ISSN 2029-7564 (online)
SOCIALINĖS TECHNOLOGIJOS
SOCIAL TECHNOLOGIES
2013, 3(1), p. 189–207

KIBERNETINIO SAUGUMO TEISINIS REGULIAVIMAS: KIBERNETINIO SAUGUMO STRATEGIJOS

Darius Štitilis

Mykolo Romerio universitetas, Lietuva, stitilis@mruni.eu

doi:10.13165/ST-13-3-1-13

Santrauka

Tikslas *– išanalizuoti kibernetinio saugumo teisinį reguliavimą (strategijas) ES ir šio teisinio reguliavimo kontekste įvertinti Lietuvos kibernetinio saugumo programą.*

Metodologija *– tyrimui atlikti taikyti keli skirtingi metodai: tirdamas ES teisinę bazę dėl kibernetinio saugumo (kiek tai susiję su strategijomis), autorius pasitelkė lyginamąjį metodą. ES bei pasirinktų užsienio valstybių kibernetinio saugumo teisinio reguliavimo nustatymui taikytas empirinis teisinių dokumentų analizės metodas. Buvo tiriami ES, pasirinktų valstybių ir Lietuvos dokumentai dėl kibernetinio saugumo strategijų. Šis metodas leidžia ištyrus oficialius dokumentus tiksliai nustatyti ir aprašyti atitinkamo santykio galiojantį teisinį reguliavimą. Naudodamas mokslinės literatūros šaltinius autoriaus taikė dedukcijos metodą, leidžiantį daryti pakankamai patikimas išvadas. Taip pat autorius pasitelkė naujausią mokslinę literatūrą.*

Rezultatai *– tyrimas atskleidė, jog Lietuvos kibernetinio saugumo strategija per daug abstrakti ir neužtikrina tų pagrindinių tikslų bei uždavinių, kurie akcentuojami ES strategijoje bei atskirų užsienio valstybių kibernetinio saugumo strategijose. Be to, Lietuvoje trūksta pamatinių teisės normų kibernetinio saugumo srityje. Prieš kelis metus buvo parengtas Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo projektas, tačiau šis projektas taip ir nebuvo priimtas.*

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, kibernetinio saugumo strategijas.*

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

Užsienio valstybių praktikos analizė apsiribojo trijų pagrindinių pasirinktų valstybių kibernetinio saugumo strategijų analize bei kitų autorių atlikto tyrimo pristatymu. Tyrimo metu taip pat nebuvo detaliai analizuojamas teisės normų kibernetinio saugumo srityje įgyvendinimas.

Praktinė reikšmė – *tyrimo rezultatai gali būti pritaikomi kuriant naujas teisės normas ar atliekant egzistuojančių teisės normų pakeitimus, kiek tai susiję su kibernetiniu saugumu. Atsižvelgiant į išsakytą Kibernetinio saugumo programos kritiką, ši programa galėtų būti papildyta ir sukonkretinta. Į nurodytas teisinio reguliavimo problemas galėtų būti atsižvelgta ir kuriant naują Kibernetinio saugumo įstatymo projektą.*

Originalumas / vertingumas – *straipsnyje pristatomas tyrimas yra naujas Lietuvoje. Mokslinių darbų dėl kibernetinio saugumo teisinio reguliavimo (strategijų) kol kas trūksta ne tik Lietuvoje, bet ir užsienyje.*

Raktažodžiai: *kibernetinis saugumas, teisinis reguliavimas.*

Tyrimo tipas: *tyrimo pristatymas, požiūrio pristatymas.*

1. Įvadas

Internetas (arba elektroninė erdvė) turi vis daugiau įtakos kasdieniniam gyvenimui, taip pat ir globaliai ekonomikai. Šiuolaikinių organizacijų vidiniai valdymo procesai yra neįmanomi ir neįsivaizduojami be informacinių technologijų ir informacinių sistemų bei interneto prieigos. Interneto, informacinių technologijų plėtra, informacijos perkėlimas į elektroninę erdvę didina informacinių procesų ir veiklos kokybę, užtikrina geresnį konkurencingumą bei efektyvumą. Informacija internete, anot P. Rosenzweigo, keičiamasi fiziniame pasaulyje precedento neturinčiu greičiu ir formomis[1]. Tačiau tai sukelia ir neigiamas pasekmes, tokias kaip svarbios elektroninės informacijos praradimas ar net skatina elektroninį nusikalstamumą. Elektroninės erdvės globalumas sukūrė beprecedentes sąlygas daryti nusikaltimus iš bet kurio pasaulio taško, kuriame yra internetas. Todėl labai svarbu apsisaugoti nuo elektroninių nusikaltimų, vykdomų pasitelkiant internetą. Kibernetinis saugumas tampa vienu iš pagrindinių tikslų, turint omenyje, kad grėsmės elektroninėje erdvėje kyla ne tik atskiriems vartotojams, bet net valstybėms. Kibernetinį saugumą Schjolberg ir Ghernaouti-Hele įvardija kertiniu informacinės visuomenės akmeniu.

Joel P. Trachtman kibernetinį saugumą apibrėžia kaip apsaugą nuo netinkamo interneto infrastruktūros naudojimo ir piktnaudžiavimo (žlugdymo). Pagal D. Shoemakerį ir A. Conkliną, kibernetinis saugumas susijęs su procesų, susijusių su kylančių kibernetinių grėsmių identifikavimu bei sąnaudomis pagrįstų kontrapriemonių taikymu, kūrimu ir palaikymu[2].

1 Rosenzweig, P. 2013. *Cyberwarfare: how conflicts in cyberspace are challenging America and changing the world*. Library of Congress Cataloging, p. 22.

2 Shoemaker, D. and Conklin, A. 2012. *Cybersecurity: the Essential body of knowledge*. Course technology, p. 11.

Kibernetinis saugumas – labai svarbi ir specifinė veiklos rūšis, kuri taip pat reikalauja nuoseklaus ir detalaus teisinio reglamentavimo. Vieni iš pagrindinių dokumentų šioje srityje – strateginiai dokumentai, kibernetinio saugumo strategijos[3]. Pastaruoju metu visos pasaulio valstybės vis daugiau dėmesio skiria kibernetiniam saugumui ir teisiniam reguliavimui, ne išimtis ir Lietuvos Respublika. Lietuva kibernetinio saugumo užtikrinimui yra priėmusi Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metų programą[4]. 2012 metais Europos Komisija priėmė vieną iš svarbiausių pastarojo meto dokumentų kibernetinio saugumo srityje – Kibernetinio saugumo strategiją, tai pat pasiūlė direktyvos projektą. Kai kuriose užsienio valstybėse pastaraisiais metais taip pat priimti strateginiai dokumentai kibernetinio saugumo srityje.

Todėl straipsnio **tikslas** – pristatyti pagrindinius strateginius pastarųjų metų dokumentus kibernetinio saugumo srityje bei išanalizuoti pasirinktų užsienio valstybių kibernetinio saugumo strateginio teisinio reguliavimo praktiką. **Tyrimo objektas** – ES norminiai dokumentai – kibernetinio saugumo strategijos, pasirinktų valstybių kibernetinio saugumo strategijos ir Lietuvos kibernetinio saugumo programa. **Tyrimo metodai**: lyginamasis, teisinių dokumentų analizės, dedukcijos.

Kibernetinio saugumo strateginio teisinio reguliavimo klausimais užsienio mokslininkų darbų labai mažai, Lietuvoje D. Štitilis ir Ž. Paškauskas yra nagrinėję informacijos saugos strategiją iki 2008 metų. Naujoji ES kibernetinio saugumo strategija, taip pat Lietuvos kibernetinio saugumo programa praktiškai nenagrinėtos.

2. Europos Sąjungos kibernetinio saugumo strategija

Elektroninės informacijos sauga (kibernetinis saugumas) akcentuojama ne viename Europos Sąjungos dokumente. Jau 2001 metais Europos Sąjungos teisės aktuose yra nurodoma, kad informacinės ir telekomunikacinės technologijos tapo šiuolaikinės visuomenės gyvenimo kamienu ir nuo jų vis labiau yra priklausomi socialiniai ir ekonominiai visuomenės gerovės aspektai[5], o 2006 metais atkreipė ypatingą dėmesį į saugios Europos kibernetinės erdvės sukūrimą pasitelkiant visus socialinius valdžios partnerius[6]. Didžiuliai informacijos kiekiai yra saugomi privačių įmonių duomenų centruose,

---

3 Mitrakas A. 2006. Information Security Law in Europe: Risks Checked . *Information & Communications Technology Law* 15(1), p. 36.

4 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).

5 Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. Network and Information Security: Proposal for A European Policy Approach. COM/2001/298 [interaktyvus]. Briuselis, 2001 [žiūrėta 2013-05-20]. < http://eur-lex.europa.eu/LexUriServ/site/en/com/2001/com2001_0298en01.pdf>.

6 Komisijos komunikatas Tarybai, Europos Parlamentui, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui. Saugios informacinės visuomenės strategija – „Dialogas, partnerystė ir teisių suteikimas“.COM/2006/251 [interaktyvus]. Briuselis, 2006 [žiūrėta 2013-05-20]. <http://eurlex.europa.eu/Notice.do?mode=dbl&lang=en&ihmlang=en&lng1=en,lt&lng2=cs,da,de,el,en,es,et,fi,fr,hu,it,lt,lv,nl,pl,pt,sk,sl,sv,&val=427504:cs>.

valstybės institucijų duomenų saugyklose ir informacinių sistemų duomenų bazėse. Tokios informacijos paviešinimas, nesavalaikis panaudojimas ar sugadinimas gali sukelti didžiules problemas ir ženklius piniginius nuostolius verslo organizacijoms ar viešojo administravimo subjektams.

Europos Sąjungos valstybės ypatingą dėmesį atkreipia į tai, kad reikalingas glaudesnis Sąjungos šalių narių bendradarbiavimas kovojant su nusikaltimais elektroninėje erdvėje, taip pat užtikrinant kibernetinės erdvės bei „ypatingos svarbos informacinės infrastruktūros" apsaugą nuo kibernetinių išpuolių. Europos Sąjungos dokumentuose pažymima, kad „ypatingos svarbos informacinės infrastruktūros objektai gyvybiškai būtini ES ekonomikos ir visuomenės plėtrai", o informacinių technologijų ir interneto plėtra (skvarba) gerina ekonominius rodiklius, užtikrina visuomenės socialinės gerovės augimą bei piliečių gyvenimo kokybę.

Pastaraisiais metais Europos Sąjungoje kibernetinio saugumo sričiai skiriamas ypatingas dėmesys. 2012 m. Europos Komisija paskelbė konsultaciją kibernetinio saugumo teisinio reguliavimo srityje. Konsultacijoje labai aktyviai dalyvavo tiek viešojo sektoriaus, tiek privataus sektoriaus subjektai.

2013 m. vasario 7 d. Europos Komisija ir Sąjungos vyriausioji įgaliotinė užsienio reikalams ir saugumo politikai paskelbė kibernetinio saugumo strategiją[7] (toliau – Kibernetinio saugumo strategija) kartu su Komisijos direktyvos dėl tinklų ir informacinių sistemų saugumo pasiūlymu[8].

Kibernetinio saugumo strategija „Atvira, saugi ir patikima kibernetinė erdvė" yra išsami ES vizija, kaip geriausiai užirsti kelią kibernetinės veiklos sutrikdymui bei atakoms ir kokių atsakomųjų priemonių imtis. Taip siekiama remti europines laisvės ir demokratijos vertybes ir užtikrinti saugų skaitmeninės ekonomikos augimą. Konkrečiais veiksmais siekiama didinti informacinių sistemų atsparumą elektroniniams nusikaltimams ir stiprinti ES tarptautinę kibernetinio saugumo politiką ir kibernetinę gynybą.

Išskiriami šie pagrindiniai kibernetinio saugumo principai[9]:

1. Pagrindinių žmogaus teisių, nuomonės reiškimo laisvės, privatumo ir asmens duomenų apsauga

Kibernetinis saugumas gali būti efektyvus tik tuo atveju, jei paremtas pagrindinių teisių ir laisvių apsauga, taip pat grįstas esminėmis ES vertybėmis. Atitinkamai, individų teisės nageli būti užtikrintos be saugių tinklų ir sistemų. Bet koks informacijos

7 Joint Communication to the European Parliament, the Council, the European Ecomonic and Social Committee and the Committee of Regions „Cybersecurity strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN/2013/1 final [interaktyvus]. Briuselis, 2013 [žiūrėta 2013-05-20]. <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667>.

8 Proposal for a Directive of European parliament and the Council concerning measures to ensure a high common level of network and information security across the Union, COM/2013/48 final [interaktyvus]. Briuselis, 2013 [žiūrėta 2013-05-20]. <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1666>.

9 Joint Communication to the European Parliament, the Council, the European Ecomonic and Social Committee and the Committee of Regions „Cybersecurity strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN/2013/1 final. [interaktyvus]. Briuselis, 2013 [žiūrėta 2013-05-20]. <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667>, p. 1.2.

dalinimasis kibernetinio saugumo tikslais, kai įtraukti asmens duomenys, turi būti vykdomas laikantis ES duomenų apsaugos reguliavimo ir užtikrinti visapusišką individų teisių apsaugą šioje srityje.

2. Prieiga visiems

Ribota prieiga prie interneto ar tokios prieigos nebuvimas sukelia nepatogumus piliečiams. Kiekvienas turi turėti prieigą prie interneto bei informacijos. Interneto integralumas bei saugumas turi būti garantuojamas, kad būtų užtikrinta saugi prieiga visiems.

3. Demokratinis ir efektyvus valdymas

Skaitmeninis pasaulis nėra kontroliuojamas vienos struktūros (bendrovės). Šiuo metu yra keletas „žaidėjų“, kurių daugelis yra komerciniai arba nevyriausybiniai dariniai ir kurie įsitraukę į kasdieninį interneto resursų valdymą, protokolų ir standartų internetui kūrimą. Pabrėžtina tokių „žaidėjų“ svarba dabartiniame interneto valdymo modelyje ir parama šiam daugialypio valdymo požiūriui.

4. Bendra atsakomybė užtikrinant saugumą

Didėjanti priklausomybė nuo informacijos ir komunikacijų technologijų suponavo pažeidžiamas vietas, kurios turi būti išanalizuotos, sumažintos ir apgintos. Tiek viešasis sektorius, tiek privačios įmonės, tiek individualūs vartotojai turi pripažinti šią bendrą atsakomybę, imtis apsaugos priemonių ir, jei reikia, – užtikrinti koordinuotus veiksmus, siekiant sustiprinti kibernetinį saugumą.

Kibernetinio saugumo strategijoje akcentuojami penki strateginiai prioritetai[10]:

1. Pasiekti kibernetinį atsparumą;
2. Radikaliai sumažinti elektroninių nusikaltimų skaičių;
3. Sukurti kibernetinės gynybos politiką ir pajėgumus, kiek tai susiję su bendra saugumo ir gynybos politika;
4. Plėtoti pramonės ir technologinius išteklius, skirtus kibernetiniam saugumui užtikrinti;
5. Sukurti nuoseklią tarptautinę elektroninės erdvės politiką ir remti pagrindines ES vertybes.

Toliau kiekvienas iš šių prioritetų aptartinas atskirai.

1. Pasiekti kibernetinį atsparumą

Norint užtikrinti kibernetinį atsparumą, tiek viešasis, tiek privatus sektorius turi tiek vystyti kibernetinio atsparumo galimybes, tiek glaudžiai bendradarbiauti tarpusavyje. Šiame kontekste paminėtina ENISA, kuri buvo įkurta 2004 metais, taip pat daugelis teisinio reguliavimo priemonių, skirtų valdyti rizikas elektroniniuose ryšiuose ar apsaugoti asmens duomenis. Tačiau nepaisant visų priemonių, egzistuoja daugelis spragų vi-

10 Joint Communication to the European Parliament, the Council, the European Ecomonic and Social Committee and the Committee of Regions „Cybersecurity strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN/2013/1 final [interaktyvus]. Briuselis, 2013 [žiūrėta 2013-05-20]. <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667>, p. 2.

soje ES, ypatingai susijusių su nacionaliniais pajėgumais tarptautinių incidentų atveju, taip pat susijusių su privataus sektoriaus įsitraukimu sprendžiant kibernetinio saugumo grėsmes. Dėl to Kibernetinio saugumo strategija siejama su teisinio reguliavimo siūlymais, įskaitant:

- Minimalių bendrųjų reikalavimų nacionalinėms informacijos infrastruktūroms sukūrimą. Valstybės narės būtų įpareigotos paskirti kompetentingas institucijas, įkurti gerai veikiančius CERT, priimti nacionalines informacijos infrastruktūros strategijas ar atlikti kitus veiksmus.
- Įkurti koordinuotus prevencijos, aptikimo bei reagavimo mechanizmus, įgalinančius dalintis informacija ir tarpusavyje bendradarbiauti kompetentingas nacionalines institucijas.
- Gerinti privataus sektoriaus įsitraukimą ir pasirengimą. Kadangi didžiąją daugumą tinklų ir informacinių sistemų valdo privatūs subjektai / bendrovės, privataus sektoriaus įsitraukimas į kibernetinio saugumo užtikrinimą yra kritiškai svarbus.

2. Radikaliai sumažinti elektroninių nusikaltimų skaičių

Kuo daugiau gyvename skaitmeniniame pasaulyje, tuo daugiau sudarome galimybių elektroniniams nusikaltėliams veikti. Elektroniniai nusikaltimai yra viena iš labiausiai augančių nusikaltimų rūšių. Elektroniniai nusikaltėliai tampa vis pažangesni. Elektroniniai nusikaltimai santykinai pasižymi tuo, kad rizika dažniausiai maža, o pelnas didelis. Nusikaltėliai pasinaudoja tuo, kad elektroninėje erdvėje susekti nusikaltėlio pėdsakus yra gana sunku. Be to, elektroniniams nusikaltimams neegzistuoja valstybių sienos. Dėl to teisėsaugos institucijos turi bendradarbiauti tarpusavyje, keistis informacija ir veiksmais, tam kad duotų tinkamą atkirtį šiai augančiai grėsmei.

Dėl to teigiama, kad ES turi būti taikomi griežti ir efektyvūs įstatymai, nukreipti prieš elektroninius nusikaltimus. Paminėtina, kad Konvencija dėl elektroninių nusikaltimų yra vienintelis teisiškai įpareigojantis tarptautinis dokumentas elektroninių nusikaltimų srityje, kuris sukuria reikiamą sistemą prieš elektroninius nusikaltimus, kurią turi įgyvendinti prie konvencijos prisijungusios valstybės. Tačiau ir Europos Komisija turi imtis atitinkamų veiksmų, įskaitant direktyvų ar kitų dokumentų elektroninių nusikaltimų srityje išleidimą / tobulinimą ar raginimą valstybes ratifikuoti Konvenciją dėl elektroninių nusikaltimų.

3. Sukurti kibernetinės gynybos politiką ir pajėgumus, kiek tai susiję su bendra saugumo ir gynybos politika

Kibernetinio saugumo pastangos ES taip pat apima ir kibernetinės gynybos dimensiją. Norint užtikrinti informacijos ir komunikacijos sistemų atsparumą, kibernetinės gynybos pajėgumų vystymas turi būti koncentruotas į aptikimą, atsaką ir resursų atkūrimą po kibernetinių atakų. Šiame kontekste labai svarbi kibernetinės gynybos politika ir sugebėjimų duoti atkirtį kibernetinėms atakoms vystymas. Ypatingai turi būti vystoma sinergija tarp privataus sektoriaus ir valstybinio sektoriaus tikslu apsaugoti kibernetinius resursus nuo kibernetinių atakų.

4. Plėtoti pramonės ir technologinius išteklius, skirtus kibernetiniam saugumui užtikrinti

ES turi puikias tyrimo ir vystymo galimybes, tačiau dauguma pasaulio technologijų lyderių, kuriančių inovatyvius ICT produktus ir paslaugas, yra įsikūrė už ES ribų. Dėl to kyla rizika, kad Europa pasidarys priklausoma nuo ICT produktų, kildinamų ne Europoje, taip pat nuo saugumo sprendimų, kildinamų ne iš Europos. Todėl Europoje daugiau turi būti vystomi kibernetinio saugumo sprendimai.

5. Sukurti nuoseklią tarptautinę elektroninės erdvės politiką ir remti pagrindines ES vertybes

Komisija turi vystyti tinkamą elektroninės erdvės politiką, kuri užtikrintų geresnį tarptautinių partnerių ir organizacijų įsitraukimą ir glaudesnį bendradarbiavimą, taip pat glaudesnius ryšius su bendruomenėmis ir privačiu sektoriumi.

Vienas iš pagrindinių ES tarptautinės elektroninės erdvės politikos aspektų būtų skatinti, kad elektroninė erdvė būtų laikoma laisvės vieta, taip pat vieta, kurioje pasireiškia žmogaus teisės ir laisvės.

Funkcijos ir atsakomybės pagal ES Kibernetinio saugumo strategiją

Šiuolaikinėje visuomenėje kibernetiniai incidentai neturi sienų. Visi dalyviai, tiek nacionaliniu, tiek ES lygiu, turi dirbti kartu, siekiant užtikrinti kibernetinį saugumą. Kadangi gali būti taikomi skirtingi teisės aktai ir skirtingos jurisdikcijos, vienas iš pagrindinių ES uždavinių yra išgryninti visų pagrindinių „žaidėjų“ vaidmenis ir atsakomybes.

Šiuo metu centralizuotos europinės priežiūros koncepcija nepalaikoma. Manoma, kad nacionalinės vyriausybės yra geriausia, kas gali organizuoti kibernetinių atakų prevenciją bei atsaką į šias atakas, taip pat sukurti ryšius su privačiu sektoriumi. Be abejo, dėl galimos tarptautinės rizikų kilmės efektyvus nacionalinis atsakas dažnai reikalautų ES lygio įsitraukimo.

ES kibernetinio saugumo strategijoje yra išskiriami trys lygiai, kuriais būtų veikiama, siekiant užtikrinti kibernetinį saugumą: nacionalinis lygis, ES lygis ir tarptautinis lygis.

Nacionaliniu lygiu teigiama, kad valstybės narės turi turėti atitinkamas struktūras elektroninių nusikaltimų ir gynybos srityje. Šios struktūros turėtų užtikrinti reikiamus pajėgumus kovojant su kibernetiniais incidentais. Koordinavimo veiklą šioje srityje turėtų vykdyti ministerijos. Kibernetinio saugumo strategijose valstybės narės turėtų nustatyti įvairių nacionalinių institucijų funkcijas. Taip pat turėtų būti užtikrinamas reikiamas apsikeitimas informacija ne tik tarp valstybės institucijų, bet ir su privačiu sektoriumi. Kibernetinių incidentų atveju turėtų būti užtikrinamas atitinkamų saugumo planų veikimas, įskaitant ir atitinkamų funkcijų bei atsakomybių nustatymą.

ES mastu taip pat yra nemažai institucijų, veikiančių kibernetinio saugumo srityje. Atitinkamai, ENISA, Europolas ir EDA yra institucijos, aktyviai veikiančios kibernetinio saugumo srityje. Ypač svarbus yra bendradarbiavimas tarp šių institucijų tokiose srityse kaip rizikos valdymas, mokymai, apsikeitimas geriausia praktika ir kt.

Tarptautiniu mastu labai svarbu koordinuoti tarpusavio veiksmus kibernetinio saugumo srityje. Tarptautiniu mastu Europos Komisija remia pagrindines vertybes ir palaiko viešą bei skaidrų kibernetinių technologijų naudojimą. Europos Komisija taip pat pasisako už bendradarbiavimą su pagrindiniais tarptautiniais partneriais ir organizacijomis: Europos Taryba, EBPO ir kt.

Pasiūlyta tinklų ir informacinių sistemų saugumo **direktyva** (projektas) yra pagrindinė bendrosios strategijos sudedamoji dalis, todėl reikės, kad visos valstybės narės, pagrindiniai interneto teikėjai ir ypatingos svarbos infrastruktūros objektų, pavyzdžiui, e. prekybos platformų ir socialinių tinklų, operatoriai ir energijos, transporto, bankininkystės ir sveikatos priežiūros paslaugų operatoriai užtikrintų saugią ir patikimą skaitmeninę aplinką visoje ES. Pasiūlytoje direktyvoje nustatytos šios priemonės[11]:

a) valstybės narės turi priimti tinklų ir informacinių sistemų saugumo strategiją ir paskirti nacionalinę tinklų ir informacinių sistemų saugumo kompetentingą instituciją, kuri turėtų tinkamų finansinių ir žmogiškųjų išteklių užkirsti kelią tinklų ir informacinių sistemų saugumo rizikai ir incidentams, juos spręsti ir imtis atsakomųjų priemonių;

b) sukurti valstybių narių ir Komisijos bendradarbiavimo mechanizmą: saugia infrastruktūra būtų iš anksto pranešama apie riziką ir incidentus, bendradarbiaujama ir reguliariai rengiami tarpusavio vertinimai;

c) kai kurių sektorių (finansinių paslaugų, transporto, energetikos, sveikatos priežiūros) ypatingos svarbos infrastruktūros objektų operatoriai, informacinės visuomenės paslaugų teikėjai (visų pirma programinės įrangos parduotuvių e. prekybos platformų, mokėjimo internetu, nuotolinių kompiuterinių išteklių paslaugų, paieškos sistemų, socialinių tinklų) ir viešojo administravimo institucijos turi patvirtinti rizikos valdymo praktiką ir pranešti apie pagrindinius saugumo incidentus savo pagrindinėse tarnybose.

2. Kai kurių užsienio valstybių patirtis reglamentuojant kibernetinį saugumą (strateginiai dokumentai)

Nors ES kibernetinio saugumo strategija ir direktyva dar nepatvirtinta ir atitinkamose ES valstybėse neįgyvendinta, reikia paminėti, kad, nepaisant to, kai kuriose pasaulio valstybėse jau yra priimtos kibernetinio saugumo strategijos. 2013 m. balandžio mėnesį 13 ES valstybių buvo pasitvirtinusios nacionalines kibernetinio saugumo strategijas. Jungtinės Karalystės kibernetinio saugumo strategijos apžvalgoje[12] buvo išnagrinėtos ir palygintos devynių valstybių[13] kibernetinio saugumo strategijos. Šių valstybių kibernetinio saugumo strategijos buvo lygintos su JK kibernetinio saugumo strategija. Palyginimo išvadose pateikti rezultatai liudija, kad JK kibernetinio saugumo strategija

11 Proposal for a Directive of European parliament and the Council concerning measures to ensure a high common level of network and information security across the Union, COM/2013/48 final [interaktyvus]. Briuselis, 2013 [žiūrėta 2013-05-20]. <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1666>, art. 5.

12 The UK cyber security strategy: Landscape review [interaktyvus]. 2013 [žiūrėta 2013-05-20]. <http://www.nao.org.uk/report/the-uk-cyber-security-strategy-landscape-review/>.

13 Australija, Kinija, Estija, Prancūzija, Vokietija, Indija, Japonija, Rusija ir JAV.

išsiskiria „svoriu“, kurį strategijai suteikė JK vyriausybė su tikslu sudaryti saugias sąlygas elektroninei komercijai bei kitiems svarbiems santykiams. Keletas kitų rezultatų:

- Keturios valstybės, kaip ir JK, kibernetinio saugumo programose yra nustačiusios tikslą kovoti su elektroniniais nusikaltimais;
- Visos tirtos valstybės kelia tikslą gerinti atsparumą kibernetinėms atakoms ir saugoti nacionalinį saugumą;
- Tik viena valstybė, taip pat ir JK, palaiko atviros visuomenės idėją;
- Visos valstybės kelia tikslą vystyti kibernetinio saugumo žinias bei pajėgumus užtikrinant kibernetinį saugumą.

Detaliau palygintinos trijų valstybių kibernetinio saugumo strategijos[14]: Jungtinės Karalystės, Vokietijos ir Prancūzijos.

Jungtinės Karalystės kibernetinio saugumo strategija[15] „Jungtinės Karalystės apsauga ir palaikymas skaitmeniniame pasaulyje“ patvirtinta 2011 m. lapkričio mėnesį. Strategijoje nustatyta kibernetinio saugumo vizija 2015 metams: iš energingos, tvirtos ir saugios elektroninės erdvės gauti didžiulę ekonominę ir socialinę vertę, kur šalies veiksmai, valdomi šalies esminių laisvės vertybių, teisingumo, skaidrumo ir įstatymų galios, didins gerovę, nacionalinį saugumą ir tvirtą visuomenę[16]. Kad įgyvendintų šią viziją iki numatyto termino, Jungtinė Karalystė pateikia šiuos keturis tikslus:

1. Kovoti su elektroniniais nusikaltimais Jungtinėje Karalystėje ir tapti viena iš saugiausių šalių pasaulyje verslui elektroninėje erdvėje vystyti;
2. Būti atsparesnei kibernetiniams išpuoliams ir gebėti geriau apsaugoti savo interesus elektroninėje erdvėje;
3. Jungtinė Karalystė, padedanti formuoti atvirą, stabilią ir energingą elektroninę erdvę, kurią šalies visuomenė galės saugiai naudoti, kas palaikytų atviras visuomenes;
4. Jungtinė Karalystė, turinti puikias žinias, įgūdžius ir gebėjimus, leidžiančius palaikyti visus išsikeltus tikslus elektroninės erdvės saugumui užtikrinti.

Vokietijos kibernetinio saugumo strategija[17] patvirtinta 2011 m. vasario mėnesį. Strategijoje nenustatytos datos, todėl galima daryti išvadą, kad strategija bus aktuali iki kitos strategijos patvirtinimo arba iki esamos strategijos atnaujinimo. Vokietijos strategijoje išskiriami šie pagrindiniai elektroninės erdvės saugumo strateginiai tikslai ir priemonės saugumui užtikrinti[18]:

---

14 Šios valstybės pasirinktos ekspertiniam vertinimui kaip valstybės, kuriose daugiausia pažengęs kibernetinis saugumas ir jo teisinis reguliavimas.

15 UK cybersecurity strategy. Protecting and promoting the UK in a digital world [interaktyvus]. 2011 [žiūrėta 2013-05-20]. <http://www.carlisle.army.mil/dime/documents/UK%20Cyber%20Security%20Strategy.pdf>.

16 UK cybersecurity strategy Protecting and promoting the UK in a digital world [interaktyvus]. 2011 [žiūrėta 2013-05-20]. <http://www.carlisle.army.mil/dime/documents/UK%20Cyber%20Security%20Strategy.pdf>, p. 7.

17 Cybersecurity Strategy for Germany [interaktyvus]. 2011 [žiūrėta 2013-05-20]. <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile>.

18 Cybersecurity Strategy for Germany [interaktyvus]. 2011 [žiūrėta 2013-05-20]. <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile>, p. 7–12.

1. Ypatingos svarbos informacinių struktūrų apsauga;
2. Saugios informacinės technologijos (toliau – IT) Vokietijoje;
3. IT apsaugos stiprinimas viešojo valdymo sektoriuje;
4. Nacionalinis reagavimo į kibernetines nelaimes centras;
5. Nacionalinė kibernetinės erdvės apsaugos taryba;
6. Efektyvi nusikaltimų kontrolė, taip pat ir kibernetinėje erdvėje;
7. Efektyvūs koordinuoti veiksmai siekiant užtikrinti kibernetinį saugumą Europoje ir pasaulyje;
8. Patikimų ir vertų pasitikėjimo informacinių technologijų naudojimas;
9. Personalo plėtra federalinėje valdžioje;
10. Reagavimo į kibernetinius išpuolius įrankiai.

Prancūzijos informacinių sistemų gynybos ir saugumo strategija[19] priimta 2011 m. vasarį. Strategijoje taip pat neminimos konkrečios datos. Prancūzijos strategijoje nurodyti šie pagrindiniai strategijos tikslai[20]:

1. Įgyti pasaulinę galią kibernetinės gynybos srityje;
2. Apsaugoti Prancūzijos gebėjimą priimti sprendimus apsaugant informaciją, susijusią su jos suverenitetu;
3. Stiprinti svarbiausių nacionalinių infrastruktūrų kibernetinį saugumą;
4. Užtikrinti elektroninės erdvės saugumą.

Išnagrinėjus ir apibendrinus minėtų valstybių kibernetinio saugumo strategijų nuostatas, galima pastebėti, kad visos valstybės kelia šiuos pagrindinius klausimus:

– glaudaus bendradarbiavimo tiek nacionaliniu, tiek tarptautiniu lygiu bei informacijos keitimosi;
– kritinės informacinės infrastruktūros apsaugos;
– visuomenės informavimo;
– IT apsaugos stiprinimo viešajame sektoriuje;
– saugių IT naudojimo ir kt.

Šios strategijos ir jų nuostatos galėtų būti pavyzdžiu kitoms valstybėms kuriant kibernetinio saugumo strategijas.

Paminėtina, jog be šių strategijų, kurios buvo priimtos beveik vienu metu, Vokietijoje 2013 metais jau yra parengtos ir siūlomos priimti įstatymo nuostatos dėl kibernetinio saugumo.

3. Iniciatyvos Lietuvoje kibernetinį saugumą reglamentuoti įstatymo lygmeniu

Užuomazgos kibernetinio saugumo teisiniam reguliavimui įstatymu Lietuvoje kilo jau 2006 metais, kai Lietuvos Respublikos Vyriausybė nutarimu Nr. 1211 patvirtino

19 France information systems defence and security strategy [interaktyvus]. 2011 [žiūrėta 2013-05-20]. <http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf>.

20 France information systems defence and security strategy [interaktyvus]. 2011 [žiūrėta 2013-05-20]. <http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf>, p. 7–11.

Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepciją[21]. Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepcija parengta įgyvendinant Lietuvos Respublikos Vyriausybės 2006–2008 metų programos įgyvendinimo priemonių, patvirtintų Lietuvos Respublikos Vyriausybės 2006 m. spalio 17 d. nutarimu Nr. 1020 (Žin., 2006, Nr. 112-4273), 157 punktą.

Šioje koncepcijoje buvo numatyta, jog „*Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymas reglamentuos santykius, susijusius su elektroninių ryšių tinklų ir informacijos saugumu (toliau vadinama – tinklų ir informacijos saugumas), sudarys sąlygas saugios informacinės visuomenės plėtrai, didins vartotojų pasitikėjimą informacine visuomene*“[22]. Svarbiausias įstatymo tikslas pagal koncepciją turėjo būti toks – apibrėžti ir įtvirtinti visuomeninių santykių, susijusių su tinklų ir informacijos saugumu, teisinio reguliavimo pagrindus. Įstatymas užpildys ir su elektroninių ryšių paslaugų teikimu susijusių santykių teisinio reguliavimo spragas, kiek tai susiję su tinklų ir informacijos saugumu teikiant elektroninių ryšių paslaugas.

Įstatyme pagal Koncepciją turėjo būti numatyta:

- „*aiški valstybės institucijų struktūra tinklų ir informacijos saugumo srityje, kad nebūtų dubliuojamos institucijų funkcijos ir atsakingos institucijos veiksmingai bendradarbiautų;*
- *nustatyti bendrieji tinklų ir informacijos saugumo reikalavimai, daugiausia skirti vartotojams apsaugoti nuo tinklų ir informacijos saugumo incidentų;*
- *valstybės ir savivaldybių institucijų tinklų ir informacinių sistemų, saugaus informacijos perdavimo tarp valstybės ir savivaldybių institucijų, kritinių informacinių infrastruktūrų tinklų ir informacijos saugumo reikalavimai;*
- *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.*“[23]

Po šios koncepcijos patvirtinimo buvo pradėtas rengti ir Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo projektas. Buvo sudaryta darbo grupė šio įstatymo projektui rengti. Darbo grupė įstatymo variantą parengė, tačiau įstatymas taip ir nebuvo priimtas. Pagal projektą, įstatymas turėjo reglamentuoti visuomeninius santykius, susijusius su elektroninių ryšių tinklų ir informacijos saugumu, nustatant bendruosius reikalavimus elektroninių ryšių tinklų ir informacijos saugumui užtikrinti, taip pat visuomeninius santykius, susijusius su valstybės ir vietos savivaldos

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

22 Ibid., 2 p.

23 Lietuvos Respublikos Vyriausybės nutarimas Nr. 1211 „Dėl Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepcijos patvirtinimo“. *Valstybės žinios*. 2006, Nr. 134-5081, 41 p.

institucijų bei kritinių informacinių infrastruktūrų elektroninių ryšių tinklų ir informacijos saugumu bei elektroninių ryšių tinklų ir informacijos saugumo audito bei techninės ir programinės įrangos saugumo vertinimu.

Šiuo metu Lietuvoje nėra galiojančio įstatymo, holistiškai reguliuojančio kibernetinio saugumo sritį. Tam tikros įstatymo nuostatos numatytos Lietuvos Respublikos valstybės informacinių išteklių įstatyme[24], tačiau yra reglamentuota tik valstybės informacinių išteklių sauga bei saugos įgaliotinio institutas. Šios įstatymo teisės normos, deja, nereglamentuoja informacijos saugos privačiame sektoriuje, o ir informacijos sauga valstybės institucijų sektoriuje reglamentuojama fragmentiškai, pavyzdžiui, įstatyme nenumatyta informacijos saugos institucinės kontrolės ir politikos šioje srityje formavimo sistema. Tai kad teisės aktuose nėra įvardinta nė viena už informacijos saugumo koordinavimą atsakinga institucija, turinti įgaliojimus ir resursus ne tik rengti ar vertinti teisės aktus, bet ir vykdyti realius informacijos saugumo auditus, kaip problemą kelia ir dr. Saulius Jastiuginas[25].

4. Lietuvos kibernetinio saugumo strategija

Elektroninės informacijos saugos teisinis reguliavimas strategijos forma prasidėjo nuo 2006 m., kai buvo patvirtinta Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinė strategija, kuri galiojo nuo 2006 m. iki 2008 m. 2008 m. Lietuvos Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinė strategija iki 2008 metų[26] (toliau – Valstybinė strategija) ir jos įgyvendinimo priemonių planas Lietuvos Respublikos Vyriausybės nutarimu Nr. 601 buvo patvirtinti 2006 m. birželio 19 d. Jau iš strategijos pavadinimo tapo aišku, kad Valstybinė strategija buvo skirta išimtinai valstybės institucijų sektoriui. Valstybinės strategijos pagrindiniai numatyti pasiekti tikslai buvo tokie:

- „*tobulinti elektroninės informacijos saugos koordinavimą ir priežiūrą. Šiam tikslui pasiekti numatyti tokie uždaviniai: užtikrinti elektroninės informacijos saugos koordinavimą; sukurti efektyvią 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;*

---

24 Lietuvos Respublikos valstybės informacinių išteklių įstatymas Nr. XI1807. *Valstybės žinios*. 2011, Nr. 163-7739; V skyrius

25 VU mokslininkas: informacijos saugumo klausimą reikia kelti jau šiandien. *Technologijos.lt* [interaktyvus]. 2013-03-06 [žiūrėta 2013-05-20]. <http://www.technologijos.lt/n/technologijos/it/S-31575/straipsnis/VU-mokslininkas-informacijos-saugumo-klausima-reikia-kelti-jau-siandien?l=2&p=1 >.

26 Lietuvos Respublikos Vyriausybės nutarimas Nr. 601 „Dėl elektroninės informacijos saugos valstybės institucijų informacinėse sistemose strategijos iki 2008 metų ir jos įgyvendinimo priemonių plano patvirtinimo“ . *Valstybės žinios*. 2006, Nr. 70-2575.

- *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;*
- *bei skatinti elektroninės informacijos saugos užtikrinimo projektų įgyvendinimą. Šiam tikslui pasiekti numatytas uždavinys – naudotis privataus sektoriaus patirtimi, įgyvendinant elektroninės informacijos saugos projektus.* "[27]

Reikia pasakyti, kad, nepaisant šioje strategijoje užsibrėžtų pasiekti tikslų, uždavinių, skirtų šiems tikslams pasiekti, formuluotės buvo gana deklaratyvios, abstrakčios ir nekonkrečios[28].

Minima Valstybinė strategija nustojo galioti 2008 metais ir po šios datos Lietuvoje nebuvo jokios galiojančios informacijos saugos strategijos ar programos.

Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimu Nr. 796 „Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo" buvo patvirtinta Kibernetinio saugumo plėtros programa 2011–2019 metams[29] (toliau – Kibernetinio saugumo programa). Atkreiptinas dėmesys, kad Kibernetinio saugumo programa buvo patvirtinta dar 2011 m., kai Europos Komisija dar net nebuvo paskelbusi konsultacijos dėl ES kibernetinio saugumo strategijos, todėl Kibernetinio saugumo programa formaliai nederinta su ES kibernetinio saugumo strategija.

Kibernetinio saugumo programa parengta atsižvelgiant į tai, kad „*valstybės ir visuomenės gyvenime vis didesnę reikšmę įgyja informacinėmis ir ryšių technologijomis tvarkoma ir perduodama elektroninė informacija, atsiradusios elektroninės informacijos tvarkymo galimybės paskatino nacionalinių ir globalių informacinių visuomenių atsiradimą ir sudarė sąlygas toliau modernizuoti šalių ūkius ir efektyviau valdyti valstybę, tačiau tuo pačiu metu į elektroninę formą perkeliama vis daugiau informacijos, sparčiai automatizuojami įvairūs šalies valdymo ir ūkio veiklos procesai, globali kibernetinė erdvė ir joje teikiamos viešosios paslaugos tapo patraukliu atskirų asmenų, nusikalstamų grupuočių, politinių jėgų ir kitų subjektų taikiniu*"[30].

Programos paskirtis – „*nustatyti elektroninės informacijos saugos (kibernetinio saugumo) plėtros tikslus ir uždavinius, kad būtų užtikrintas elektroninės informacijos*

27 Lietuvos Respublikos Vyriausybės nutarimas Nr. 601 „Dėl elektroninės informacijos saugos valstybės institucijų informacinėse sistemose strategijos iki 2008 metų ir jos įgyvendinimo priemonių plano patvirtinimo". *Valstybės žinios*. 2006, Nr. 70-2575, 9 p.

28 Štitilis, D. ir Paškauskas, Ž. 2007. Valstybės elektroninės informacijos saugos strategija – vienas iš pagrindinių elektroninės informacijos saugos reguliavimo instrumentų: lyginamoji analizė. *Jurisprudencija.* 2(92): 41.

29 Lietuvos Respublikos vyriausybės 2011 metų birželio 29 dienos 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).

30 Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimas Nr. 796 „Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metų programos patvirtinimo". *Valstybės žinios*. 2011, Nr. 83-4033; 2011, Nr. 106 (atitaisymas), 1 p.

ir kibernetinėje erdvėje teikiamų paslaugų konfidencialumas, vientisumas ir prieinamumas, elektroninių ryšių tinklų, informacinių sistemų ir ypatingos svarbos informacinės infrastruktūros apsauga nuo incidentų ir kibernetinių atakų, asmens duomenų ir privatumo apsauga, taip pat nustatyti uždavinius, kurių įgyvendinimas leistų užtikrinti bendrą kibernetinės erdvės ir joje veiklą vykdančių subjektų saugumą“[31].

Programos strateginis tikslas –„*plėtoti elektroninės informacijos saugą Lietuvoje, užtikrinti kibernetinį saugumą ir pasiekti, kad 2019 metais teisės aktų nustatytus elektroninės informacijos saugos (kibernetinio saugumo) reikalavimus atitinkančių valstybės informacinių išteklių dalis pasiektų 98 procentus 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 procentų*“[32].

Nustatyti šie Kibernetinio saugumo programos įgyvendinimo tikslai[33]:

1. *Pasiekti, kad būtų užtikrintas valstybės informacinių išteklių saugumas*.

Kibernetinio saugumo programoje pažymima, kad nesukurta kibernetinio saugumo valdymo sistema, tačiau nėra reglamentuojama, kaip tokią sistemą reikėtų sukurti. Tai pat rašoma, kad trūksta privataus ir viešojo sektorių bendradarbiavimo, tačiau nereglamentuojama, kaip tokį bendradarbiavimą reikėtų skatinti ir / ar įgyvendinti.

2. *Užtikrinti veiksmingą ypatingos svarbos informacinės infrastruktūros funkcionavimą*.

Kibernetinio saugumo programoje pažymima, kad tokios infrastruktūros saugumas užtikrinamas tik atskirose organizacijose ir nėra koordinuojamas, nenustatyti tarpusavio ryšiai ir nevertinamas poveikis nacionaliniu mastu.

3. *Siekti užtikrinti Lietuvos gyventojų ir asmenų, esančių Lietuvoje, saugumą kibernetinėje erdvėje*.

Kaip teigiama Kibernetinio saugumo programoje, „*kibernetinės erdvės saugumui užtikrinti būtina nenutrūkstamai veikianti ir tinkamai valdoma sistema, apimanti visą incidentų gyvavimo ciklą: išankstinio perspėjimo, prevencijos, aptikimo, likvidavimo ir tyrimo fazes. Siekiant kovoti su kenksminga programine įranga nuotoliniu būdu valdomų kompiuterių tinklais ar kitais kenkėjiškos veiklos kibernetinėje erdvėje būdais, veiksminga blokuoti interneto prieigą kenkėjišką veiklą vykdantiems asmenims ir (ar) įrenginiams. Šiuo metu visuomenėje yra susiformavęs stereotipas dėl nebaudžiamumo už neteisėtus veiksmus kibernetinėje erdvėje, todėl svarbu šį stereotipą panaikinti*“[34].

---

31 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), 2 p.

32 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), 3 p.

33 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), II skyrius.

34 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), 6.3 p.

Kiekvienam tikslui keliami ir atitinkami uždaviniai. Visa tai pasiekti įmanoma tik turint pakankamai gerai parengtus specialistus, kurių įgytas išsilavinimas būtų glaudžiai susijęs su informacinių technologijų ir informacijos saugumo vadyba. Lietuvos Respublikos Vyriausybės nutarime yra pažymima, kad jau šiuo laiku yra jaučiamas kvalifikuotų informacijos saugos specialistų trūkumas ir numatoma, kad ateityje tas trūkumas tik dar labiau didės. Tokių specialistų trūkumas taip pat yra akcentuojamas ir Europos Sąjungos dokumentuose.

Paminėtina, kad kibernetinio saugumo programos vertinimo kriterijai ir jų reikšmės pateikiami šios programos priede. Kibernetinio saugumo programos įgyvendinimą koordinuoja Lietuvos Respublikos vidaus reikalų ministerija, o už programos tikslų ir uždavinių įgyvendinimą atsako priede nurodytos institucijos ir įstaigos.

Analizuojant Lietuvos kibernetinio saugumo programą ES kibernetinio saugumo strategijos bei direktyvos, taip pat kitų nagrinėtų užsienio valstybių kibernetinio saugumo strategijų kontekste pažymėtina, kad programa neužtikrina visapusiškos Lietuvos kibernetinio saugumo strategijos, kol kas neatitinka visų Europos Komisijos projekte nustatytų kibernetinio saugumo prioritetų, taip pat neužtikrina kitų valstybių kibernetinio saugumo strategijose numatytų kai kurių svarbiausių tikslų ir uždavinių.

Pirma, programoje nenumatytos priemonės dėl valstybės ir privataus sektoriaus bendradarbiavimo kibernetinio saugumo srityje. Turint omenyje, kad šiuo metu didžioji dauguma infrastruktūros priklauso privačiam sektoriui, toks bendradarbiavimas būtinas.

Antra, programoje per mažai dėmesio skiriama elektroniniams nusikaltimams ir jų skaičiaus mažinimui. Elektroninių nusikaltimų latentiškumas, kaip rodo tyrimai, yra didžiulis. Elektroniniai nusikaltimai yra kibernetinių atakų pavadinimas baudžiamosios teisės kontekste, todėl šiai nusikaltimų rūšiai programoje turėtų būti skiriamas deramas dėmesys.

Trečia, programoje nenumatyta išsami ir sisteminė kibernetinės gynybos politika. Šiuo metu Lietuvoje nėra nustatyta, kokie veiksmai turi būti vykdomi kilus kibernetinėms grėsmėms, kokios yra atskirų „žaidėjų“ funkcijos ir atsakomybės, kokie prioritetai saugant kritinę infrastruktūrą nuo kibernetinių atakų, kokie institucijų ir privataus sektoriaus veiksmai kibernetinių atakų atveju. Šį trūkumą būtina kuo skubiau šalinti.

Ketvirta, programoje neaptariami instituciniai klausimai, nedetalizuojamos atitinkamų institucijų funkcijos ir atsakomybės kibernetinio saugumo srityje.

Penkta, programoje nenumatyti tikslai ir uždaviniai, susiję su visuomenės informavimu ir švietimu, kas yra būtina šiuolaikinėje informacinėje visuomenėje, nes kibernetinio saugumo grėsmės dažnai susijusios su galutiniais interneto vartotojais.

Paminėtina, kad strategijoje iškelti tikslai ir uždaviniai nepakankamai konkretūs, abstraktūs, ne visais atvejais atspindi elektroninės erdvės keliamus pavojus bei rizikas. Tikslams ir uždaviniams pasiekti nėra sukurta kibernetinio saugumo valdymo koordinavimo sistema, taip pat nėra numatytas konkrečių lėšų skyrimas.

Kaip minėta aukščiau, dėl kibernetinio saugumo teisinio reguliavimo Lietuvoje apskritai pažymėtinas pamatinių teisės normų trūkumas. Vis dėlto pagrindiniai kibernetinio saugumo klausimai turėtų būti reglamentuojami įstatymu. Nors Elektroninių ryšių tinklų ir informacijos saugumo įstatymas ir nebuvo priimtas, pamatinės teisės normos kibernetinio saugumo srityje yra Lietuvai kritiškai būtinos. Be kitų svarbių klausimų,

tokiame įstatyme turėtų būti reglamentuojama ir institucinė kibernetinio saugumo kontrolė bei politikos formavimo aspektai, taip pat interneto paslaugų teikėjų pareigos. Interneto paslaugų teikėjų pareigų institutą akcentuoja M. F. Grady[35], o kibernetinio saugumo strategijoje, neprieštaraujant įstatymui, galėtų būti įvardijami strateginiai kibernetinio saugumo plėtros ir palaikymo aspektai.

5. Išvados

1. Viena iš naujausių iniciatyvų – ES kibernetinio saugumo strategija bei direktyvos projektas. Kibernetinio saugumo strategija vertintina kaip išsamus strateginis dokumentas, nuo kurio įgyvendinimo priklausys kiekvienos iš ES valstybių kibernetinis saugumas

2. Lietuvoje nėra pamatinių teisės normų, reglamentuojančių kibernetinio saugumo klausimus. Tam tikros holistinio kibernetinio saugumo teisinio reguliavimo iniciatyvos žlugo: buvo parengtas Lietuvos Respublikos elektroninių ryšių tinkle ir informacijos saugumo įstatymo projektas, tačiau šis projektas nebuvo priimtas.

3. Tam tikros teisės normos dėl kibernetinio saugumo numatytos tik Lietuvos Respublikos valstybės informacinių išteklių įstatyme, tačiau jos reglamentuoja tik valstybės informacinių išteklių saugą bei saugos įgaliotinio institutą, be to, yra fragmentiškos.

4. Lietuvoje patvirtinta kibernetinio saugumo programa vertintina kaip teigiamas žingsnis reglamentuojant kibernetinį saugumą. Tačiau programa turi nemažai trūkumų, yra fragmentiška, nekonkreti, neatitinka kai kurių pagrindinių kibernetinio saugumo tikslų ir uždavinių, todėl tobulintina.

5. Lietuvoje aiškiai jaučiamas pamatinių teisės normų kibernetinio saugumo srityje trūkumas. Be kitų klausimų, tokiame įstatyme turėtų būti aptariami ir institucinės kontrolės bei politikos formavimo kibernetinio saugumo srityje klausimai, taip pat interneto paslaugų teikėjų funkcijos užtikrinant kibernetinį saugumą.

Literatūra

Cybersecurity Strategy for Germany [interaktyvus]. 2011 [žiūrėta 2013-05-20]. <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile>.

Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. Network and Information Security: Proposal for A European Policy Approach. COM/2001/298 [interaktyvus]. Briuselis, 2001 [žiūrėta 2013-05-20]. <http://eur-lex.europa.eu/LexUriServ/site/en/com/2001/com2001_0298en01.pdf>.

Digital Agenda – Commission consults on a future EU Network and Information Security legislative initiative [interaktyvus]. Briuselis,

35 Grady, M. F.; Parisi, F. 2006. *The Law and Economics of Cybersecurity*. Cambridge University press, p. 221–256.

2012 [žiūrėta: 2013-05-20]. < http://europa.eu/rapid/press-release_IP-12-818_en.htm >.

Europos Komisija: pranešimas spaudai. ES kibernetinio saugumo planu siekiama apsaugoti atvirą internetą, elektroninę laisvę ir galimybes [interaktyvus]. Briuselis, 2013 [žiūrėta 2013-05-20]. <http://europa.eu/rapid/press-release_IP-13-94_lt.htm>.

France information systems defence and security strategy [interaktyvus]. 2011 [žiūrėta 2013-05-20]. <http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf>.

Grady, M. F.; Parisi, F. 2006. The Law and Economics of Cybersecurity. Cambridge University press.

Jastiuginas, S. 2011. Informacijos saugumo valdymas Lietuvos viešajame sektoriuje. *Informacijos mokslai*. 57 [interaktyvus]. Vilnius [žiūrėta 2013-05-20]. < http://www.leidykla.eu/fileadmin/Informacijos_mokslai/2011-57/7-25.pdf >.

Joint Communication to the European Parliament, the Council, the European Ecomonic and Social Committee and the Committee of Regions „Cybersecurity strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN/2013/1 final [interaktyvus]. Briuselis, 2013 [žiūrėta 2013-05-20]. <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667>.

Komisijos 2009 m. kovo 30 d. komunikatas COM/2009/149 Tarybai, Europos Parlamentui, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui. „Europos apsauga nuo didelio masto kibernetinių antpuolių ir veiklos sutrukdymo – geresnė parengtis, didesnis saugumas ir atsparumas“ [interaktyvus]. Briuselis, 2009 [žiūrėta 2013-05-20]. <http://eurlex.europa.eu/Notice.do?mode=dbl&lang=en&ihmlang=en&lng1=en,lt&lng2=bg,cs,da,de,el,en,es,et,fi,fr,hu,it,lt,lv,mt,nl,pl,pt,ro,sk,sl,sv,&val=493232:cs >.

Komisijos 2012 m. kovo 28 d. komunikatas COM/2012/140 Tarybai ir Europos Parlamentui. Kova su nusikalstamumu skaitmeniniame amžiuje. Europos kovos su elektroniniu nusikalstamumu centro kūrimas [interaktyvus]. Briuselis, 2012 [žiūrėta 2013-05-20]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:LT:PDF>.

Komisijos komunikatas Tarybai, Europos Parlamentui, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui. Saugios informacinės visuomenės strategija – „Dialogas, partnerystė ir teisių suteikimas“. COM/2006/251 [interaktyvus]. Briuselis, 2006 [žiūrėta 2013-05-20]. <http://eurlex.europa.eu/Notice.do?mode=dbl&lang=en&ihmlang=en&lng1=en,lt&lng2=cs,da,de,el,en,es,et,fi,fr,hu,it,lt,lv,nl,pl,pt,sk,sl,sv,&val=427504:cs>.

Lietuvos Respublikos valstybės informacinių išteklių įstatymas Nr. XI1807. *Valstybės žinios*. 2011, Nr. 163-7739.

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

Lietuvos Respublikos Vyriausybės nutarimas Nr. 601 „Dėl elektroninės informacijos saugos valstybės institucijų informacinėse sistemose strategijos iki 2008 metų ir jos įgyvendinimo priemonių plano patvirtinimo“. *Valstybės žinios.* 2006, Nr. 70-2575.

Mitrakas, A. 2006. Information Security Law in Europe: Risks Checked. *Information & Communications Technology Law*. 15(1).

Proposal for a Directive of European parliament and the Council concerning measures to

ensure a high common level of network and information security across the Union, COM/2013/48 final [interaktyvus]. Briuselis, 2013 [žiūrėta 2013-05-20]. <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1666 >.

Reich, P. C. et al. 2010. Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents – and the Dilemma of Anonymity. *European Journal of Law and Technology*. 1(2).

Rosenzweig, P. 2013. Cyberwarfare: how conflicts in cyberspace are challenging America and changing the world. Library of Congress Cataloging.

Shoemaker, D.; Conklin, A. 2012. Cybersecurity: the Essential body of knowledge. Course technology.

Štitilis, D.; Klišauskas, V. 2012. Elektroninės informacijos saugos reglamentavimas Lietuvoje ir Rusijoje: lyginamieji aspektai. *Socialinės technologijos*. 2 (2): 441–455 [interaktyvus]. [žiūrėta 2013-05-20]. <http://www.mruni.eu/lt/mokslo_darbai/st/archyvas/dwn.php?id=340084>.

Štitilis, D.; Paškauskas, Ž. 2007. Valstybės elektroninės informacijos saugos strategija – vienas iš pagrindinių elektroninės informacijos saugos reguliavimo instrumentų: lyginamoji analizė. *Jurisprudencija*. 2 (92): 37–46.

The UK cyber security strategy: Landscape review [interaktyvus]. 2013 [žiūrėta 2013-05-20]. <http://www.nao.org.uk/report/the-uk-cyber-security-strategy-landscape-review/>.

UK cybersecurity strategy. Protecting and promoting the UK in a digital world [interaktyvus]. 2011 [žiūrėta 2013-05-20]. <http://www.carlisle.army.mil/dime/documents/UK%20Cyber%20Security%20Strategy.pdf>.

VU mokslininkas: informacijos saugumo klausimą reikia kelti jau šiandien. Technologijos.lt [interaktyvus]. 2013-03-06 [žiūrėta 2013-05-20]. <http://www.technologijos.lt/n/technologijos/it/S-31575/straipsnis/VU-mokslininkas-informacijos-saugumo-klausima-reikia-kelti-jau-siandien?l=2&p=1>.

THE LEGAL REGULATION OF CYBERSECURITY

Darius Štitilis

Mykolas Romeris University, Lithuania, stitilis@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 offences such as terrorism and drug trafficking due to its risks and profitability. Cybersecurity is the central category to fight cybercrime in cyberspace. Therefore, the strategic legal regulation of cybersecurity is one of the most relevant problems in EU, including Lithuania. So far cybersecurity legal regulation analysis in scientific literature has been rather limited.*

The European Commission, together with the High Representative of the Union for Foreign Affairs and Security Policy, has published a cybersecurity strategy alongside a Commission proposed directive on network and information security (NIS). The cybersecurity strategy – "An Open, Safe and Secure Cyberspace" - represents the EU's comprehensive vision on how best to prevent and respond to cyber disruptions and attacks. The purpose of its is to further European values of freedom and democracy and ensure the digital economy can safely

grow. Specific actions are aimed at enhancing cyber resilience of information systems, reducing cybercrime and strengthening EU international cyber-security policy and cyber defence.

The main goal of the paper is to analyze and compare the EU cybersecurity strategy and experience of several foreign countries with the strategic legal regulation of cybersecurity in Lithuania.

The article consists of four parts. The first part dealt with the EU cybersecurity strategy. The second part of the article examines the comparative aspect of foreign cybersecurity strategic legal regulation. The third part deals with attempts in Lithuania to draft cybersecurity law and the holistic approach of cybersecurity legal regulation. The fourth part examines Lithuanian cybersecurity strategy and comments on the main probleas related with the strategy.

Several different approaches have been used in the research. The author have used a comparative method to investigate the EU cybersecurity strategy as well a, Lithuanian and foreign situations. The empirical analysis of legal documents was used to determine the legal regulation of the cybersecurity in Lithuania. In addition, Legal acts of the Republic of Lithuania have been analyzed. Having analyzed the official documents, the method allows identifying and describing the relationship between the valid legal regulations accurately. Using literature resources, the author has used the deductive method which allows drawing sufficiently reliable conclusions.

Keywords: *cybersecurity, legal regulation.*