės nutarimu Nr. 796[11]. Šioje Lietuvos programoje įvardijamos pagrindinės elektroninės informacijos saugos (kibernetinio saugumo) problemos, nustatomi elektroninės informacijos saugos (kibernetinio saugumo) plėtros tikslai ir uždaviniai.

Rusijoje strateginis dokumentas, kuris apibrėžia valstybės politiką elektroninės informacijos saugos srityje, yra 2000 m. rugsėjo 9 d. Rusijos Prezidento patvirtinta Doktrina dėl informacijos saugumo Rusijos Federacijoje[12] (toliau – Rusijos doktrina). Šioje Rusijos doktrinoje, taip pat kaip ir Lietuvos programoje, įvardijamos pagrindinės informacijos saugos problemos, nustatomi informacijos saugos tikslai, uždaviniai, principai ir pagrindinės kryptys užtikrinant informacijos saugą Rusijos Federacijoje. Tačiau skirtingai negu Lietuvos programoje, Rusijos doktrinoje žymiai daugiau dėmesio skiriama informacinės saugos būklės aprašymui, galimų grėsmių ir šių grėsmių šaltinių įvardijimui, joje taip pat įvardijamos informacinės saugos užtikrinimo įvairiose visuomeninio gyvenimo srityse ypatybės (pvz., ekonomikos, vidaus ir išorės politikos, mokslo ir technikos bei kt.). Mūsų nuomone, Lietuvos programoje taip pat galėtų būti padaryta gilesnė esamos būklės analizė, įvardintos galimos grėsmės, dėl kokių priežasčių atitin-

10 Tačiau ši strategija buvo taikoma tik valstybės institucijų sektoriui.

11 Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimas Nr. 796 „Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo“. *Valstybės žinios*. 2011, Nr. 83-4033; 2011, Nr. 106 (atitaisymas).

12 Доктрина информационной безопасности Российской Федерации. Maskva, 2000. Žiūrėta 2012 m. spalio 10 d. Prieiga per internetą: http://www.scrf.gov.ru/documents/5.html.

kami uždaviniai gali būti nepasiekti, nes tai galėtų padėti lengviau planuoti žingsnius, būtinus, kad nustatyti tikslai ir uždaviniai būtų pasiekti.

Lietuvos programos 2 punkte nustatytas pakankamai konkretus ir ambicingas strateginis tikslas, kuris turėtų būti pasiektas iki 2019 m. – plėtoti elektroninės informacijos saugą Lietuvoje, užtikrinti kibernetinį saugumą ir pasiekti, kad 2019 m. teisės aktų nustatytus elektroninės informacijos saugos (kibernetinio saugumo) reikalavimus atitinkančių valstybės informacinių išteklių dalis pasiektų 98 proc. visų valstybės informacinių išteklių, vidutinis ypatingos svarbos informacinės infrastruktūros incidentų likvidavimo laikas sumažėtų iki 0,5 valandos, o Lietuvos gyventojų, kurie saugiai jaučiasi kibernetinėje erdvėje, dalis pasiektų 60 proc.

Apibendrindami Lietuvos programos 6–10 punkte išdėstytas nuostatas galime teigti, kad joje nustatyti šie pagrindiniai siektini tikslai ir uždaviniai:

- Pasiekti, kad būtų užtikrintas valstybės informacinių išteklių saugumas. Šiam tikslui pasiekti numatyti tokie uždaviniai: tobulinti elektroninės informacijos saugos (kibernetinio saugumo) koordinavimą ir priežiūrą; tobulinti elektroninės informacijos saugos (kibernetinio saugumo) teisinį reglamentavimą; plėsti ir tobulinti saugią valstybės informacinę infrastruktūrą; skatinti elektroninės informacijos saugos (kibernetinio saugumo) projektų įgyvendinimą; plėtoti tarptautinį bendradarbiavimą elektroninės informacijos saugos (kibernetinio saugumo) srityje.
- Užtikrinti veiksmingą ypatingos svarbos informacinės infrastruktūros funkcionavimą. Šiam tikslui pasiekti numatytas uždavinys – užtikrinti ypatingos svarbos informacinės infrastruktūros saugumą.
- Siekti užtikrinti Lietuvos gyventojų ir asmenų, esančių Lietuvoje, saugumą kibernetinėje erdvėje. Šiam tikslui pasiekti numatyti tokie uždaviniai: kelti elektroninės informacijos saugos (kibernetinio saugumo) kultūrą; stiprinti Lietuvos kibernetinės erdvės saugumą; užtikrinti virtualaus Lietuvos kibernetinės erdvės perimetro apsaugą nuo išorinių kibernetinių atakų; stiprinti kibernetinėje erdvėje teikiamų paslaugų saugumą.

Lietuvos programos priede šalia siektinų tikslų ir uždavinių nustatyti ir programos įgyvendinimo vertinimo kriterijai ir siekiamos jų reikšmės 2011, 2015 ir 2019 m. bei už šių kriterijų įgyvendinimą atsakingos institucijos. Reikia pasakyti, kad nustatytos konkrečios ir ambicingos vertinimo kriterijų reikšmės, tik nežinia, kiek realiai įgyvendinamos, nes daugelis indikatorių iki Lietuvos programos priėmimo iš viso nebuvo vertinami, pvz., numatyta, kad iki 2015 m. saugią valstybės infrastruktūrą naudojančių informacinių išteklių dalis pasieks 70 proc., o 2019 m. – 100 proc., nors nėra žinoma, koks šis rodiklis buvo 2011 m. Mūsų nuomone, atsižvelgiant į tai, kad daugelio vertinimo kriterijų reikšmės nėra žinomos, Lietuvos programoje reikėjo nustatyti, kad pirmasis įvertinimas būtų atliktas daug anksčiau negu 2015 m., siekiant nustatyti pirmines atitinkamų rodiklių reikšmes (t. y. įvertinti esamą situaciją), o tuomet jau nuosekliai būtų galima nustatyti ir reikšmes, kurias reikėtų pasiekti tolesniais metais.

Be to, mūsų nuomone, kai kuriuos indikatorius iš viso gali būti sunku tiksliai įvertinti, pvz., nustatyta, kad saugiai besijaučiančių kibernetinėje erdvėje Lietuvos gyven-

tojų dalis 2015 m. turėtų siekti 40 proc., o 2019 m. – jau 60 proc., nors nežinia, kaip tą saugumo pojūtį reikės įvertinti. Nors Lietuvos programoje daug dėmesio skiriama visuomenės švietimui elektroninės informacijos srityje, tačiau, mūsų nuomone, trūksta konkretesnių priemonių, skirtų kovai su tam tikromis problemomis, pvz., piratinės programavimo įrangos naudojimui, kuri yra tikrai aktuali. „Microsoft" korporacijos užsakymu atliktos pasaulinės apklausos (Dėl kenkėjiškų programų per metus nukentėjo daugiau nei pusė interneto vartotojų, 2010) duomenimis, trys ketvirtadaliai kompiuterių vartotojų sutinka, kad naudotis nelegalia programine įranga yra nesaugu. Bendrovės „Synopticom" Lietuvoje atlikto interneto vartotojų tyrimo (Virusai ir kenkėjiškos programos trukdo dirbti daugiau nei pusei vartotojų Lietuvoje, 2010) duomenimis, Lietuvoje daugiau nei pusė vartotojų naudojasi nelegalia programine įranga.

Rusijos doktrinoje yra pateikiamos iš esmės 2 nacionalinių interesų (tikslų) grupės informacijos saugos srityje. Išanalizavus Rusijos doktrinos 1 straipsnį galima daryti prielaidą, kad pirmoji interesų (tikslų) grupė yra išskiriama pagal tai, kam šie interesai priklauso:

- asmeniui – realizuoti konstitucinę teisę į informacijos prieinamumą, apsaugoti asmeninę informaciją, turėti galimybę naudoti įstatymo nedraudžiamu būdu informaciją fiziniam, dvasiniam ir intelektualiniam vystymuisi ir kt.;
- visuomenei – užtikrinti asmens interesus informacijos saugos srityje, sukurti teisinę-socialinę valstybę, pasiekti ir išlaikyti bendrą sutarimą ir kt.
- valstybei – sudaryti sąlygas harmoningam Rusijos informacijos infrastruktūros vystymuisi, parengti reikalingus įstatymus ir tvarkas, vystyti tarptautinį bendradarbiavimą ir kt.

Analizuojant į antrąją grupę įtrauktų interesų turinį, galima daryti prielaidą, kad ši grupė yra išskirta pagal interesų svarbą:

- Gerbti žmogaus konstitucines teises ir laisves informacijos gavimo ir naudojimo srityje.
- Užtikrinti valstybės vidaus politikos saugą, kad Rusijos ir tarptautinei visuomenei būtų pateikiama patikima informacija apie Rusijos Federacijos vykdomą vidaus ir išorės politiką.
- Skatinti šiuolaikinių informacinių technologijų bei Rusijos Federacijos pramonės informavimo priemonių telekomunikacijų ir ryšių srityje vystymąsi, kad ši pramonė galėtų patenkinti poreikius tiek vidaus, tiek išorės rinkose.
- Apsaugoti informacinius išteklius nuo neteisėtos prieigos, užtikrinti informacijos perdavimo infrastruktūros saugą.

Rusijos doktrinos 9 straipsnyje išskiriamos tokios prioritetinės priemonės informacijos saugos srityje:

- sukurti ir įgyvendinti mechanizmus, padėsiančius įgyvendinti teisės normas, reguliuojančias santykius informacijos srityje, taip pat parengti teisinio informacijos apsaugos užtikrinimo koncepciją;
- sukurti ir įgyvendinti mechanizmus, padėsiančius padidinti valdžios vadovavimo valstybinių visuomenės informavimo priemonių darbui efektyvumą, įgyvendinti valstybinę informacinę politiką;

- priimti ir įgyvendinti federalines programas, kuriose būtų numatyta formuoti visiems prieinamus valstybinės valdžios įstaigų / organizacijų informacinius archyvus, didinti teisinę kultūrą ir piliečių kompiuterinį raštingumą, tobulinti Rusijos Federacijos bendrą informacinę erdvę, imtis kompleksinių veiksmų prieš informacinių karų grėsmes ir pan.;
- tobulinti personalo, dirbančio Rusijos Federacijos informacijos saugos srityje, rengimo sistemą;
- tobulinti valstybės standartus informatizavimo ir informacinės saugos srityje ir pan.

Mūsų nuomone, Rusijos doktrinoje nurodytų tikslų ir prioritetinių priemonių formuluotės yra ganėtinai deklaratyvios ir nekonkrečios. Taip teigia ir Lietuvos mokslininkai – Rusijos Federacijoje formaliai informacijos saugai skiriama nemažai dėmesio, įskaitant ir teisės aktus. Tačiau nuostatos yra deklaratyvios, todėl jos primena labiau šūkius, o ne konkrečias informacijos saugos užtikrinimo priemones (Štitilis et al., 2011). Taip pat, skirtingai negu Lietuvos programoje, nenustatyta jokių vertinimo kriterijų, pagal kuriuos būtų galima spręsti, ar ši Rusijos doktrina yra sėkmingai įgyvendinama. Е. К. Волчинская (2009) analizuodama valstybės vaidmenį užtikrinant informacijos apsaugą nurodo, kad, jos nuomone, dauguma Rusijos doktrinoje nurodytų priemonių yra neįgyvendinama, pvz., nesukurta valstybės politika šioje srityje, neparengta tikslinė federalinė programa.

Rusijos doktrinoje, skirtingai negu Lietuvos programoje, dar papildomai yra įtvirtinti ir valstybinės informacijos apsaugos metodai. Jie suskirstyti į teisinius, organizacinius-techninius ir ekonominius. Prie teisinių informacijos saugumo užtikrinimo metodų priskiriamas norminių teisės aktų, kurie reglamentuotų informacinius santykius, ir norminių metodinių dokumentų dėl informacijos saugumo užtikrinimo Rusijos Federacijoje kūrimas. Organizaciniams-techniniams metodams dėl informacijos saugumo užtikrinimo priskiriami: teisėsaugos organų sustiprinimas; informacijos apsaugos priemonių sukūrimas ir panaudojimas, jų efektyvumo kontrolė; apsaugotų telekomunikacinių sistemų vystymas, specialios programinės įrangos patikimumo didinimas; priemonių ir sistemų, galėsiančių apsaugoti informaciją nuo neteisėto – nesankcionuoto, prisijungimo ir pakenkimo, sunaikinimo ar pakeitimo, kūrimas ir pan. Ekonominiams informacijos saugumo užtikrinimo metodams priskiriami: informacijos saugumo užtikrinimo programų kūrimas ir jų finansavimo tvarkos nustatymas; darbų, susijusių su teisinių ir organizacinių-techninių informacijos apsaugos metodų įgyvendinimu, finansavimo sistemos sukūrimas; fizinių ir juridinių asmenų informacinės rizikos draudimo sistemos sukūrimas ir pan. Mūsų nuomone, toks valstybinės informacijos apsaugos metodų įtvirtinimas strateginiame dokumente yra perteklinis ir nereikalingas, nes svarbiausi būtini atlikti veiksmai tokio pobūdžio strateginiuose dokumentuose turėtų būti nustatomi priemonių dalyje.

Pažymėtina, kad Lietuvos programoje neišskiriama konkrečių institucijų kompetencija elektroninės informacijos saugos srityje, tiktai nurodoma, kurios Lietuvos institucijos ir už kokių konkrečiai programoje nustatytų tikslų ir uždavinių įgyvendinimą atsakingos. Už Lietuvos programos įgyvendinimo koordinavimą, Lietuvos programoje numatytų uždavinių ir jų vertinimo kriterijų reikšmių pokyčių peržiūrą ir programos atnaujinimą atsakinga Vidaus reikalų ministerija. Už Lietuvos programos tikslų ir užda-

vinių įgyvendinimą atsako institucijos ir įstaigos – Ministro Pirmininko Tarnyba, Ryšių reguliavimo tarnyba, Valstybinė duomenų apsaugos inspekcija, Policijos departamentas prie VRM, Krašto apsaugos ministerija, Susisiekimo ministerija, Finansų ministerija, Švietimo ir mokslo ministerija bei Ūkio ministerija.

Tuo tarpu Rusijos doktrinoje yra ganėtinai aiškiai atskirta įstatymų leidžiamosios, vykdomosios ir teisminės valdžios kompetencija informacijos saugos srityje. Detalizuojama, kokias funkcijas šioje srityje atlieka Rusijos Federacijos Prezidentas, Rusijos Federacijos Dūma, Vyriausybė, Rusijos Federacijos saugumo taryba, Rusijos Federacijos Prezidento ir Vyriausybės paskirti vykdomųjų institucijų subjektai, tarpinstitucinės ir valstybinės komisijos savivaldos institucijos, teismai ir kt.

Mūsų nuomone, siekiant formuoti ir įgyvendinti veiksmingą politiką elektroninės informacijos saugos srityje, Lietuvos programoje taip pat turėtų būti nurodyta ne tik kokia institucija yra atsakinga už konkrečios priemonės įgyvendinimą, bet taip pat aiškiai atskirtos kiekvienos institucijos funkcijos šioje srityje.

4. Pagrindiniai įstatymai ir kiti teisės aktai, reguliuojantys elektroninės informacijos saugą Lietuvoje ir Rusijoje

Šioje dalyje analizuojant pagrindinius įstatymus ir kitus teisės aktus, reguliuojančius elektroninės informacijos saugą Lietuvoje ir Rusijoje, tyrimo objektas apsiribos ne žemesnio kaip vyriausybės lygiu priimtais teisės aktais.

Atkreiptinas dėmesys, kad Lietuvoje elektroninės informacijos saugos santykiai tam tikra dalimi reguliuojami daugelyje įstatymų, Vyriausybės nutarimų, ministrų ar atitinkamos įstaigos vadovų pasirašytų įsakymų. Būtų galima paminėti keletą, mūsų nuomone, svarbesnių įstatymų, kuriuose fragmentiškai yra reglamentuoti šie santykiai: Lietuvos Respublikos elektroninių ryšių, Lietuvos Respublikos asmens duomenų teisinės apsaugos, Lietuvos Respublikos autorių teisių ir gretutinių teisių, Lietuvos Respublikos elektroninio parašo ir kt. įstatymuose. Tačiau šių įstatymų nuostatos, kiek tai susiję su elektroninės informacijos sauga, fragmentiškos, teisės normos nesusistemintos, trūksta vieno požiūrio, dalis svarbių visuomeninių santykių iš viso nereglamentuojama (pvz., ypatingos svarbos elektroninės informacijos infrastruktūros apsauga). Štitilis et al. (2011) atkreipia dėmesį, kad „<...> galiojantys teisės aktai neužtikrina visapusiško ir nuoseklaus tinklų ir elektroninės informacijos saugumo visuomeninių santykių reglamentavimo, nesudaro sąlygų vartotojų pasitikėjimui informacine visuomene ir saugios informacinės visuomenės plėtrai“. Manytume, kad šią problemą padėtų išspręsti pamatinio įstatymo, reglamentuojančio visuomeninius santykius, susijusius su elektroninės informacijos sauga, priėmimas. Deja, Lietuvoje iki šiol toks įstatymas nėra priimtas, nors jau 2006 m. gruodžio 6 d. Vyriausybės nutarimu Nr. 1211 buvo patvirtinta Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepcija[13] (toliau – Koncepcija).

13 Lietuvos Respublikos Vyriausybės 2006 m. gruodžio 6 d. nutarimas Nr. 1211 „Dėl Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepcijos patvirtinimo“. *Valstybės žinios*. 2006, Nr. 134-5081.

Koncepcijos 2 punkte numatyta, kad Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymas reglamentuos santykius, susijusius su elektroninių ryšių tinklų ir informacijos saugumu, sudarys sąlygas saugios informacinės visuomenės plėtrai, didins vartotojų pasitikėjimą informacine visuomene. 10 punkte detalizuota, kad Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatyme bus numatyta:

1. aiški valstybės institucijų struktūra tinklų ir informacijos saugumo srityje, kad nebūtų dubliuojamos institucijų funkcijos ir atsakingos institucijos veiksmingai bendradarbiautų;

2. nustatyti bendrieji tinklų ir informacijos saugumo reikalavimai, daugiausia skirti vartotojams apsaugoti nuo tinklų ir informacijos saugumo incidentų;

3. valstybės ir savivaldybių institucijų tinklų ir informacinių sistemų, saugaus informacijos perdavimo tarp valstybės ir savivaldybių institucijų, kritinių informacinių infrastruktūrų tinklų ir informacijos saugumo reikalavimai;

4. aiški tinklų ir informacijos saugumo lygio įvertinimo sistema, reglamentuojanti tinklų ir informacijos saugumo audito atlikimą, techninės ir programinės įrangos saugumo įvertinimą. Ši sistema daugiausia bus taikoma valstybės ir savivaldybių institucijų tinklams ir informacinėms sistemoms, kritinėms informacinėms infrastruktūroms, didesnių įmonių, taip pat informacinės visuomenės paslaugų teikėjų tinklams ir informacinėms sistemoms – t. y. tais atvejais, kai tinklų ir informacijos saugumas daugiausia užtikrinamas laikantis atitinkamos saugumo politikos.

Reikėtų atkreipti dėmesį, kad Koncepcijos 21 punkte nurodoma, kad numatomu įstatymu nebus siekiama pakeisti Lietuvos Respublikos baudžiamajame kodekse įtvirtintos nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui [14] sistemos. Jis sudarys galimybes ne tik reaguoti į jau įvykusius pažeidimus (nubausti asmenis), bet ir užtikrinti tokių pažeidimų prevenciją, užkirsti kelią neigiamiems jų padariniams. Taip pat aiškiai nustatys elgesio ribas – apibrėš veikas, kurios formaliai nėra kriminalizuotos (dėl to, kad Lietuvos Respublikos baudžiamasis kodeksas kai kurias veikas kriminalizuoja tik įtraukdamas papildomą požymį – padarytą žalą), bet yra aiškiai pavojingos – neteisėtas poveikis elektroniniams duomenims; neteisėtas poveikis informacinei sistemai; elektroninio pašto adreso rinkimas, platinimas, įsigijimas, naudojimas ar kitoks disponavimas elektroninio pašto adresu be naudotojo sutikimo tiesioginės rinkodaros tikslu ir panašiai, o už tokių veikų padarymą Lietuvos Respublikos administracinių teisės pažeidimų kodekse bus numatyta administracinė atsakomybė.

Jeigu Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymas būtų priimtas, jį būtų galima vadinti „holistinio elektroninės informacijos saugos teisinio reguliavimo apraiška“ (Štitilis, 2011). Deja, tenka konstatuoti, kad Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo priėmimas ypač užsitęsė. Kaip jau minėjome aukščiau, Koncepcija buvo patvirtinta jau 2006 m. gruodžio 6 d., taigi daugiau kaip prieš penkerius metus.

---

14 Lietuvos Respublikos baudžiamojo kodekso patvirtinimo ir įsigaliojimo įstatymas. Baudžiamasis kodeksas. *Valstybės žinios*. 2012, Nr. VIII-1968.

Lietuvos Respublikos Vyriausybės 2008–2012 metų programos įgyvendinimo priemonėse, patvirtintose Lietuvos Respublikos Vyriausybės 2009 m. vasario 25 d. nutarimu Nr. 189[15] buvo numatyta, kad Susisiekimo ministerija, Vidaus reikalų ministerija, Ryšių reguliavimo tarnyba turi parengti Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo projektą 2009 m. II ketvirtį. Tačiau nepavyko rasti informacijos, kad Lietuvos Respublikos Seime šiuo metu jau būtų užregistruotas tokio įstatymo projektas. Taigi šiuo metu Lietuvoje nėra įstatymo, kuris kompleksiškai reglamentuotų elektroninės informacijos saugos sritį (Štitilis et al., 2011).

Analizuodami elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos, patvirtintos Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimu Nr. 796[16], priedą matome, kad Vidaus reikalų ir Susisiekimo ministerijoms bei Ryšių reguliavimo tarnybai pavesta priimti esminius su elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimu susijusius reikalavimus, nustatančius specialius atitinkamą veiką ir teisinius santykius reglamentuojančius įstatymus (tarp jų Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymas). Tačiau šios užduoties įvykdymas bus pirmą kartą vertinamas tik 2015 m., o vėliau 2019 m., taigi, galima daryti prielaidą, jog tikėtina, kad Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo priėmimas nusikels dar mažiausiai porą metų.

Vienas iš pagrindinių įstatymų Rusijos Federacijoje, reguliuojančių elektroninės informacijos saugos sritį, yra 2006 m. liepos 27 d. Rusijos Federacijos federalinis įstatymas Nr. 149-FZ „Dėl informacijos, informatizacijos ir informacijos apsaugos“[17]. Šis federalinis įstatymas reglamentuoja santykius, kylančius:

- įgyvendinant teisę į informacijos paiešką, gavimą, perdavimą, kūrimą ir skleidimą;
- taikant informacines technologijas;
- užtikrinant informacijos apsaugą.

Rusijos Federacijoje, taip pat kaip ir Lietuvoje, yra nemažai įstatymų, kuriuose galima rasti nuostatų, susijusių su elektroninės informacijos saugos klausimais: Rusijos Federacijos federalinis įstatymas „Dėl ryšių“, Rusijos Federacijos federalinis įstatymas „Dėl masinės informacijos priemonių“, Rusijos Federacijos civilinio kodekso IV dalis ir kt. Taip pat nuostatų, susijusių su šia sritimi, galima rasti ir Rusijos Federacijos Prezidento įsakuose, Vyriausybės potvarkiuose, valstybiniuose ir tam tikros pramonės šakos standartuose ir kt.

---

15 Lietuvos Respublikos Vyriausybės 2009 m. vasario 25 d. nutarimas Nr. 189 „Dėl Lietuvos Respublikos Vyriausybės 2008–2012 metų programos įgyvendinimo priemonių patvirtinimo“. *Valstybės žinios*. 2009, Nr. 33-1268.

16 Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimas Nr. 796 „Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo“. *Valstybės žinios*. 2011, Nr. 83-4033; 2011, Nr.106 (atitaisymas).

17 Федеральный закон „Об информации, информационных технологиях и о защите информации“. Žiūrėta 2012 m. vasario 18 d. Prieiga per internetą: http://www.rg.ru/2006/07/29/informacia-dok.html.

Išanalizavę pagrindinius Lietuvos ir Rusijos Federacijos teisės aktus, reglamentuojančius elektroninės informacijos saugą, galime daryti išvadą, kad šiuo metu Lietuvos Respublikoje ir Rusijos Federacijoje yra priimti strateginiai dokumentai, kurie apibrėžia planuojamą valstybės politiką elektroninės informacijos saugos srityje, tačiau Lietuvos programoje nustatyti pakankamai konkretūs ir ambicingi, kai kurie galbūt realiai netgi sunkiai įgyvendinami, tikslai, uždaviniai ir programos vertinimo kriterijai, tuo tarpu Rusijos doktrinoje nurodytų tikslų ir prioritetinių priemonių formuluotės yra ganėtinai deklaratyvios ir nekonkrečios, taip pat, skirtingai negu Lietuvos programoje, nenustatyta jokių vertinimo kriterijų, pagal kuriuos būtų galima spręsti, ar ši Rusijos doktrina yra sėkmingai įgyvendinama. Abiejose lyginamose valstybėse yra daug įstatymų ir poįstatyminių teisės aktų, kuriuose yra įtvirtintos pavienės nuostatos, reglamentuojančios elektroninės informacijos saugos santykius, tačiau Rusijos Federacijoje yra priimtas vienas pagrindinis įstatymas, reguliuojantis elektroninės informacijos saugos sritį, tuo tarpu Lietuvoje dar iki šiol nėra priimtas įstatymas, kuriuo visapusiškai ir nuosekliai būtų reglamentuoti visuomeniniai santykiai, susiję su elektroninės informacijos sauga, nors koncepcija dėl šio įstatymo priėmimo buvo patvirtinta jau daugiau kaip prieš penkerius metus. Mūsų nuomone, siekiant užtikrinti visapusišką ir veiksmingą elektroninės informacijos saugą, būtina kiek įmanoma greičiau patvirtinti Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymą, neatidėliojant jo priėmimo dar keletui metų, kaip buvo daroma iki šiol.

Išvados

1. Rusijos Federacijos teisės aktai, reglamentuojantys elektroninės informacijos saugą, yra labai panašūs į Lietuvos Respublikos teisės aktus, tačiau Rusijos įstatymai numato griežtesnes apsaugos priemones elektroninės informacijos saugos srityje.

2. Lietuvos Respublikos ir Rusijos Federacijos teisės aktų analizė elektroninės informacijos saugos srityje parodė, kad šiuo metu abiejose valstybėse yra priimti strateginiai dokumentai, kurie apibrėžia planuojamą valstybės politiką šioje srityje, tačiau Lietuvos programoje, siekiant formuoti ir įgyvendinti veiksmingą politiką elektroninės informacijos saugos srityje (kaip šiuo metu yra padaryta Rusijos doktrinoje) reikėtų aiškiai išskirti konkrečių institucijų (tiek valstybinių, tiek savivaldos institucijų) kompetencijas elektroninės informacijos saugos srityje.

3. Siekiant tinkamai užtikrinti elektroninės informacijos saugą Lietuvoje turėtų būti padaryta išsamesnė esamos būklės analizė, įvardinant galimas grėsmes, dėl kurių atitinkami tikslai ir uždaviniai, numatyti Lietuvos programoje, gali būti nepasiekti.

4. Lietuvos programoje nustatytos konkrečios ir ambicingos vertinimo kriterijų reikšmės, tik nežinia, kiek realiai įgyvendinamos, nes daugelis indikatorių iki Lietuvos programos priėmimo iš viso nebuvo vertinami. Atsižvelgiant į tai, kad daugelio vertinimo kriterijų reikšmės nėra žinomos, Lietuvos programoje reikėjo nustatyti, kad pirmasis įvertinimas būtų atliktas daug anksčiau negu 2015 m., siekiant nustatyti pirmines atitinkamų rodiklių reikšmes (t. y. įvertinti esamą situaciją), o tuomet jau nuosekliai būtų galima nustatyti ir reikšmes, kurias reikėtų pasiekti tolesniais metais.

5. Abiejose lyginamose valstybėse yra daug įstatymų, kuriuose yra įtvirtintos pavienės nuostatos, reglamentuojančios elektroninės informacijos saugos santykius, tačiau Rusijos Federacijoje yra priimtas vienas pagrindinis įstatymas, reguliuojantis elektroninės informacijos saugos sritį, tuo tarpu Lietuvoje dar iki šiol nėra priimtas įstatymas, kuriuo visapusiškai ir nuosekliai būtų reglamentuoti visuomeniniai santykiai, susiję su elektroninės informacijos sauga, nors koncepcija dėl šio įstatymo priėmimo buvo patvirtinta jau daugiau kaip prieš penkerius metus. Mūsų nuomone, siekiant užtikrinti visapusišką ir veiksmingą elektroninės informacijos saugą, būtina kiek įmanoma greičiau patvirtinti Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymą, neatidėliojant jo priėmimo dar keletui metų, kaip buvo nuolat daroma iki šiol.

Literatūra

Доктрина информационной безопасности Российской Федерации. Maskva, 2000. Žiūrėta 2012 m. spalio 10 d. Prieiga per internetą: http://www.scrf.gov.ru/documents/5.html.

Europos Komisijos 2009 m. kovo 30 d. komunikatas COM/2009/149 Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui dėl ypatingos svarbos informacinės infrastruktūros apsaugos „Europos apsauga nuo didelio masto kibernetinių antpuolių ir veiklos sutrukdymo – geresnė parengtis, didesnis saugumas ir atsparumas“. Žiūrėta 2012 m. spalio 10 d. Prieiga per internetą: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:LT:HTML.

Europos Komisijos 2011 m. kovo 31 d. komunikatas COM/2011/163 Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui dėl ypatingos svarbos informacinės infrastruktūros apsaugos „Visuotinio kibernetinio saugumo užtikrinimas. Laimėjimai ir tolesni veiksmai“. Žiūrėta 2012 m. spalio 10 d. Prieiga per internetą: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:LT:HTML.

Europos Komisijos 2008 m. liepos 14 d. ataskaita COM/2008/448 Tarybai parengta pagal 2005 m. vasario 24 d. Tarybos pamatinio sprendimo dėl atakų prieš informacines sistemas 12 straipsnį. Žiūrėta 2012 m. spalio 10 d. Prieigs per internetą: http://eur-law.eu/LT/Komisijos-ataskaita-Tarybai-parengta-2005-m-vasario-24,480987,d.

Europos Komisija: pranešimas spaudai. Briuselis, 2012. Žiūrėta 2012 m. salio 10 d. Prieiga per internetą:
http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/949&format=HTML&aged=0&language=LT&guiLanguage=en.

Europos Parlamento ir Tarybos 2011 m. birželio 8 d. reglamentas 2011/580/ES, kuriuo iš dalies keičiamas Reglamentas 2004/460/EB, įsteigiantis Europos tinklų ir informacijos apsaugos agentūrą, jos veiklos trukmės atžvilgiu. Žiūrėta 2012 m. spalio 10 d. Prieiga per internetą: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:165:0003:0004:LT:PDF.

Федеральный закон „Об информации, информационных технологиях и о защите информации“. Žiūrėta 2012 m. vasario 18 d. Prieiga per internetą: http://www.rg.ru/2006/07/29/informacia-dok.html.

Kiškis, M. et al. (2006). *Teisės informatika ir informatikos teisė*. Vilnius: Mykolo Romerio universitetas.

Lietuvos Respublikos baudžiamojo kodekso patvirtinimo ir įsigaliojimo įstatymas. Baudžiamasis kodeksas. *Valstybės žinios*. 2012, Nr. VIII-1968.

Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimas Nr. 796 „Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo“. *Valstybės žinios*. 2011, Nr. 83-4033; 2011, Nr.106 (atitaisymas).

Lietuvos Respublikos Vyriausybės 2006 m. gruodžio 6 d. nutarimas Nr. 1211 „Dėl Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepcijos patvirtinimo“. *Valstybės žinios*. 2006, Nr.134-5081.

Lietuvos Respublikos Vyriausybės 2009 m. vasario 25 d. nutarimas Nr. 189 „Dėl Lietuvos Respublikos Vyriausybės 2008–2012 metų programos įgyvendinimo priemonių patvirtinimo“. *Valstybės žinios*. 2009, Nr. 33-1268.

Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimas Nr. 952. „Dėl duomenų saugos valstybės ir savivaldybių informacinėse sistemose“. *Valstybės žinios*. 2007, Nr. 49-1891.

List of OECD Member countries - Ratification of the Convention on the OECD. Paris, 1960. Žiūrėta 2012 m. spalio 10 d. Prieiga per internetą: http://www.oecd.org/general/listofoecdmembercountriesratificationoftheconventionontheoecd.htm.

Petrauskas, R. et al. (2006).International Legislative Regulation Provisions Concerning the Security of Information Systems and Information. Implementation of the Provisions in Lithuania. - Databases and Information Systems: Seventh International Baltic Conference on Databases and Information Systems. Communications, Materials of Doctoral Consortium. Vilnius, Technika.

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. Paris, 2002. Žiūrėta 2012 m. spalio 10 d. Prieiga per internetą: http://www.oecd.org/internet/interneteconomy/15582260.pdf.

Schjolberg, S., Ghernaouti-Hele, S. (2011). A Global Treaty on Cybersecurity and Cybercrime, Geneva. Žiūrėta 2012 m. spalio 10 d. Prieiga per internetą: .http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf.

Synopticom Dėl kenkėjiškų programų per metus nukentėjo daugiau nei pusė interneto vartotojų Vilnius, 2010. Žiūrėta 2012 m. spalio 10 d. Prieiga per internetą: https://www.synopticom.com/?p=224.

Synopticom Virusai ir kenkėjiškos programos trukdo dirbti daugiau nei pusei vartotojų Lietuvoje. Vilnius, 2010. Žiūrėta 2012 m. spalio 15 d. Prieiga per internetą: https://www.synopticom.com/?p=224.

Štitilis, D. (2011). *Elektroniniai nusikaltimai: metodinė priemonė*. Vilnius: Mykolo Romerio universitetas.

Štitilis, D., Paškauskas, Ž. (2007). Valstybės elektroninės informacijos saugos strategija – vienas iš pagrindinių elektroninės informacijos saugos reguliavimo instrumentų: lyginamoji analizė. *Jurisprudencija*. 2 (92).

Štitilis, D. et al. (2011). Teisinė aplinka siekiant išvengti tapatybės vagystės elektroninėje erdvėje: JAV ir Lietuvos teisės aktų lyginamoji analizė. *Socialinės technologijos*. 1(1).

Štitilis, D. *et al.* (2011). *Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai*. Vilnius: Mykolo Romerio universitetas.

Волчинская, Е. К. (2009). Роль государства в обеспечении информационной безопасности. Maskva. Žiūrėta 2012 m. vasario 18 d. Prieiga per internetą: rniiis.ru/article-sip409/volchinskaya.doc.

THE REGULATION OF THE SECURITY OF ELECTRONIC INFORMATION IN LITHUANIA AND RUSSIA: THE COMPARATIVE ASPECTS

Darius Štitilis

Mykolas Romeris University, Lithuania, stitilis@mruni.eu

Valdas Klisauskas

Mykolas Romeris University, Lithuania, v.klisauskas@mruni.eu

Summary. *Cybercrime has become a global phenomenon, which is causing more harm to individual citizens, organizations, society and the state. Most countries in the world compare cybercrime with such offences as terrorism and drug trafficking due to its risks and profitability. Therefore, the legal regulation of cybercrime is one of the most relevant problems in the world, including Lithuania and our neighbouring country, Russia. So far cybercrime analysis in scientific literature has been rather limited. We have not succeeded in finding a comparison between the regulatory practices of cybercrime in the Russian Federation and the Republic of Lithuania in any of the references.*

The main goal of the thesis paper is to analyse and to compare the electronic information security legal framework of the Russian Federation and the Republic of Lithuania.

The article consists of two parts. The first part deals with the comparative aspect of strategic documents—the program governing electronic information protection in Lithuania and the Russian Federation.

The second part of the article examines the comparative aspect of electronic information protection legislative, legal framework Republic of Lithuania and the Russian Federation. It was found that at the moment in both countries there is a strategic document which defines the planned state policy in this area, but the lack of a Lithuanian Law which can fully and consistently regulate social relations in relation to electronic information security.

Several different approaches have been used in the research. The authors have used a comparative method to investigate the Lithuanian and Russian legal framework for the security of electronic information. Empirical analysis of legal documents was used to determine the legal regulation of the security of electronic information in Lithuania and Russia. Legal acts of the Republic of Lithuania and the Russian Federation have been analysed. Having analysed the official documents, the method allows identification and description of the relationship between the valid legal regulations accurately. Using literature resources the authors have used the deductive method, which allows drawing sufficiently reliable conclusions. The latest scientific literature and dictionaries have been used to study the definitions.

Keywords: *security of electronic information, legal regulation.*