KLAIPĖDOS UNIVERSITETAS

Socialinių ir humanitarinių mokslų fakultetas

Viešojo administravimo ir politikos mokslų katedra

KIBERNETINIO SAUGUMO AKTUALIZAVIMAS LIETUVOS NACIONALINIO SAUGUMO STRATEGIJOJE

Magistro darbas

Autorius SMNNS18 gr. stud. Marija Tamošaitytė

Vadovas doc. dr. Julius Žukas

Klaipėda, 2019 m.

MAGISTRO BAIGIAMOJO DARBO LYDRAŠTIS

Marija Tamošaitytė
(magistro baigiamojo darbo autoriaus vardas, pavardė)

Kibernetinio saugumo aktualizavimas Lietuvos nacionalinio saugumo strategijoje
(magistro baigiamojo darbo pavadinimas lietuvių kalba)

Patvirtinu, kad magistro baigiamasis darbas parašytas savarankiškai, nepažeidžiant kitiems asmenims priklausančių autorių teisių, visas magistro baigiamasis darbas ar jo dalis nebuvo panaudotas Klaipėdos universitete ir kitose aukštosiose mokyklose.

Marija Tamošaitytė
(magistro baigiamojo darbo autoriaus vardas, pavardė ir parašas)

Sutinku, kad magistro baigiamasis darbas būtų naudojamas neatlygintinai 5 m. Klaipėdos universiteto studijų procese.

Marija Tamošaitytė
(magistro darbo autoriaus vardas, pavardė ir parašas)

Magistro baigiamąjį darbą ginti .....
(įrašyti – leidžiu arba neleidžiu)

....
(data) (magistro baigiamojo darbo vadovo vardas, pavardė ir parašas)

Baigiamasis darbas įregistruotas katedroje .....
(data)

.....
(katedros sekretorės vardas, pavardė ir parašas)

Magistro baigiamąjį darbą ginti .....
(įrašyti – leidžiu arba neleidžiu)

....
(data) (katedros vedėjo vardas, pavardė ir parašas)

Recenzentu(-ais) skiriu .....

.....
(įrašyti recenzento(ų) vardą, pavardę)

....
(data) (katedros vedėjo vardas, pavardė ir parašas)

SANTRAUKA

Marija Tamošaitytė (el. paštas: marijatami@gmail.com). **Kibernetinio saugumo aktualizavimas Lietuvos nacionalinio saugumo strategijoje**. Socialinių mokslų magistro darbas. Darbo vadovas: dr. Julius Žukas. Klaipėdos Universitetas, Socialinių ir humanitarinių mokslų fakultetas, Viešojo administravimo ir politikos mokslų katedra, 2019 metai.

Šio darbo tikslas – išanalizuoti kibernetinio saugumo aktualumą nacionalinio saugumo kontekste. Darbą sudaro įvadas, keturi skyriai su poskyriais bei išvados. Pirmajame skyriuje aptariamas nacionalinio saugumo daugialypiškumas ir kibernetinio saugumo samprata bei jo užtikrinimo specifiškumas. Antrajame skyriuje analizuojami nacionalinį saugumą užtikrinantys teisės aktai ir grėsmės, darančios įtaką nacionaliniam saugumui. Taip pat aptariami kibernetinį saugumą reglamentuojantys teisės aktai ir kibernetinio saugumo politiką įgyvendinančios institucijos. Trečiame skyriuje apžvelgiamas NATO ir ES požiūris į kibernetinį saugumą ir gynybą, aptariami teisės aktai, kibernetinį saugumą užtikrinančių agentūrų darbas ir tarptautinio bendradarbiavimo svarba. Ketvirtame skyriuje vertintos Lietuvos kibernetinių grėsmių užkardymo galimybės ir priemonės, analizuojama kibernetinių incidentų ir kibernetinių šnipinėjimų pokytis ir apžvelgiama reali situacija. Aptariama Lietuvos, NATO ir ES sąveikos svarba ir būtinybė kibernetinio saugumo ir gynybos klausimais.

SUMMARY

Marija Tamošaitytė (e mail: marijatami@gmail.com). Cybersecurity actualization in the National Security Strategy of Lithuania. Master of Social Sciences Thesis. Supervisor: Dr. Julius Žukas. Klaipėda University, Department of Social and Humanitarian Sciences, Public Administration and Political Science Branch, 2019.

The purpose of this thesis is to analyze the relevance of cybersecurity in the overall context of national security. The paper consists of introduction, four chapters with subchapters and conclusions. The first section approaches the multidimensionality of national security and the concept of cybersecurity, as well as the specifics of its enforcement. The second section analyzes national security legislation and threats that affect national security. The third chapter reviews the NATO and EU approach to cyber security and defense, discusses legal framework, activities of cybersecurity agencies, and the importance of international co-operation. analyzing the changes in cyber incidents and cyber espionage and reviewing the current real life situation. The importance and necessity of collaboration among Lithuania, NATO and the EU on cyber security and defense issues are also discussed.

Turinys

Santrumpos

AE – atominė elektrinė

AOTD – Antrasis operatyvinių tarnybų departamentas

CCDCOE - The NATO Cooperative Cyber Defence Centre of Excellence

CERT-LT – Lietuvos Respublikos Ryšių reguliavimo tarnybos Tinklų ir informacijos saugumo departamento Saugumo incidentų tyrimo skyrius

ES – Europos Sąjunga

ESCD - EmergingSecurityChallengesDivision

IT – informacinės technologijos

KAM – Krašto apsaugos ministerija

LR – Lietuvos Respublika

LRV – Lietuvos Respublikos vyriausybė

NATO – North Atlantic Treaty Organization

NKSC- Nacionalinio kibernetinio saugumo centras

PESCO – Permanent Structured Cooperation

RRT – Ryšių reguliavimo tarnyba

SCADA – kompiuterizuota, tinklais valdoma programuojama pramoninių procesų valdymo sistema

Įvadas

Temos aktualumas. Valstybės nepriklausomybė ir jos teritorija yra visų šalies piliečių saugumo garantas. Saugoti ir ginti valstybę nuo įvairių vidaus ir išorės grėsmių bei pavojų reikia tam, kad kiekvienas šalies pilietis galėtų laisvai gyventi ir dirbti. Tradicinis saugumo supratimas buvo siejamas tik su kariniu saugumu, tačiau vykstant globalizacijos procesams, klimato pokyčiams, spartėjant ekonomikos augimui, vykstant teroristiniams išpuoliams buvo pradėta galvoti apie saugumo sąvokos praplėtimą.Bėgant laikui valstybės susiduria su vis sudėtingesnėmis grėsmėmis ir iššūkiais. Valstybių nesugebėjimas tvarkytis pasireiškia nusikalstamumu, didėjančia migracija, terorizmu, kas turi didelės įtakos šalių saugumui.

Valstybės saugumą veikia įvairūs valstybės ir visuomenės veiksniai, šalia tradicinių saugumo sektorių atsiranda naujas, ir vis labiau aktualus – kibernetinis saugumas. Kibernetinio saugumo užtikrinimas tampa šių dienų problema. Sparčiai besivystant informacinėms technologijoms, kibernetinė erdvė tampa tinkamu įrankiu nuolat vykdyti kibernetines atakas ne tik prieš individus ar organizacijas, tačiau taip pat siekiant padaryti žalos visai visuomenei ar valstybei.Kibernetinių atakų skaičiui tik augant, kibernetinio saugumo svarba neabejoja niekas. Tiek nacionaliniu, tiek tarptautiniu lygmeniu vis dažniau yra aptariami kibernetinio saugumo ir gynybos klausimai ir problemos.Siekiant sustiprinti kibernetinį atsparumą būtina laikytis bendro ir plataus požiūrio. Europos komisija deda visas pastangas apsaugoti ES piliečius elektroninėje erdvėje, todėl 2013 m. buvo priimta ES kibernetinio saugumo strategija, taip pat priimta daug kitų teisės aktų ir pasiūlymų rinkinių, susijusių su elektroninių ryšių tinklų ir informacijos saugumu. 2014 m.ES skyrė daugiau nei 600 mln. eurų ES investicijų moksliniams tyrimams ir naujovėms kibernetinio saugumo srityje ir skatino bendradarbiavimą tiek ES viduje, tiek ir su pratneriais pasaulinėje arenoje. 2016 m. NATO ir ES pasirašė deklaraciją dėl bendradarbiavimo kibernetinės erdvės valdymo srityje.Gilesnio bendradarbiavimo tarp ES ir NATO poreikis jau kurį laiką atsispindi Europos šalių vadovų darbotvarkėse – vyksta bendradarbiavimas tarp ES ir NATO kibernetinio saugumo institucijų, organizacijos keičiasi informacija, rengia mokymus ir tyrimus. Tiek ES, tiek NATO kibernetinis saugumas yra strateginis klausimas, turintis įtakos ir valstybių narių, ir pačių organizacijų saugumui ir gynybai. Abiejų organizacijų misijos kibernetinio saugumo srityje: NATO daugiausia dėmesio skiria kibernetinio saugumo ir gynybos aspektams, o ES susiduria su platesniais, daugiausia nekariniais, elektroninės erdvės klausimais (interneto laisvė ir valdymas, internetinės teisės ir duomenų apsauga) ir vidaus saugumo aspektais.

Kibernetinis saugumas svarbus ne tik tarptautiniu lygmeniu, bet ir nacionaliniu. Laikas parodė, kad kibernetinių atakų sudėtingumas tampa iššūkiu nacionaliniam saugumui ir nei viena šalis nėra nuo to apsaugota. Kibernetinis saugumas tampa svarbiausiu prioritetu Lietuvai. Krašto apsaugos ministeriją paskyrus atsakingą už kibernetinio saugumo politikos formavimą, pertvarkius

Nacionalinio kibernetinio saugumo centrą ir 2018 m. atnaujinus Kibernetinio saugumo strategiją Lietuva pateko tarp lyderių kibernetinio saugumo srityje.[1] Vis dėl to, kibernetinis saugumas yra nuolatinis procesas ir nereikia galvoti, kad Lietuva jau pasiekė tokį lygį, kai nėra kur daugiau tobulėti. Viena iš svarbiausių sričių, kurią Lietuvai dar reikėtų tobulinti yra kibernetinio saugumo kultūra. Tai svarbi problema tiek viešajame, tiek privačiame sektoriuje. Būtent žmogiškasis faktorius išlieka silpniausia grandimi stiprinant kibernetinį saugumą. Kibernetinis saugumas nėra tik kariškiams ar kitiems pareigūnams svarbi sritis. Ji yra svarbi kiekvienam iš mūsų, kadangi mūsų naudojami išmanieji telefonai arba namų kompiuteriai gali tapti lygiai tokiais pačiais taikiniais, kaip kritinė infrastruktūra. Dėl šios priežasties kibernetinio saugumo tema, bėgant laikui, tobulėjant technologijoms ir vis didesniam kiekiui svarbios informacijos persikeliant į internetą, taps tik jautresnė ir sulauks dar daugiau dėmesio. Tik suvokdami naująsias grėsmes, galėsime ruoštis jas atremti.

Tyrimo ištirtumas. analizuojant Lietuvos, NATO ir ES situaciją kibernetinio saugumo srityje buvo naudojama nemaža teisinių šaltinių bazė, 2002 m. LR Nacionalinio saugumo strategija yra svarbiausių saugios valstybės raidą apibrėžiančių nuostatų visuma, kurioje nustatomi gyvybiniai ir pirmaeiliai nacionalinio saugumo interesai, rizikos veiksniai, pavojai ir grėsmės. 2019 m. LR Nacionalinio saugumo pagrindų įstatymas, kuris nustato Lietuvos nacionalinio saugumo užtikrinimo pagrindus. 1997 m. buvo priimtas LRV nutarimas „Dėl duomenų apsaugos valstybės ir vietos savivaldos informacinėse sistemose“, šiuo nutarimu buvo patvirtinti pirmieji informacijos saugumo reikalavimai, kuriais buvo siekiama užtikrinti duomenų patikimumą bei apsaugą nuo neteisėto panaudojimo. 2011 m. buvo priimtas LRV nutarimas „Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 metais programos patvirtinimo“, šios programos paskirtis – plėtoti elektroninės informacijos saugą Lietuvoje ir užtikrinti kibernetinį saugumą. 2018 m. priimtas kibernetinio saugumo įstatymas, jis nustato kibernetinio saugumo principus, kibernetinio saugumo politikos formavimo institucijas, kibernetinio saugumo subjektų pareigas ir tarpinstitucinį bendradarbiavimą. Taip pat buvo nagrinėjami tarptautinio lygmens dokumentais ir teisės aktai. 2002 m. pasirašyta Europos Parlamento ir Tarybos direktyva 2002/21/EB „Dėl elektroninių ryšių tinklų ir paslaugų bendrosios reguliavimo sistemos“, kuria elektroninių ryšių paslaugų teikėjai įpareigojami tinkamai valdyti jų tinklams kylančias grėsmes ir pranešti apie svarbius saugumo pažeidimus. 2013 m. buvo paskelbta Europos kibernetinio saugumo strategija, šioje strategijoje siūlomi konkretūs veiksmai, kuriais galima pagerti ES pasiektus rezultatus kibernetinio saugumo srityje. 2008 m. priimta NATO kibernetinės gynybos politika, kuria siekiama stiprinti savo kibernetinį saugumą, gynybą ir atgrasymo strategijas. 2011 m. buvo patvirtinta antroji NATO kibernetinė gynybos politika, koncepcija ir veiksmų planas, kuriame išdėstyta koordinuotų

[1]National Cyber Security Index, https://ncsi.ega.ee/

kibernetinės gynybos pastangų visame Aljanse vizija ir susijusių veiksmų planas kibernetinės gynybos politikai įgyvendinti.

Kibernetinio saugumo sąvoka šiais laikais tampa vis aktualesniu ir daugiau dėmesio sulaukiančiu reiškiniu. Nėra visuotinai apibrėžtos ir patvirtintos kibernetinio saugumo sąvokos. Kibernetinį saugumą savo darbuose bandė apibrėžti Richard A. Kemmerer, „Cyber security“, Tomas Stamulis, „Kibernetinis saugumas. Ką saugom ir nuo ko saugom?“, James A. Lewis, „CybersecurityandCriticalinfrastructureprotection“ ir daugelis kitų Lietuvos ir užsienio autorių.Lietuvos kibernetinio saugumo teisinį reguliavimą savo darbe nagrinėjo Darius Štitilis, „Kibernetinio saugumo teisinis reguliavimas: kibernetinio saugumo strategijos“, savo darbe Justine M. Chauvin „NATO Cyber Drfence Policy“ siekia išnagrinėti klausimus susijusius su kibernetiniu saugumu, atkreipiant dėmesį į kibernetinių grėsmių suvokimo svarbą tarptautiniu lygmeniu, kaip pavyzdį naudojant NATO kibernetinio saugumo gynybos politiką.

Tyrime taip pat panaudotos AOTD prie KAM, CERT-LT, NKSC ataskaitos.

Tyrimo objektas – kibernetinio saugumo aktualumas Lietuvos nacionalinio saugumo strategijoje.

Tyrimo problema:Ar įmanomas visiškas kibernetinio saugumo grėsmių užkardymas? Kas lemia kibernetinio saugumo užtikrinimo specifiką?

Tyrimo tikslas –išanalizuoti kibernetinio saugumo aktualumą nacionalinio saugumo kontekste.

Tyrimo uždaviniai:

1. Aptarti nacionalinio saugumo teorinius aspektus.
2. Pateikti kibernetinio saugumo sampratą.
3. Išnagrinėti nacionaliniam saugumui kylančias grėsmes, pavojus ir rizikos veiksnius.
4. Apžvelgti kibernetinio saugumo Lietuvoje teisinį reglamentavimą.
5. Aptarti Europos Sąjungos ir NATO požiūrį į kibernetinį saugumą.
6. Išanalizuoti kibernetinių grėsmių užkardymo galimybes ir priemones.
7. Aptarti Lietuvos, ES ir NATO bendradarbiavimą kibernetinio saugumo srityje.

Ginamieji teiginiai:

1. Kibernetinio saugumo teisinio reglamentavimo trūkumas lemia kibernetinio saugumo problematiką Lietuvoje.

2. Lietuvoje, ES ir NATO kibernetinis saugumas nėra prioritetinis saugumo politikos aspektas.

Tyrimo metodai: mokslinės literatūros analizė, dokumentų analizė, teisinių aktų analizė, aprašomasis, lyginamasis, statistinis, grafinis, antrinių duomenų analizė.

1. NACIONALINIO IR KIBERNETINIO SAUGUMO TEORINIAI ASPEKTAI

1.1 Nacionalinio saugumo samprata

Kas yra saugumas? Ar įmanoma visiškai jį užtikrinti? Nors jau gana ilgą laiko tarpą nacionalinės studijos gilinasi į šią sąvoka, saugumo studijos nuolat tobulėja, keliamos vis naujos hipotezės ir taikomi vis naujesni analizės būdai, bet vis dar negalima konkrečiai atsakyti į šiuos klausimus.Saugumas yra pagrindinis tarptautinių santykių pagrindas. Kartu tai iš esmės ginčijama sąvoka, nes dėl jos apibrėžimo ir turinio niekaip nesusitariama.Saugumo sąvoka yra sunku tiksliai apibrėžti, tiek mokslinėje literatūroje, tiek politikoje ar visuomenėje ši sąvoka interpretuojama gana skirtingai. Kaip teigia Barry Buzan „pati saugumo sąvokos prigimtis neleidžia suformuluoti tikslaus jos apibrėžimo“,[2] kadangi šis terminas yra plačiai naudojamas, kyla sunkumų norint nustatyti jo ribas.

Nacionalinio saugumo sąvoka yra vartojama moksliniu, politiniu ir visuomeniniu požiūriais, todėl dažnai jos interpretacijos skiriasi. Visuomeniniu požiūriu ši sąvoka suprantama kaip šalies nepriklausomybės išsaugojimas ir jo gynyba nuo grėsmių, kylančių iš užsienio. Politiniu požiūriu nacionalinis saugumas traktuojamas kaip valstybės nepriklausomybės, jos teritorinio vientisumo ir konstitucinės santvarkos apsauga ir jos gynyba nuo įvairių grėsmių, kylančių tiek iš išorės tiek ir šalies viduje.[3] Nors saugumo sąvoka neturi vienareikšmio apibrėžimo, kaip matome iš žemiau pateiktų autorių nuomonių, literatūroje buvo ne vienas bandymas ją apibrėžti.

Pirmuoju žingsniu saugumo link galime laikyti 1684 metais sudarytą Vestfalijos sutartį, kurioje saugumo sąvoka buvo siejama būtent su valstybe. Sudarant šią taikos sutartį pirmiausia buvo atsižvelgta į nepriklausomybės principą, o tai reiškė, kad sutarties šalys pasižada gerbti kitų šalių teritorijas ir nesikišti į vidaus politikos reikalus taip užtikrinant sutarties šalių saugumą. Nacionalinio saugumo sąvoka palyginus su saugumo sąvoka yra naujesnė. Pirmą kartą nacionalinio saugumo terminas paminėtas 1947 m. JAV nacionalinio saugumo akte.

Ilgą laiką saugumo sąvoką buvo grindžiama realizmo teorijomis. Vokiečių mokslininkas John H. Herz 1951 m. savo knygoje „Politinis realizmas ir politinis idealizmas“ iškėlė saugumo dilemos terminą, kuris tarptautiniuose santykiuose nurodo situaciją, kurioje siekdamos savo tikslų ir pasitelkdamos karinę galią ar Aljansus, valstybės siekia didinti savo saugumą, taip sukeldamos kitų valstybių nesaugumo jausmą. Karinės jėgos telkimas padėjo konsoliduoti pačią valstybę: prievartos instrumentų – karinių pajėgumų – kūrimas padarė valstybę pagrindiniu saugumo teikėju, tačiau

[2]Buzan B., Žmonės, valstybės ir baimės, Vilnius: Eugrimas, 1997 m. 49 p.
[3]A. Petrauskaitė, R. Markelienė, R. Gedminienė – „Šalies saugumas ir gynyba“, Vilnius 2016, 13 p.

kartu ir pagrindiniu jo interpretatoriumi.[4] Realizmas daugiau dėmesio skiria išorinėms grėsmėms, šiuo atveju, saugumas suprantamas kaip valstybės pagrindinių vertybių, tokių kaip politinė nepriklausomybė ir teritorinis integralumas, apsauga ir išsaugojimas. Būtent valstybė yra saugumo objektas. J. Herzo suformuluota „saugumo idėjos“ dilema: savarankiški valstybių bandymai rūpintis savo saugumu nepaisant gerų norų, didina kitų valstybių nesaugumą, nes jei viena valstybė savo priemones laiko grynai gynybinėmis, tai kitos valstybės – potencialiai grėsmingomis.[5] Žiūrint iš realistų pozicijos saugumas buvo suprantamas kaip karinės galios didinimas siekiant užsitikrinti saugumą. Tačiau vienų valstybių bandymas užsitikrinti išlikimą didinant savo karinę/ekonominė galią gali būti suvokiamas kaip keliantis grėsmę kitų valstybių saugumui ir tapti valstybinių konfliktų priežastimi. Tokiomis sąlygomis valstybės negali pasitikėti viena kita, nes nuolat egzistuoja karo grėsmė.

Ilgą laiką nacionalinio saugumo sąvoka buvo suprantama kaip karinė problema, tačiau bėgant laikui buvo pateikta naujų argumentų raginančių plėsti ir gilinti saugumo sąvokos sampratą.Klasikinis saugumo apibrėžimas teigia, kad saugumas – tai tiesioginės karinės grėsmės šalies suverenumui bei teritoriniam integralumui nebuvimas. Šiandieninė saugumo samprata yra daug platesnė už tradicinę klasikinę ir saugumą apibrėžia, kaip grėsmės esamoms vertybėms nebuvimą.[6]Vertybių problema tampa nepaprastai svarbiu kiekvienos valstybės nacionalinio saugumo sistemos aspektu, kadangi valstybė, kurios prioritetai yra tokios vertybės, kaip tolerancija, piliečių teisės ir laisvės, yra daug atsparesnė išorinėms ir vidinėms grėsmėms.[7] Jei valstybė nesugeba apginti savo teritorijos ir apsaugoti savo žmonių, galima suabejoti jos suverenitetu.[8]

Taip pat gana reikšminga saugumo sampratos išplėtojimui buvo 1973-1974 metų naftos krizė, kuri iškėlė ekonominės priklausomybės nuo kitų šalių problemą. Kaip teigia L. Brown saugumo samprata turėtų būti išplėsta įtraukiant aplinkos grėsmes, kurios kyla dėl resursų stokos ir demografinių problemų. Saugumo sąvoka išplėtojama taip, kad ji reiškia laisvės nuo karinių, politinių, socialinių ekonominių bei ekologinių grėsmių siekimą.

Velso mokyklos atstovas K. Booth‘o teigia, kad saugumas turėtų būti suprantamas kaip emancipacija, žmonių-individų ar grupių išsilaisvinimas nuo fizinių ar kitokių apribojimų – skurdo, prievartos, politinės priespaudos ir t.t. Ne galia, ne tvarka, o emancipacija sukuria tikrąjį saugumą. Teoriškai, emancipacija ir yra saugumas. Šios mokyklos atstovai saugumą sieja su individais. Žmogiškosios dimensijos ignoravimas saugumo konceptualizavime prieštarauja logikai – kad

[4]Paulauskas K. Saugumo studijų būklė ir raidos tendencijos. Lietuvos metinė strateginė apžvalga 2006. Vilnius: VU TSPMI, 2007 m. 197 p.
[5]Erika Matulionytė „Grėsmių nacionaliniam saugumui nustatymas ir jų prevencijos galimybės“, Vilnius, 2008 m. 94 p.
[6]Margarita Šešelgytė, „Europos saugumas: nauji iššūkiai ir bendradarbiavimo galimybės“, 2003 m. 135-136 p.
[7]Rolanda Kauzlauskaitė-Markelienė, Audronė Petrauskaitė „Pilietinė visuomenė ir nacionalinis saugumas: teorinė problemos apžvalga“, 2011 m. 239 p.
[8]Held D., Mc Grew A. ir kt. Globaliniai pokyčiai: politika, ekonomika ir kultūra. Vilnius: Margi raštai, 2002 m. 169 p.

„saugumo“ sąvoka turėtų prasmę tarptautiniu lygmeniu, ji pirmiausia turi turėti atpažįstamą prasmę individualiu lygmeniu. „Saugumas“ esąs prigimtinis, pasąmoningas, kiekvienam individui nuo kūdikystės būdingas impulsas ar poreikis jaustis saugiai socialiniuose santykiuose ir kontroliuoti situaciją. Šios mokyklos atstovai smarkiai kritikuoja į karinio saugumo ir konfliktų sprendimus orientuotą požiūrį. Geležiniai ginklai ir kariniai veiksmai yra kraštutinė nacionalinio saugumo užtikrinimo priemonė. Nacionalinis saugumas – tai tautos saugumas, tautos gyvybingumo išlaikymas.[9]

Kopenhagos mokyklos atstovų nuomone „saugumo“ terminas reiškia nesugebėjimą išspręsti problemų „normalios politikos“ keliu, jeigu valstybė praranda suverenitetą, ji nustoja egzistuoti kaip valstybė. Atitinkamai, jeigu visuomenė praranda savo identitetą, ji nustoja egzistuoti kaip visuomenė. Kopenhagos mokyklos atstovai saugumo studijose pabrėžia visuomenės identiteto kaip saugumo objekto svarbą, jie teigia, kad valstybė išlieka „idealiu saugumo veikėju“, sugebančiu geriausiai užtikrinti saugumą.[10]

I. Kantas savo veikale „Į amžinąją taiką”, išplėtojo teoriją, kuria teigiama, kad saugumą gali užtikrinti gerai veikianti teisinė sistema. Reikia sukurti tokias taisykles, kurių visuotinai norėtų laikytis. Jei pilietinėje visuomenėje nekils prieštaravimų tarp individų, saugumo lygis tik augs. Liberal-idealizmo šalininkai, skirtingai nuo realistų, teigia, kad pasaulinė anarchija nėra natūralus pasaulio būvis. Natūralus būvis yra gyvenimas, laikantis teisės normų. Pasaulinės taikos viršūnė yra vadinamoji demokratinė taika – būsena, kai pasaulį sudarys demokratinės valstybės, kurios savo iniciatyva nepradeda karų, kurios konkuruoja pagal taisykles.[11]

Feministinės saugumo studijos savo idėjomis yra artimos anksčiau minėtos Velso mokyklos idėjoms. Anot feminisčių, pagrindinis saugumo objektas turėtų būti individas, saugumas priklauso nuo to, kaip subjektas pasirenka savo tapatybę ir interesus, todėl tik emancipacija yra būdas išlaisvinti individus iš socialinių, teisinių, politinių apribojimų ir priespaudos. Feminizmo atstovai teigia, kad tradicinis į valstybę orientuotas karinis saugumas ne didina, o kaip tik mažina moterų nesaugumą.[12] Feminizmo atstovai, kalbėdami apie saugumą, akcentuoja ryšį tarp neturto, skolų, populiacijos augimo, bei skatina mąstyti apie resursus ir jų paskirstymą.[13]

Radikalūs postmodernistai apskritai nesiūlo jokios saugumo teorijos – jie neigia ir kritikuoja saugumą. James Der Derrianas, Walkeris kelia klausimą, kodėl saugumas turėtų apskritai kam nors rūpėti – geriau gyventi įdomų ir neprognozuojamą gyvenimą. Tačiau šiame pasaulyje,

[9]J. Vaškūnas „Tautinė kultūra – pagrindinis šių laikų nacionalinio saugumo uždavinys“, 2019 m.
[10]Jurgita Jakevičiūtė, „Paradigminės konstruktyvistų ir Neorealistų diskusijos saugumo objekto ir jam kylančių grėsmių prigimties Klausimais: bendros ES karinio saugumo Sistemos idėja“, Vilnius, 2011 m. 154 p.
[11]E. Vareikis – “Kas yra krikščioniškoji demokratija (X). Karas ir saugumas“, 2015 m. http://www.arche.lt/2015/11/egidijus-vareikis-kas-yra.html
[12]Ieva Karpavičiūtė, „Saugumo sampratos kaita. Globalizacija ir transnacionalinių saugumo grėsmių išskyrimas“, 28 p.
[13]J. Ann Tickner. Saugumo re-vizijos. Ken Booth, SteveSmith „Tarptautinių santykių teorija šiandien“ Vilnius, 2000 m., 187 p.

kuriame dominuoja terorizmas, masinio naikinimo ginklai, įvairūs virusai ir kitos grėsmės, tokia idėja atrodo juokinga.

Apibendrinus pateiktas teorines įžvalgas, galima teigti, kad nacionalinio saugumo sąvoka mokslinėje literatūroje nėra vienareikšmiškai apibrėžta ir apima daug prieštaravimų ir problemų. Dėl egzistuojančių skirtumų tarp valstybių vargu ar galima tikėtis, kad nacionalinio saugumo sąvokoje slypėtų bent kokia vieningo ir universalaus apibrėžimo galimybė,[14] nes tai kas tinka vienai valstybei, nebūtinai tiks kitai. Kiekviena valstybė nusistato savo prioritetus ir apsibrėžia sau pritaikytą nacionalinio saugumo sąvoką.

1.2 Kibernetinis saugumas ir jo užtikrinimo specifika

Nacionalinį saugumą veikia įvairūs valstybės ir visuomenės veiksniai. B. Buzan išskiria penkis valstybės saugumo sektorius: karinį, politinį, ekonominį, socialinį ir ekologinį.[15] Šalia šių tradicinių saugumo sektorių, šiais laikais vis aktualesni darosi ir nauji saugumo sektoriai: informacinis saugumas ir kibernetinis saugumas. Šiame poskyryje plačiau aptarsime kibernetinio saugumo sampratą, aktualumą ir jo užtikrinimo specifiką.

Kibernetinio saugumo sąvoka šiais laikais tampa vis aktualesniu ir daugiau dėmesio sulaukiančiu reiškiniu. Kompiuteriniams tinklams išsiplėtojus visame pasaulyje, atsivėrė beribės galimybės efektyviau spręsti atsiradusias problemas, našiau dirbti, paprasčiau išsirinkti įdomesnes atostogas ar tiesiog paprasčiau gyventi. Kompiuterių tinklai gyventojams, įmonėms ir kitoms institucijoms tampa ekonominės ir socialinės gerovės užsitikrinimo įrankiu. Vis labiau augant kompiuterinių tinklų galimybėms didėja ir kompiuterinių tinklų reikšmė visoms žmonių gyvenimo sritims. Nors kompiuterių tinklai palengvina kasdieninį žmonių gyvenimą ir gali būti panaudoti naudingai veiklai, atsiranda asmenų, kurie siekdami piktų kėslų, pasinaudoję kompiuteriniais tinklais, gali pridaryti nepataisomos žalos. Kibernetinis saugumas yra plačiai naudojamas terminas, kurio apibrėžimai būna labai įvairūs, dažnai subjektyvūs, o kartais net neinformatyvūs. Visuotinai priimtos, trumpos ir aiškiai apibrėžtos sąvokos nebuvimas, kuriame būtų apibrėžtas kibernetinio saugumo daugialypiškumas, trukdo technologinei ir mokslinei raidai.

Pirmiausia, kibernetinis saugumas – tai požiūris į informacijos saugumą, kuris padeda apsaugoti informaciją nuo neteisėtos prieigos, naudojimo, atskleidimo, trikdymo, modifikavimo ir sunaikinimo. Šiuo metu šį požiūrį siekiama išplėsti, siekiant užtikrinti kibernetinės erdvės rizikų valdymą. Kibernetinis saugumas susideda iš grėsmių analizės ir grėsmių suvaldymo proceso, siekiant užkardyti bet kokią riziką, susijusią su informacijos ir duomenų naudojimu, apdorojimu,

[14]Buzan B., Žmonės, valstybės ir baimės, Vilnius: Eugrimas, 1997 m. 108 p.
[15]Buzan B. Žmonės, valstybės ir baimė. Vilnius: Eugrimas, 1997, 52–53 p.

saugojimu ir perdavimu. Antra, kibernetinis saugumas apibrėžiamas, kaip priemonės, kurių imtasi siekiant apsaugoti kompiuterį ar kompiuterių tinklus nuo neleistinos prieigos ar atakos.[16]

Kibernetinis saugumas – tai kompiuterių, serverių, mobiliųjų įrenginių, elektroninių sistemų, tinklų ir duomenų apsaugojimas nuo kenkėjiškų atakų. Jis taip pat žinomas kaip informacinių technologijų saugumas arba elektroninis informacijos saugumas.[17]

Kibernetinis saugumas daugiausiai susideda iš gynybos metodų, naudojamų aptikti ir užkirsti kelią galimiems įsibrovėliams.[18]

Kibernetinis saugumas apima kompiuterinių tinklų ir turimos informacijos apsaugą nuo kenksmingos žalos ir sutrikimų.[19] Kibernetinis saugumas mažina pavojingų programinės įrangos, kompiuterių ir tinklų atakų riziką. Jis padeda aptikti įsilaužėlius, stabdo virusus, blokuoja pavojingas prieigas, naudoja identifikavimo sistemą ir pan.[20] Tai gebėjimas apsaugoti ir ginti kibernetinę erdvę nuo kibernetinių atakų.

Joel P. Trachtman kibernetinį saugumą apibrėžia kaip apsaugą nuo netinkamo interneto infrastruktūros naudojimo ir piktnaudžiavimo (žlugdymo). Pagal D. Shoemakerį ir A. Conkliną, kibernetinis saugumas siejamas su procesais, susijusiais su kylančių kibernetinių grėsmių identifikavimu, bei sąnaudomis pagrįstų, kontrapriemonių taikymu, kūrimu ir palaikymu.[21]

Kibernetinis saugumas – tai visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų kibernetiniams incidentams išvengti, aptikti, analizuoti ir reaguoti į juos, taip pat įprastinei elektroninių ryšių tinklų, informacinių sistemų ar pramoninių procesų valdymo sistemų veiklai, įvykus kibernetiniams incidentams, atkurti.[22]

Kaip teigia D. Štitilis[23] elektroninės erdvės globalumas sukūrė beprecedentes sąlygas daryti nusikaltimus iš bet kurio pasaulio taško, kuriame yra internetas. Todėl labai svarbu apsisaugoti nuo elektroninių nusikaltimų, kurie vyksta elektroninėje erdvėje. Kibernetinis saugumas tampa vienu iš pagrindinių tikslų, siekiant užkardyti bet kokias nusikalstamas veikas, turint omenyje, kad elektroninės grėsmės daro įtaką ne tik atskiriems vartotojams, bet ir valstybių saugumui. Kaip ir bet koks informacijos saugumas taip ir kibernetinis saugumas turi būti tinkamai užtikrinamas. Šiuo metu egzistuoja daug mechanizmų, kurie užtikrina kibernetinį saugumą, siekiant užkirsti kelią didelėms grėsmėms. Tai apima rizikos vertinimą, rizikos valdymą, saugumo

[16]E.F.Chamorro, Dr. J. R. C. Fernandez, R.M.Lopez. S.L. Fernandez, „National Cyber Security, a commitment for everybody“, 2012 m. 13 p.
[17]Kaspersky Lab, „What is Cyber-Security?, https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security.
[18]Richard A. Kemmerer, „Cybersecurity“, University of California, 2003 m.
[19]James A. Lewis, „Cyber security and Critical infrastructure protection“, Center for Strategic and International studies, 2006 m.
[20]Dan Craigen, Nadia Diakun-Thibault, Randy Purse, „Defining Cybersecurity“, 2014 m. 15 p.
[21]Shoemaker, D. and Conklin, A.. Cyberse curity: the Essential body of knowledge. Course technology, 2012 m., 11 p.
[22]LR KAM, Tomas Stamulis, „Kibernetinis saugumas. Ką saugom ir nuo ko saugom?“ 2015 m.
[23]Darius Štitilis, „Kibernetinio saugumo teisinis reguliavimas: kibernetinio saugumo strategijos“, 2013 m. 190 p.

užtikrinimą ir auditą.Moksliniai tyrimai rodo, kad kibernetinė rizika negali būti vengiama, ji turi būti atitinkamai valdoma. Siekiant užtikrinti kibernetinį saugumą svarbiausias dėmesys turėtų būti skiriamas informacijos privatumui ir duomenų apsaugai, duomenų išsaugojimui ir archyvavimui, taip pat reiktų laikytis standartinių kriterijų, tokių kaip konfidencialumas (informacijos slaptumas), vientisumas (informacijos nepakeičiamumas išsaugant ar persiunčiant) ir prieinamumas (informacija pasiekiama tada, kai jos reikia). Nacionalinis technologijų ir standartų institutas kibernetinio saugumo užtikrinimą apibrėžia kaip pagrindinių kriterijų (konfidencialumas, vientisumas, prieinamumas) atitinkamą įgyvendinimą. Tinkamą įgyvendinimą apima:užtikrinta apsauga nuo nenumatytų klaidų (naudotojo ar programinės įrangos), tinkamas atsparumo užtikrinimas nuo tyčinių įsiskverbimų.[24] Nors bėgant laikui kibernetinio saugumo suvokimo terminai ir keičiasi, tačiau vienas iš pagrindinių tikslų visada bus toks pat–informacijos apsauga, kurią apdorojame ir už kurią esame atsakingi.

Galima išskirti tokius kibernetinio saugumo pagrindinius tikslus:

- pasiekti, kad kibernetinio saugumo politika, standartai ir procedūros būtų tinkamos ir veiksmingos;
- užtikrinti, kad atsirandanti rizika būtų greitai nustatoma, tinkamai įvertinama ir imtasi atitinkamų veiksmų;
- siekti, kad kibernetinės atakos būtų laiku nustatomos ir tinkamai pašalinamos;
- didinti IT sistemų, tinklų ir kritinės infrastruktūros saugumą, vientisumą.

Organizacijos siekdamos įgyvendinti kibernetinio saugumo keliamus tikslus, kuria kibernetinio saugumo užtikrinimo planus. Tokio plano tikslas – užtikrinti, kad kibernetinio saugumo sistemos būtų veiksmingos ir atitiktų keliamus reikalavimus. Taip pat šiame plane apibrėžiami kibernetinio saugumo užtikrinimo mechanizmai.Įgyvendinant šį planą skatinama savarankiškai gerinti rizikų valdymą ir užkirsti kelią kibernetinėms grėsmėms. Tam įgyvendinti pasitelkiamas: vidaus ir išorės auditas.[25]

Vidaus auditas nustato procesų svarbą, užtikrina tinkamą kibernetinio saugumo išteklių valdymą, kontroliuoja, kad būtų imtasi tinkamų priemonių siekiant veiksmingai suvaldyti kylančias grėsmes. Vidaus audito vertinimas ir teikiamos rekomendacijos sustiprina kibernetinio saugumo kontrolės aplinką organizacijoje. Nors vidaus auditas siejamas su finansine (apima procedūras ir įrašus, kurie susiję su finansinių ataskaitų patikrinimu ir turto saugojimu) ir administracine (apima procedūras ir įrašus, kurie padeda pasiekti organizacijos tikslus) sritimis, tačiau vis daugiau dėmesio pradedama skirti kibernetiniam saugumui. Vidaus audito dėka yra užtikrinama organizacijos veiklos valdymas ir kibernetinio saugumo kontrolė. Audito rekomendacijų pagalba, įmonės gali sutelkti

[24]National Institute of Standards and Technology. NISTIR 7298, revision 2, glossary of key information security terms. 2013 m. 105 p.
[25]ISACA, „Auditing Cyber Security: Evaluating Risk and Auditing Controls“, 2017 m. 11 p.

dėmesį į atsiradusias problemines sritis, įvertinti galimą riziką ir užkirsti kelią gręsiančioms problemoms.

Organizacijos turėdamos sutartis su išorės auditoriais gali užsitikrinti nepriklausomą finansinės, administracinės veiklos ir kibernetinio saugumo įvertinimą. Išorės auditas yra tuomet kai auditą atlieka ne pati organizacija, o kitos kompetentingos, dažniausiai valstybės, tam tikslui paskirtos institucijos. Vidaus auditas gali turėti nepakankamai įgūdžių vertinant organizacijos kibernetinį saugumą, tam reikalingas išorės auditas, turintis reikalingų įgūdžių specializuotai analizei atlikti pvz. skverbimosi testavimas, serverio konfigūracijos tyrimai, informacijos saugumo užtikrinimo valdymas.

Atsižvelgiant į tinklų mąstą ir jų sudėtingumą, įmonių sistemas ir nuolat besivystančių kibernetinių grėsmių įvairovę ir pažeidžiamų sistemų skaičių, ypač svarbus vaidmuo kibernetinėje veikloje skiriamas saugumui ir informacijos užtikrinimui.Siekiant apsaugoti informacijos duomenis ir turtą išskiriamos šios apsaugos priemonių rūšys:

- administracinė kontrolė – dokumentacija, saugumo politika, vidinės procedūros, organizacinė struktūra, standartai, nuostatos, saugumo švietimas;
- techninė kontrolė – programinės, techninės priemonės, kuriomis realizuojama techninių prieigų kontrolė, užšifravimo, identifikavimo ir autentifikavimo sprendimai;
- fizinė kontrolė – patalpų, aplinkos fizinė apsauga, neautorizuotas patekimas į patalpas, įsibrovimo sekimas.[26]

Būtent šios kontrolės rūšys formuoja saugumo strategijos pagrindus.

Administracinė kontrolė yra laikoma pirmaeilės svarbos priemone. Šiame etape parengiama teisinė dokumentacija ir nuostatai, formuojama saugumo politika, atliekamos tam tikros vidaus procedūros. Administracinės kontrolės dėka tinkamai parenkama ir įdiegiama techninė ir fizinė kontrolė. Techninės kontrolės metu kontroliuojamos prieigos prie informacijos ir kompiuterinių sistemų (slaptažodžiai, užkardos, pasikėsinimas į asmeninius duomenis). Fizinės kontrolės metu užtikrinama patalpų apsauga, ji reikalinga siekiant apsaugoti ir saugoti visą pažeidžiamą turtą.

Kitas svarbus veiksnys, siekiant užtikrinti kibernetinį saugumą, yra visuomenės supratimas. Nors technologijų vystymasis yra naudingas visam pasauliui ir visoms gyvenimo sritims, tačiau sparti technologijų pažanga daro didelę įtaką požiūriui į kibernetinį saugumą ir suteikia didesnes galimybes asmeniui gauti prieigą prie bet kokios informacijos. Tai suteikia galimybę panaikinti ar platinti didelio kiekio svarbius duomenis vieno mygtuko paspaudimu. Būtent žmogiškasis faktorius išlieka viena iš silpnųjų grandžių siekiant užtikrinti kibernetinį saugumą. Vartotojų saugumo kultūra, kaip žmogiškasis – socialinis veiksnys yra vienas iš svarbiausių

[26]I. Urmanavičiūtė, „Duomenų apsaugos priemonių kompiuterizuoto parinkimo ir įvertinimo metodika“, 2010 m. 13 p.

klausimų, susijusių su kibernetinėmis grėsmėmis. Teigiama, kad 95 % duomenų praradimų susiję su žmogiškaisiais veiksniais.[27] Žmogiškoji klaida gali sukelti grėsmę kibernetiniam saugumui, kaip bet koks virusas ar kita kenkėjiška programinė įranga. Vartotojai neįvertinę rizikos atskleidžia savo turimus slaptažodžius ar atidarinėja elektroninio pašto priedus nepatikrinę ar ten nėra virusų, jie taip elgiasi manydami, kad tai yra naudinga (slaptažodžių atskleidimas) ir kad taip sutaupo laiko (netikrina virusų). PwC atliktoje apklausoje teigiama, kad pagrindiniai veiksniai sukeliantys pavojų įmonės duomenų saugumui yra tos įmonės darbuotojai. Netyčinė žmogaus klaida (48%), nepakankamas asmenų informavimas (33%), asmenų silpnumas (pasidavimas kitų įtakai) (17%) yra lemiami veiksniai organizacijos saugumo pažeidimams.[28] Vis tik žmogaus elgesys nėra nuoseklus ir žmonės yra linkę rizikuoti taip pridarydami žalos informacijos saugumui. Viena iš prevencijos priemonių – baimė. Baimė daryti tai, kas sukeltų vadovybės nepasitenkinimą. Ji yra kaip kontrolinis veiksnys, kuris gali atnešti sėkmingų rezultatų. Baimė apima šiuos komponentus – suvokimas apie grėsmės sunkumą, suvokiamos grėsmės jautrumas, atsakas į padarytus veiksmus. Siekiant stiprinti kibernetinį saugumą reikia orientuotis į žmogiškųjų veiksnių vertinimą. Siūloma sukurti konkrečią vertinimo sistemą, pagrįstą praktika, vertinant padarytą neigiamą poveikį kibernetiniam saugumui. Nors supratimas apie kibernetinį saugumą tobulės ir vystysis, tačiau nereiktų pamiršti statistikos, rodančios, kad vis dar neišsprendėme rizikos, susijusios su kibernetinio saugumo elementu – žmogaus klaida.

Kibernetinis saugumas yra specifinis veiksnys, kurio iki galo užtikrinti yra neįmanoma. Tobulėjant technologijoms, atsiranda vis naujų grėsmių kibernetiniam saugumui. Nors kuriamos strategijos, teisės aktai, kibernetinio saugumo įgyvendinimo planai, keliami nauji tikslai, pasitelkiamas išorės ir vidaus auditas vis dar ieškoma patikimų būdų užtikrinti kibernetinės erdvės saugumą. Siekiant užtikrinti kibernetinį saugumą, geriausi rezultatai gali būti pasiekti tik jeigu suinteresuotieji subjektai – naudotojai, gamintojai ir mokslininkai dirbs kartu. Vartotojai supranta savo poreikius, gamintojai – dabartinę technologijų būklę, o mokslininkai – ateities tendencijas.

[27]Shahri A, Ismail Z, Rahim N. „Security effectiveness in health information system: through improving the human factors by education and training“, Australian Journal of Basic and Applied Sciences 2012 m. 230 p.
[28]PWC. „2015 Informationsecuritybreachessurvey“, 2015 m. 4 p.

2. KIBERNETINIS SAUGUMAS NACIONALINIO SAUGUMO KONTEKSTE

2.1 Nacionalinio saugumo politikos nuostatos

Nacionalinis saugumas yra bet kurios valstybės ir jos piliečių suverenios egzistencijos ir laisvos raidos pagrindas. Todėl nacionalinio saugumo užtikrinimas yra aukščiausias kiekvienos valstybės vidaus ir užsienio politikos tikslas.[29] Lietuvos nacionalinio saugumo samprata yra įtvirtinta Lietuvos Respublikos nacionalinio saugumo pagrindų įstatyme. Jame teigiama, kad „Lietuvos nacionalinio saugumo užtikrinimas – tai Tautos ir valstybės laisvos ir demokratinės raidos sąlygų sudarymas, Lietuvos valstybės nepriklausomybės, jos teritorijos vientisumo ir konstitucinės santvarkos apsauga ir gynimas“.[30] Norint pasiekti šių tikslų nacionalinio saugumo politika vykdoma dviem kryptimis – vidaus ir užsienio politika. Šalies vidaus politikos tikslas – sumažinti valstybės pažeidžiamumą, sudaryti sąlygas saugiam ir laisvam piliečių gyvenimui. Šalies užsienio politikos tikslas – sumažinti išorines grėsmes ir daryti įtaką jų šaltiniams.

LR nacionalinio saugumo pagrindų įstatyme teigiama, kad pasiekti nacionalinio saugumo politikos tikslus galima tik sutelktomis valstybės ir piliečių pastangomis plėtoti ir stiprinti demokratiją, užtikrinti Tautos saugų būvį ir valstybės vidaus ir išorės saugumą, atgrasyti kiekvieną potencialų užpuoliką, ginti Lietuvos valstybės nepriklausomybę, teritorijos vientisumą ir konstitucinę santvarką. Norint pasiekti šių tikslų Lietuvos nacionalinio saugumo sistema remiasi valstybės institucijų veikla ir kiekvieno Lietuvos piliečio dalyvavimu, atvira pilietine visuomene, suvokiančia pavojus ir savo atsakomybę, pilietiškai susipratusia ir pasirengusia ginti Lietuvos laisvę.[31]

Teisinius Lietuvos nacionalinio saugumo pagrindus reglamentuoja įvairūs teisės aktai: Lietuvos Respublikos Konstitucija, Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas, tarptautinės teisės principai ir normos, kiti šalies įstatymai. Lietuva, vykdydama nacionalinio saugumo politiką, vadovaujasi nacionalinio saugumo strategija ir savo veiksmus derina su Europos Sąjungos bendros saugumo ir gynybos politikos strateginiais tikslais.

Žemiau pateikiami pagrindiniai teisės aktai, reglamentuojantys Lietuvos Respublikos nacionalinį saugumą.

Lietuvos Respublikos konstitucija – priimta Lietuvos Respublikos piliečių 1992 m. spalio 25 d. referendumu. Konstitucija reglamentuoja pamatinius Lietuvos valstybės ir visuomenės gyvenimo aspektus, esminius nacionalinio saugumo klausimus, t.y.: teisė priešintis ir ginti valstybę, Lietuvos Respublikos vyriausybės pareiga užtikrinti teritorijos neliečiamybę, garantuoti saugumą ir

[29]A. Petrauskaitė, R. Markelienė, R. Gedminienė – „Šalies saugumas ir gynyba“, Vilnius 2016 m. 9 p.
[30]Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas, 1997, Nr. VIII-49. Aktuali redakcija nuo 2019-01-01.1 p.
[31]Ten pat. 3 p.

viešąją tvarką, vadovautis visuotinai pripažintais tarptautinės teisės principais ir normomis, užtikrinti piliečių gerovę ir pagrindines jų teises bei laisves.

Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas - LR Seimas priėmė 1996 m. gruodžio 19 d., aktuali redakcija 2019 m. sausio 1 d. Tai yra pagrindinis įstatymas, apibrėžiantis esminius Lietuvos Respublikos nacionalinio saugumo principus, reglamentuojantis jos nacionalinio saugumo sistemą, apibrėžiantis pagrindines vidaus ir užsienio politikos nuostatas, užtikrinančias nacionalinį saugumą ir šalies gynybos principus, jų tikslus bei uždavinius. Įstatyme yra numatyta, kad nacionalinio saugumo užtikrinimo priemones sudaro: dalyvavimas tarptautinėse saugumą stiprinančiose organizacijose, narystė Šiaurės Atlanto sutarties organizacijoje ir Europos Sąjungoje, nacionalinio saugumo strateginis planavimas ir ilgalaikių valstybinių saugumo stiprinimo programų rengimas ir vykdymas, nacionalinį saugumą užtikrinančių institucijų veikla, saugumo ir gynybos sistemą reglamentuojantys įstatymai.[32]

Lietuvos Respublikos nacionalinė saugumo strategija –2002 m. patvirtina nacionalinė saugumo strategija. Tai svarbiausių saugios valstybės raidą apibrėžiančių nuostatų visuma. Strategijoje nustatomi gyvybiniai ir pirmaeiliai nacionalinio saugumo interesai, pagrindiniai rizikos veiksniai, pavojai ir grėsmės šiems interesams, nacionalinio saugumo sistemos plėtros, užsienio, gynybos ir vidaus politikos prioritetai, ilgojo ir vidutinio laikotarpių uždaviniai. Strategija yra grindžiama Lietuvos Respublikos Konstitucija, Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymu, Šiaurės Atlanto sutarties organizacijos ir Europos Sąjungos sutartimis, NATO ir ES strateginiuose saugumo politikos dokumentuose pateiktais strateginiais tikslais ir veiklos gairėmis.[33]

2.2 Grėsmės, pavojai, rizikos veiksniai

Veiksniai trukdantys valstybės ir visuomenės raidai, normaliam jos funkcionavimui, piliečių teisėms ir laisvėms, yra vertinamos kaip grėsmės nacionaliniam saugumui. Grėsmes galima suskirstyti į išorines ir vidines:

- Išorinėms grėsmėms priskiriamos tos grėsmės, kurios nepriklauso nuo žmogaus (stichinės nelaimės, gamtos katastrofos ir pan.), visuomenės (bendruomenės) ar konkrečios valstybės valios (branduolinis konfliktas tarp dviejų ar daugiau užsienio valstybių, užsienio šalių karinė intervencija, ekonominė suirutė kaimyninėje šalyje ir kt.).
- Vidinės grėsmės – tai ekonominė ir kriminogeninė situacija šalyje, socialinis saugumas, etninių mažumų padėtis ir kt.

[32]Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas, 1996 m.
[33]Lietuvos Respublikos nacionalinio saugumo strategija, 2002 m.

Lietuvos Respublikos nacionalinio saugumo strategijoje yra išskirtos grėsmės, pavojai ir rizikos veiksniai mūsų šalies saugumui. Strategijoje apibrėžiamos išorinės rizikos veiksniai, pavojai ir grėsmės Lietuvos valstybės nacionaliniam saugumui:

Konvencinės karinės grėsmės, kurias kelia Rusijos Federacijos pasirengimas panaudoti karinę jėgą siekiant savo tikslų, užmaskuotos karinės ir žvalgybos priemonės (gali būti panaudotos siekiant daryti neigiamą įtaką LR politinei sistemai, kariniams pajėgumams, teisėsaugai, socialiniam ir ekonominiam stabilumui, apsunkti nacionalinių ir NATO sprendimų priėmimo procesą ir pan.). 2018 m. išryškėjo Rusijos ambicijos globalioje politikos erdvėje ir joms pasiekti naudojamų priemonių mastai. Agresyvi užsienio politika tampa svarbiausia Rusijos naudojama priemone. Tiek Lietuva tiek kitos šalys vis aiškiau supranta Rusijos keliams grėsmes ir imasi bendrų atsako priemonių.[34]

Grėsmės euroatlantinės bendrijos vienybei (visuotiniai ir regioniniai procesai, trečiųjų šalių veikla, galintys susilpninti transatlantinius santykius).

Nestabilumas regione ir pasaulyje (konfliktai kylantys už NATO ir ES ribų, šie konfliktai sukelia didelio masto migraciją, humanitarines krizes, skatina terorizmą (terorizmo grėsmės lygis Lietuvoje išlieka žemas), organizuotą nusikalstamumą, trikdo strategiškai svarbių išteklių tiekimą).

Informacinės grėsmės (skleidžiama karo propaganda, karo ir neapykantos kurstymas, bandymai iškraipyti istorinę atmintį ir kita nepagrįsta ir klaidinanti prieš LR nacionalinio saugumo interesus nukreipta informacija), Rusija siekdama menkinti Lietuvos valstybingumą kuria nuolatinį, prieš Lietuvą nukreiptą, propagandos srautą. Jis ypač suintensyvėjo Lietuvai pradėjus atsakomuosius veiksmus prieš agresyvią Rusijos užsienio politiką.[35]

Kibernetinės grėsmės (veiksmai kibernetinėje erdvėje, kuriais siekiama sutrikdyti ypatingos svarbos informacinių infrastruktūrų funkcionavimą, vykdyti kitas nusikalstamas veikas ir taip pakenkti valstybei ir jos piliečiams), Rusijos vystomi pajėgumai kibernetinėje erdvėje tampa vienu svarbiausių elementų įgyvendinant žvalgybos ir įtakos operacijas užsienio valstybėse. Lietuvos priešininkai ir strateginiai konkurentai pasitelkdami kibernetines galimybes (kibernetinius šnipinėjimus, atakas, incidentus) bandys daryti įtaką siekiant politinio, ekonominio ir karinio pranašumo. Rusija ir Kinija pasinaudodama elektroninėmis priemonėmis įvairiais būdais sieks vogti informaciją, paveikti mūsų piliečius ar trikdyti ypatingos svarbos infrastruktūrą.[36]

Ekonominė ir energetinė priklausomybė, ekonomikos ir ūkio pažeidžiamumas, nesaugios branduolinės energetikos plėtojimas šalia LR sienų. Lietuvos kaimynystėje statoma Baltarusijos atominė elektrinė – tarptautinių branduolinės saugos standartų neatitinkantis projektas,

[34]AOTD prie KAM, Grėsmių nacionaliniam saugumui vertinimas 2019, 4 p.
[35]Ten pat. 7 p.
[36]Daniel R. Coats, „World wide threat assessment of the US intelligence community“, 2019 m. 5 p.

kuriuo siekiama stiprinti Rusijos pozicijas regione. Baltarusijos ir Rusijos atstovai daug dėmesio skiria tarptautinės bendruomenės nuomonei formuoti, taip pat Baltarusijos atstovai manipuliuoja ataskaitos rezultatais: nepaiso užfiksuotų trūkumų, teigdami, jog atominė elektrinė atitinka visus saugos reikalavimus, nepaiso pateiktų rekomendacijų, o bet kokią tarptautinių ekspertų kritiką švelnina, arba slepia.[37]

Dokumente apibrėžti ir vidaus rizikos veiksniai, pavojai ir grėsmės: socialinė ir regioninė atskirti, skurdas (socialinės atskirties didėjimas tarp regionų, aukštas skurdo lygis mažina visuomenės atsparumą neigiamai išorės įtakai ir propagandai, skatina nepasitikėjimą valstybe), demografinė krizė (mažėjantis gyventojų skaičius dėl mažo gimstamumo, visuomenės senėjimas, emigracija kelia grėsmę Lietuvos socialiniam, ekonominiam ir politiniam stabilumui bei ūkio plėtrai), korupcija (korupcijos paplitimas šalies viešajame sektoriuje, ekonomikoje ir versle gali kenkti asmenų ir valstybės interesams, kompromituoti įstatymo viršenybės principą, mažinti piliečių tikėjimą demokratijos vertybėmis, mažinti patrauklumą užsienio investuotojams), organizuotas nusikalstamumas (gali kelti pavojų visuomenės saugumui, neigiamai veikti valstybės ekonominį ir politinį gyvenimą), terorizmas, ekstremizmas, radikalėjimas (religinio ir politinio ekstremizmo ideologijoms pritariančių asmenų ketinimai ir pajėgumai vykdyti teroristinius nusikaltimus LR, tačiau radikalėjimo tendencijų Lietuvos musulmonų bendruomenėje nepastebima. Prielaidos radikalizmo apraiškoms Lietuvoje galėtų atsirasti tik jei dėl išorinių įtakų musulmonų bendruomenė skiltų ir tuo pasinaudotų iš užsienio atvykstantys prieštaringai vertinamų islamiškų organizacijų atstovai.), valstybės ekstremalios situacijos (gamtiniai, techniniai, ekologiniai, socialiniai įvykiai, epidemijos, galinčios sukelti pavojų gyventojų sveikatai, aplinkai), vertybių krizė (nepagarba prigimtinėms žmogaus teisėms, rasinės, tautinės ar religinės nesantaikos kurstymas, religinių ideologijų plitimas).[38]

Šiuolaikinių grėsmių prigimties sudėtingumą lemia egzistuojantys skirtingi grėsmių šaltiniai, kurie gali būti tiek fiziniai (gamtos stichijos), tiek socialiniai (teroristinės grupuotės, priešiškumas kitataučiams ir pan.). Grėsmės šaltinis gali būti tiek konkretus subjektas (asmuo, institucija, struktūra), tiek procesas, reiškinys ar netikėtas įvykis (migracija, uraganas, epidemija, techninė avarija ir kt.).[39] Siekiant kiekybiškai įvertinti grėsmes, stengiamasi nustatyti, kokia yra grėsmės pasireiškimo tikimybė ir kokio dydžio nuostolius grėsmė gali sukelti. Įvertinus grėsmes pagal jų tikimybes ir daromą žalą, galima sudaryti tam tikrą pasaulio, šalies ar atskiros bendruomenės grėsmių suvestinę (grėsmių lauką).[40]

[37]AOTD prie KAM, Grėsmių nacionaliniam saugumui vertinimas 2019, 49 p.
[38]Lietuvos Respublikos nacionalinio saugumo strategija, 2002 m.
[39]T. Janeliūnas, „Komunikacinis saugumas“, 2007 m. 20-21 p.
[40]Vareikis E. Tarptautinis ir nacionalinis saugumas. VDU leidykla, 2005, 12–14 p.

Iškylančias saugumo problemas valstybės gali spręsti dviem būdais: arba remtis tik savo jėgomis, arba pasirinkti tarptautinio saugumo strategiją t.y. dalyvauti įvairiose tarptautinėse organizacijose. Lietuva nacionalinį saugumą užtikrina kompleksiškai derindama abu būdus. Be to, atsižvelgiant į tai, kad tarptautinis saugumas yra nedalomas, saugumą siekiama užtikrinti kaip platesnės regioninės, europinės ir pasaulio valstybių bendrijos saugumo neatskiriamą sudedamąją dalį. Reikia įvertinti, kad Lietuva būdama palyginti nedidelė valstybė, yra gana įdomioje geografinėje/politinėje padėtyje ir turi skirti ypatingą dėmesį nacionalinio saugumo politikos formavimui bei operatyviai reaguoti į keliančius grėsmę veiksnius. Daugelis nacionalinio saugumo rizikos veiksnių ir pavojų yra tęstinio pobūdžio ir sunku juos visiškai panaikinti, todėl nacionalinio saugumo užtikrinimui lieka aktualių problemų. Tik nuolatinės ir kompleksinės pastangos gali užtikrinti minimalią jų tikimybę virsti grėsmėmis ir neleisti atsirasti nepalankiems padariniams ekonominėje, socialinėje, ekologinėje ar kitose srityse.[41]

2.3 Kibernetinio saugumo užtikrinimo Lietuvoje prielaidos ir formos

Kibernetinio saugumo sąvoka šiais laikais tampa vis aktualesniu ir daugiau dėmesio sulaukiančiu reiškiniu. Kibernetinis saugumas yra labai specifinė veiklos sritis, kuri yra svarbi ne tik dėl Lietuvos nacionalinio saugumo, bet ir dėl valstybės piliečių. Norint kuo geriau užtikrinti kibernetinį saugumą reikalingas nuoseklus ir detalus teisinis reglamentavimas. Lietuvoje kibernetinį saugumą užtikrina šie teisiniai dokumentai:

Pirmuosius informacijos saugumo reikalavimus Lietuvos Respublikos vyriausybė patvirtino 1997 metais, siekdama užtikrinti duomenų patikimumą bei apsaugą nuo neteisėto panaudojimo. Šiuo nutarimu vyriausybė įpareigoja duomenų valdytojus vadovautis rekomenduojamais Lietuvos standartais, kurie atitinka ISO/IEC standartus, arba kitomis rekomendacijomis. Taip pat duomenų valdytojas privalo pasirūpinti duomenų apsaugos sistemos tobulinimu, kasmet peržiūrėti instrukcijas bei kitus dokumentus, susijusius su duomenų apsauga ir jeigu yra pasikeitimų, juos atnaujinti.[42]

Informacinėje visuomenėje lemiamą reikšmę įgyja informacija, sudaranti sąlygas valstybės institucijoms ir įstaigoms sėkmingai vykdyti savo funkcijas, ir informacijos technologijos, leidžiančios šią informaciją gauti, apdoroti, perteikti ir saugoti. Informacinių technologijų pagalba, duomenų naudotojai turi užtikrinti tinkamą informacijos kontrolę ir apsaugą nuo galimų pavojų. Dėl šių priežasčių 2001 metais (strategija nebegalioja nuo 2013 m.) Lietuvos Respublikos vyriausybė

[41]Erika Matulonytė, „Grėsmių nacionaliniam saugumui nustatymas ir jų prevencijos galimybės“, 2008 m.
[42]Lietuvos Respublikos vyriausybės nutarimas „Dėl duomenų apsaugos valstybės ir vietos savivaldos informacinėse sistemose“, 1997 m., 3 p.

pasirašė nutarimą „Dėl informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo“.[43] Pagrindiniai šios strategijos tikslai buvo:

- informacijos technologijų saugos teisinio reglamentavimo plėtra (bendrųjų duomenų saugos reikalavimų pagal duomenų kategorijas, atsižvelgiant į tarptautinius standartus, Ekonominio bendradarbiavimo ir plėtros organizacijos, NATO ir ES rekomendacijas, Europolo ir Šengeno informacinių sistemų reikalavimus, nustatymas; elektroninio verslo saugos reikalavimų nustatymas; elektroninio susirašinėjimo saugos reikalavimų nustatymas; kompiuterių tinklų saugos reikalavimų nustatymas; interneto tarnybinių stočių saugos reikalavimų nustatymas, asmens identifikavimo elektroninio parašo saugos reikalavimų nustatymas; atsakomybės pagal pažeidimų pobūdį nustatymas;);
- svarbiausiųjų valstybės informacinių sistemų saugos stiprinimas;
- informacinių technologijų atitikties vertinimo sistemos kūrimas;
- metodologinės ir konsultacinės sistemos plėtra;
- valstybės tarnautojų mokymas informacijos technologijų saugos, duomenų saugos įgaliotinių įgūdžių ugdymas;
- informacijos technologijų saugos įgyvendinimo kontrolės užtikrinimas.

Vis dėl to valstybės informacinių išteklių ir informacijos valdymo trūkumai neleido valstybei efektyviai valdyti informacinių išteklių, todėl 2006 m. (strategija nebegalioja nuo 2008 m.) Lietuvos Respublikos vyriausybė priėmė nutarimą „Dėl elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinės strategijos iki 2008 metų ir jos įgyvendinimo priemonių plano patvirtinimo“, šis dokumentas buvo skirtas valstybinėmis institucijoms. Valstybės strategijos pagrindiniai tikslai:

- tobulinti elektroninės informacijos saugos koordinavimą ir priežiūrą;
- teisės aktais reguliuoti elektroninės informacijos saugą;
- kelti elektroninės informacijos saugos kultūrą;
- tobulinti elektroninės informacijos perdavimo infrastruktūros saugą;
- skatinti elektroninės informacijos saugos užtikrinimo projektų įgyvendinimą.

2006 m. Lietuvos Respublikos vyriausybė taip pat pasirašė nutarimą „Dėl Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepcijos patvirtinimo“.[44] Numatoma, kad Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymas reglamentuos santykius, susijusius su elektroninių ryšių tinklų ir informacijos

[43]Lietuvos Respublikos vyriausybės nutarimas „Dėl informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo“, 2001 m., 2 p.
[44]Lietuvos Respublikos vyriausybė, nutarimas „Dėl Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepcijos patvirtinimo“, 2006 m. 2p.

saugumu, sudarys sąlygas saugios informacinės visuomenės plėtrai, didins vartotojų pasitikėjimą informacine visuomene.

Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimu Nr. 796 „Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 metais programos patvirtinimo“[45] buvo patvirtinta Kibernetinio saugumo plėtros programa 2011-2019 metams. Kibernetinio saugumo programos 2011-2019 metams paskirtis – nustatyti elektroninės informacijos saugos (kibernetinio saugumo) plėtros tikslus ir uždavinius, kad būtų užtikrintas elektroninės informacijos 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.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. Nustatyti tokie kibernetinio saugumo programos įgyvendinimo tikslai:

- pasiekti, kad būtų užtikrintas valstybės informacinių išteklių saugumas.
- užtikrinti veiksmingą ypatingos svarbos informacinės infrastruktūros funkcionavimą.
- siekti užtikrinti Lietuvos gyventojų ir asmenų, esančių Lietuvoje, saugumą kibernetinėje erdvėje.

2014 m. gruodžio 11 d. Lietuvos Respublikos Seimas priėmė kibernetinio saugumo įstatymą (nauja redakcija 2018 m. birželio 27 d. Nr. XIII-1299).[46] Šis įstatymas nustato kibernetinio saugumo principus, kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijas, šių institucijų įgaliojimus kibernetinio saugumo srityje, kibernetinio saugumo subjektų pareigas, taip pat tarpinstitucinį bendradarbiavimą.

Įstatyme kibernetinis saugumas grindžiamas bendraisiais teisės principais, elektroninių ryšių veiklos reguliavimo principais ir šiais kibernetinio saugumo principais:

- kibernetinės erdvės nediskriminavimo – teisės aktų nuostatos yra taikomos, o gėriai yra saugomi vienodai tiek fizinėje, tiek kibernetinėje erdvėje;
- kibernetinio saugumo rizikos valdymo – taikomos kibernetinio saugumo priemonės turi užtikrinti kibernetinio saugumo subjektų reguliariai įvertinamos rizikos suvaldymą;

[45]Lietuvos Respublikos vyriausybė, nutarimas „Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 metais programos patvirtinimo“, 2011 m.
[46]Lietuvos Respublikos Seimas, Kibernetinio saugumo įstatymas, 2018 m.

- kibernetinio saugumo proporcingumo – taikomos teisinės, organizacinės ir techninės kibernetinio saugumo priemonės neturi apriboti kibernetinio saugumo subjektų veiklos kibernetinėje erdvėje labiau, negu tai būtina;
- viešojo intereso viršenybės – taikomos kibernetinio saugumo priemonės pirmiausia turi užtikrinti viešojo intereso apsaugą, tačiau neturi iš esmės pažeisti atskirų vartotojų teisių ar neproporcingai apriboti jų laisvės kibernetinėje erdvėje;
- standartizacijos ir technologinio neutralumo – įgyvendinant kibernetinio saugumo priemones, kibernetinio saugumo subjektai skatinami vadovautis nacionaliniais, Europos Sąjungos ir kitais tarptautiniais ryšių ir informacinių sistemų kibernetinio saugumo standartais ir specifikacijomis, nereikalaujant taikyti kokios nors konkrečios rūšies technologijos ir nesuteikiant jai pirmenybės;
- subsidiarumo – už ryšių ir informacinių sistemų ir jomis teikiamų paslaugų kibernetinį saugumą yra atsakingi šias sistemas valdantys ir paslaugas jomis teikiantys kibernetinio saugumo subjektai. Srityse, kurios priklauso išimtinei kibernetinio saugumo subjektų kompetencijai, kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos veiksmų imasi tik tada, kai ryšių ir informacinių sistemų ir jomis teikiamų paslaugų kibernetinio saugumo negali užtikrinti šias sistemas valdantys ir paslaugas jomis teikiantys kibernetinio saugumo subjektai.

Taip pat įstatyme pabrėžiama, kad taikant kibernetinį saugumą reglamentuojančias teisės normas, turi būti atsižvelgiama į visus nurodytus principus. Šie principai turi būti derinami tarpusavyje, nė vienam iš jų iš anksto nesuteikiama pirmenybė.

Kibernetinio saugumo įstatyme patvirtinta nuostata, kad Kibernetinio saugumo politikos strateginius tikslus, prioritetus ir jiems pasiekti būtinas priemones nustato Lietuvos Respublikos Vyriausybė, Kibernetinio saugumo politiką formuoja, jos įgyvendinimą organizuoja, kontroliuoja ir koordinuoja Lietuvos Respublikos krašto apsaugos ministerija. Kibernetinio saugumo politiką įgyvendina Nacionalinis kibernetinio saugumo centras, Valstybinė duomenų apsaugos inspekcija, Lietuvos policija ir kitos institucijos, kurių funkcijos yra susijusios su kibernetiniu saugumu.

Žemiau pateikiami institucijų įgaliojimai kibernetinio saugumo politikos įgyvendinime[47] (1 lent.).

1 lentelė. Kibernetinio saugumo įgyvendinimas.

Kibernetinio saugumo politikos įgyvendinimo subjektai	Suteikti įgaliojimai
Lietuvos Respublikos vyriausybė	1. Tvirtina Nacionalinę kibernetinio saugumo strategiją; 2. Tvirtina Kibernetinio saugumo tarybos institucinę sudėtį; 3. Tvirtina ypatingos svarbos informacinės

[47]Lietuvos Respublikos Seimas, Kibernetinio saugumo įstatymas, 2018 m.

	infrastruktūros identifikavimo metodiką ir ypatingos svarbos informacinės infrastruktūros ir jos valdytojų sąrašą; 4. Tvirtina organizacinius ir techninius kibernetinio saugumo reikalavimus, taikomus kibernetinio saugumo subjektams; 5. Tvirtina Nacionalinį kibernetinių incidentų valdymo planą; 6. Vadovauja kibernetinio saugumo krizių valdymui.
Krašto apsaugos ministerija	1. Koordinuoja Nacionalinės kibernetinio saugumo strategijos rengimą, teikia ją Vyriausybei tvirtinti; 2. Teikia Vyriausybei tvirtinti organizacinius ir techninius kibernetinio saugumo reikalavimus, taikomus kibernetinio saugumo objektams; 3. Teikia Vyriausybei tvirtinti Nacionalinė kibernetinių incidentų valdymo planą; 4. Teikia Vyriausybei tvirtinti ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką; 5. Teikia Vyriausybei tvirtinti ypatingos svarbos informacinės infrastruktūros ir jos valdytojų sąrašą; 6. Tvirtina tipinį kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planą; 7. Tvirtina ypatingos svarbos informacinių infrastruktūrų kibernetinės gynybos planą; 8. Nustato Nacionalinio kibernetinio saugumo centro reagavimo į kibernetinio saugumo subjektų ryšių ir informacinėse sistemose įvykusius kibernetinius incidentus tvarką; 9. Tvirtina techninių kibernetinio saugumo priemonių diegimo planą, nustato jų diegimo ir valdymo valstybės informaciniuose ištekliuose ir ypatingos svarbos informacinėje infrastruktūroje tvarką; 10. Dalyvauja kibernetinio saugumo krizių valdyme; 11. Steigia kibernetinio saugumo informacinį tinklą ir tvirtina jo nuostatus; 12. Tvirtina kibernetinio saugumo tarybos reglamentą ir personalinę sudėtį.
Kibernetinio saugumo taryba	1. teikia kibernetinio saugumo dalyviams pasiūlymus dėl kibernetinio saugumo prioritetų, plėtros krypčių, siektinų rezultatų ir jų įgyvendinimo būdų; 2. teikia kibernetinio saugumo dalyviams pasiūlymus dėl viešojo sektoriaus, verslo ir mokslo bendradarbiavimo galimybių kibernetinio saugumo užtikrinimo srityje; 3. analizuoja kibernetinio saugumo užtikrinimo tobulinimo tendencijas, teikia kibernetinio saugumo dalyviams išvadas ir pasiūlymus dėl kibernetinių incidentų valdymo; 4. teikia kibernetinio saugumo dalyviams rekomendacijas dėl kibernetinio saugumo stiprinimo.
Nacionalinis kibernetinio saugumo centras	1. atlieka kibernetinio saugumo subjektų ir jų valdomų ryšių ir informacinių sistemų atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams,

	taikomiems kibernetinio saugumo subjektams, priežiūrą ir kibernetinio saugumo būklės tyrimu 2. duoda nurodymus kibernetinio saugumo subjektams pateikti informaciją, būtiną kibernetinio saugumo subjektų ir jų valdomų ryšių ir informacinių sistemų atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams, taikomiems kibernetinio saugumo subjektams, ir kibernetinio saugumo būklės įvertinimui atlikti 3. taiko technines priemones, siekdamas įvertinti valstybės informacinių išteklių ir ypatingos svarbos informacinių infrastruktūrų atsparumą kibernetiniams incidentams; 4. duoda nurodymus, susijusius su kibernetinio saugumo užtikrinimu ir nustatytų kibernetinio saugumo trūkumų pašalinimu, nustato šių nurodymų įvykdymo terminą subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojams, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjams ir elektroninės informacijos prieglobos paslaugų teikėjams; 5. duoda nurodymus kibernetinio saugumo subjektams, išskyrus skaitmeninių paslaugų teikėjus, savo lėšomis atlikti nepriklausomą ryšių ir informacinių sistemų arba jomis teikiamų paslaugų saugumo auditą ir pateikti šio audito rezultatus, jei jie organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše nustatyta tvarka nepateikia techninės informacijos, reikalingos ryšių ir informacinių sistemų ar jomis teikiamų paslaugų kibernetinio saugumo būklei įvertinti; 6. nacionaliniu lygmeniu stebi kibernetinius incidentus ir atlieka rizikos kibernetinėje erdvėje bei kibernetinių incidentų analizę; 7. nacionaliniu lygmeniu organizuoja kibernetinių incidentų kibernetinio saugumo subjektų ryšių ir informacinėse sistemose valdymą; 8. kibernetinio incidento metu taiko būtinas kibernetinio saugumo priemones; 9. dalyvauja kibernetinio saugumo krizių valdyme.
Valstybinės duomenų apsaugos inspekcija	1. Valstybinė duomenų apsaugos inspekcija įgyvendina kibernetinio saugumo politiką asmens duomenų apsaugos srityje ir atlieka 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamente (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL 2016 L 119, p. 1) nustatytas priežiūros institucijos užduotis
Policija	1. renka, analizuoja ir apibendrina informaciją apie kibernetinius incidentus, galimai turinčius nusikalstamų veikų požymių;

	2. nustato kibernetinio saugumo subjektams informacijos, reikalingos kibernetiniams incidentams, galimai turintiems nusikalstamų veikų požymių, užkardyti ir tirti, pateikimo policijai tvarką; 3. turi teisę, kai paslaugų gavėjas galimai dalyvauja ar jo naudojama ryšių ir informacinių technologijų įranga galimai yra naudojama nusikalstamai veikai, be teismo sankcijos duoti nurodymą viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjui, elektroninės informacijos prieglobos paslaugų teikėjui ir skaitmeninių paslaugų teikėjui ne ilgiau kaip 48 valandoms, o ilgesniam laikui – su apylinkės teismo sankcija apriboti viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų ir skaitmeninių paslaugų teikimą paslaugų gavėjui ir (arba) nurodyti taikyti priemones, šalinančias nusikalstamų veikų kibernetinėje erdvėje priežastis. 4. turi teisę duoti nurodymą viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjui, elektroninės informacijos prieglobos paslaugų teikėjui ir skaitmeninių paslaugų teikėjui išsaugoti su jų teikiamomis paslaugomis susijusią informaciją, iš kurios galima nustatyti naudotos ryšio paslaugos tipą, taikytas technines priemones ir naudojimo laiką, paslaugos gavėjo tapatybę, pašto, geografinės padėties adresą, telefono ir bet kokį kitą prieigos numerį, informaciją apie sąskaitas ir atliktus mokėjimus paslaugos sutarties arba susitarimo pagrindu ir kitą informaciją ryšių aparatūros įrengimo vietoje, turimą pagal paslaugos sutartį arba susitarimą, šią informaciją gauti, o kai yra motyvuota teismo nutartis, gauti paslaugų gavėjo srauto duomenis ir kontroliuoti šiame punkte nurodytos perduodamos informacijos turinį.

Kibernetinio saugumo įstatyme pirmą kartą reglamentuotas tarpinstitucinis bendradarbiavimas ir atsakomybė už kibernetinio saugumo reikalavimų pažeidimus. Taip pat pažymima, kad Nacionalinis kibernetinio saugumo centras, Ryšių reguliavimo tarnyba, Policija turi bendradarbiauti tiriant kibernetinius nusikaltimus, keistis su kibernetinių incidentų tyrimais susijusia informacija, reikalinga pagal kompetenciją šių institucijų funkcijoms atlikti. Nacionalinis kibernetinio saugumo centras ir Valstybinė duomenų apsaugos inspekcija bendradarbiauja tiriant kibernetinius incidentus, susijusius su asmens duomenų ir (ar) privatumo apsaugos pažeidimais, keičiasi informacija, reikalinga teisės aktų nustatytoms funkcijoms, susijusioms su asmens duomenų ir (ar) privatumo apsaugą pažeidžiančių kibernetinių incidentų tyrimu, atlikti.

2018 m. buvo patvirtinta pirmoji Lietuvoje Nacionalinė kibernetinio saugumo strategija – esminis dokumentas, kuriame, atsižvelgiant į aplinkos analizės išvadas buvo įtvirtinti viešojo ir privataus sektorių, Lietuvos mokslo ir studijų institucijų penkerių metų tikslai ir uždaviniai kibernetinio saugumo srityje. Įgyvendinant strategiją yra siekiama stiprinti valstybės kibernetinį

saugumą ir kibernetinių gynybos pajėgumų plėtrą, užtikrinti nusikalstamų veikų prevenciją, užkardymą ir tyrimą, skatinti kibernetinio saugumo kultūrą ir inovacijų plėtrą, stiprinti glaudų viešojo ir privataus sektorių, tarptautinį bendradarbiavimą ir užtikrinti tarptautinių įsipareigojimų kibernetinio saugumo srityje vykdymą.[48]

Apžvelgus visus kibernetinį saugumą reglamentuojančius teisės aktus, galima teigti, kad iki 2011 metų kibernetinio saugumo užtikrinimui nebuvo skiriama pakankamai dėmesio, ir tik 2011 m. patvirtinus kibernetinio saugumo plėtros programą 2011-2019 m. buvo užsibrėžtas tikslas – plėtoti elektroninės informacijos saugą Lietuvoje, užtikrinti kibernetinį saugumą ir pasiekti, kad 2019 metais teisės aktų nustatytus elektroninės informacijos saugos reikalavimus atitinkančių valstybės informacinių išteklių dalis pasiektų 98 procentus visų valstybės informacinių išteklių.

2014 m. priėmus Kibernetinio saugumo įstatymą (nauja redakcija 2018 m.) buvo reglamentuotas kibernetinio saugumo užtikrinimas, taip pat apibrėžta, kas turi prisiimti atsakomybę ir kokios institucijos yra atsakingos už kibernetinio saugumo įgyvendinimą.

Tobulėjant informacinėms technologijoms, sunkėja ir kibernetinių atakų pobūdis, todėl būtina, kad valstybiniu lygmeniu, nuolat ir sistemingai, būtų sprendžiamos tinklų ir informacijos saugumo problemos, stiprinama teisinė bazė šioje srityje. Be teisinio reglamentavimo papildomai turi būti skiriamas dėmesys nuolatiniam informacinių technologinių resursų atnaujinimui, pastoviam finansavimui užtikrinant saugumą, nuolatiniam LR politikų dėmesiui kibernetiniam saugumui bei specialistų paruošimui dirbti institucijose, atsakingose už kibernetinį saugumą.

[48]Lietuvos Respublikos nacionalinio saugumo strategija, 2018 m.

3. EUROPINIS IR TRANSATLANTINIS LYGMUO

3.1 Europos Sąjunga ir kibernetinis saugumas

Kaip teigė buvęs ilgametis Europos Komisijos prezidentas Žanas Klodas Junkeris – kibernetinės atakos demokratijos ir ekonomikos stabilumui gali būti daug pavojingesnės nei ginklai ar tankai. Kibernetinės atakos nežino sienų ir niekas nėra nuo jų apsaugotas. Todėl kibernetinis saugumas akcentuojamas ne viename Europos Sąjungos (toliau – ES) dokumente. 2001 m. komunikate tinklų ir informacijos saugumas apibrėžiamas kaip tinklo ar informacinės sistemos atsparumas tam tikru lygmeniu atsitiktiniams įvykiams ar nusikalstamiems veiksmams, kurie kelia pavojų šiuose tinkluose ir sistemose sukauptų ir jais perduodamų duomenų bei susijusių paslaugų prieinamumui, tikrumui, vientisumui ir konfidencialumui.[49] Reaguodama į grėsmes saugumui, 2004 m. Europos bendrija nusprendė įsteigti Europos tinklų ir informacijos saugumo agentūrą (ENISA).[50] Ši agentūra prisideda prie tinklų ir informacijos saugumo kultūros plėtojimo, siekdama kuo geriau apsaugoti piliečius, vartotojus, įmones ir viešojo sektoriaus organizacijas visoje ES. 2006 m. ES atkreipė dėmesį į saugios Europos kibernetinės erdvės sukūrimą pasitelkiant visus socialinius valdžios partnerius, nes didžiuliai informacijos kiekiai yra saugomi privačių įmonių duomenų centruose, valstybės institucijų duomenų saugyklose ir informacinių sistemų duomenų bazėse. Tokios informacijos paviešinimas, nesavalaikis naudojimas ar sugadinimas gali sutelkti didžiules problemas ir ženklius nuostolius verslo organizacijoms ar viešojo administravimo subjektams.[51]

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 gerina ekonominius rodiklius, užtikrina visuomenės socialinės gerovės augimą bei piliečių gyvenimo kokybę.

2013 m. buvo paskelbta Europos kibernetinio saugumo strategija kartu su Komisijos direktyvos dėl tinklų ir informacinių sistemų saugumo siūlymu.[52] ES parengtoje kibernetinio saugumo strategijoje yra išskirti kibernetinio saugumo principai:

[49]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, 2001m.
[50][interaktyvus], Žiūrėta[2019-11-28] <https://www.enisa.europa.eu/>
[51]Komisijos komunikatas Tarybai, Europos Parlamentui, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui. Saugios informacinės visuomenės strategija – „Dialogas, partnerystė ir teisių suteikimas“, 2006 m. 6 p.
[52]Bendras komunikatas Europos parlamentui, tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir regionų komitetui, Europos Sąjungos kibernetinio saugumo strategija 2013 m.

- pagrindinių teisių, žodžio laisvės, asmens duomenų ir privatumo apsauga. Individų teisės negali būti užtikrintos be saugių tinklų ir sistemų. Bet koks su asmens duomenimis susijęs dalijimasis informacija kibernetinio saugumo tikslais turėtų atitikti ES duomenų apsaugos teisės nuostatas ir jį vykdant reikia paisyti individo teisių toje srityje;
- prieiga visiems. Kiekvienas turėtų turėti galimybę naudotis internetu ir netrukdomai gauti informaciją. Norint užtikrinti visų žmonių saugią prieigą prie interneto, turi būti užtikrintas interneto vientisumas ir saugumas;
- demokratiškas ir veiksmingas daugelio suinteresuotų šalių dalyvavimu grindžiamas valdymas. Šiuo metu interneto išteklius, protokolus ir standartus visą laiką valdo ir jo ateities plėtrą vykdo daug suinteresuotų šalių, tarp kurių nemažai komercinių ir nevyriausybinių subjektų. ES nuolat tvirtina, kad dabartiniam interneto valdymo modeliui svarbus visų suinteresuotų šalių dalyvavimas, ir remia plataus suinteresuotų šalių rato dalyvavimu grindžiamo valdymo modelį;
- bendra atsakomybė siekiant užtikrinti saugumą. Augant priklausomybei nuo informacinių ir ryšių technologijų visose žmogaus gyvenimo srityse, atsirado pažeidžiamumas, kurį reikia tinkamai apibrėžti, nuodugniai išnagrinėti, pašalinti arba sumažinti. Norint didinti kibernetinį saugumą, visi subjektą turi pripažinti, kad atsakomybė yra bendra, imtis savisaugos veiksmų ir prireikus koordinuotai sureaguoti.[53]

ES turėtų visiems užtikrinti saugią internetinę aplinką suteikdama didžiausią įmanomą laisvę ir saugumą. Pripažįstant, kad spręsti saugumo užduotis kibernetinėje erdvėje didžia dalimi yra valstybių narių užduotis, šioje strategijoje siūlomi konkretūs veiksmai, kuriais galima padidinti bendrus ES pasiektus rezultatus. Vieni veiksmai yra artimiausio laikotarpio, kiti – tolimos perspektyvos; numatyta įvairių politikos priemonių ir jos siejamos su įvairiais subjektų tipais: ES institucijomis, valstybėmis narėmis ar pramone.ES kibernetinio saugumo strategijoje išskiriami penki strateginiai prioritetai:

- pasiekti kibernetinį atsparumą. Remiant kibernetinį atsparumą Europos Sąjungoje, plėtoti pajėgumus ir veiksmingai bendradarbiauti turi ir valdžios įstaigos, ir privatusis sektorius. Naudojantis teigiamais iki šiol atliktų veiksmų rezultatais, tolesnė ES veikla gali ypač padėti pašalinti tarpvalstybinio pobūdžio kibernetinius pavojus bei grėsmes ir koordinuotai reaguoti ekstremaliose situacijose. Tai labai padėtų pagerinti vidaus rinkos veikimo sklandumą ir padidintų vidaus saugumą Europos Sąjungoje.Elektroninių ryšių pagrindų direktyvoje[54] elektroninių ryšių paslaugų teikėjai įpareigojami tinkamai valdyti jų tinklams kylančias grėsmes ir pranešti apie

[53]Bendras komunikatas Europos parlamentui, tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir regionų komitetui, Europos Sąjungos kibernetinio saugumo strategija 2013 m.
[54]Europos Parlamento ir Tarybos direktyva 2002/21/EB „Dėl elektroninių ryšių tinklų ir paslaugų bendrosios reguliavimo sistemos“, 2002 m.

svarbius saugumo pažeidimus. Taip pat ES duomenų apsaugos teisės aktuose[55] reikalaujama, kad duomenų valdytojai užtikrintų duomenų apsaugos reikalavimus ir apsaugos priemones, įskaitant su saugumu susijusias priemones, o viešai prieinamų e. ryšių paslaugų srityje duomenų valdytojai privalo apie asmens duomenų saugumo pažeidimą pranešti kompetentingoms nacionalinėms institucijoms;

- radikaliai sumažinti elektroninių nusikaltimų skaičių.Elektroniniai nusikaltimai yra viena sparčiausiai dažnėjančių nusikaltimo formų: kasdien jų aukomis tampa daugiau nei milijonas žmonių. Kibernetiniai nusikaltėliai ir elektroninių nusikaltimų tinklai tampa vis sudėtingesni; kovojant su jais reikia apsirūpinti tinkamomis veiklos priemonėmis ir pajėgumais. Elektroniniai nusikaltimai labai pelningi ir kelia mažą grėsmę piktadariams, kurie paprastai pasinaudoja svetainių domenų anonimiškumu. Elektroninių nusikaltimų sienos nesulaiko: pasaulinė interneto skvarba reiškia, kad norėdamos duoti atkirtį šiai augančiai grėsmei teisėsaugos institucijos turi veikti koordinuotai ir bendradarbiaudamos.ES kibernetinio saugumo strategijoje išskiriami būdai, kaip kuo efektyviau apsisaugoti nuo kibernetinių nusikaltimų: griežti ir veiksmingi teisės aktai, veiklos pajėgumų kovai su elektroniniais nusikaltimais didinimas, ES lygmens koordinavimo gerinimas;
- sukurti kibernetinės gynybos politiką ir pajėgumus, susijusius su bendra saugumo ir gynybos politika.Kibernetinio saugumo pastangos Europos Sąjungoje turi būti dedamos ir kibernetinės gynybos srityje. Siekiant sustiprinti valstybių narių gynybos ir nacionalinio saugumo interesams naudojamas ryšių ir informacinės sistemas, kibernetinės gynybos pajėgumai turėtų būti plėtojami aptikimo, reagavimo ir atkūrimo po sudėtingų kibernetinių grėsmių segmentuose;
- plėtoti pramoninius ir technologinius išteklius kibernetiniams saugumui užtikrinti.Europa turi puikių mokslinių tyrimų ir technologijų plėtros pajėgumų, tačiau daugelis novatoriškas informacinių ryšių technikos prekes ir paslaugas teikiančių pasaulinių lyderių įsisteigę ne Europos Sąjungoje. Kyla grėsmė, kad Europa taps pernelyg priklausoma ne tik nuo kitur pagamintų informacinių ryšių technikos, bet ir nuo anapus jos sienų sukurtų saugumo sprendimų. Būtina užtikrinti, kad ES ir trečiosiose šalyse pagaminta techninė ir programinė įranga, kuri naudojama ypatingos svarbos paslaugoms ir infrastruktūrai, ir vis labiau – nešiojamiesiems įtaisams, būtų patikima, saugi ir užtikrintų asmens duomenų apsaugą;
- sukurti nuoseklią tarptautinę elektroninės erdvės politiką ir remti pagrindines ES vertybes. Išsaugoti atvirą, laisvą ir saugią kibernetinę erdvę yra pasaulinio masto uždavinys, kurį ES turėtų spręsti kartu su atitinkamais tarptautiniais partneriais ir organizacijomis, privačiuoju sektoriumi ir pilietine visuomene. Tarptautine kibernetinės erdvės politika ES sieks skatinti interneto atvirumą ir laisvę, palaikys pastangas formuoti elgesio normas ir taikyti kibernetinėje

[55]Europos Parlamento ir Tarybos direktyva (95/46/EB) „Dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo“, 1995 m. ir Europos Parlamento ir Tarybos direktyva 2002/58/EB „Dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje“, 2002 m.

erdvėje galiojančius tarptautinius teisės aktus. ES taip pat sieks mažinti skaitmeninę atskirtį ir aktyviai prisidės prie tarptautinių pastangų sukurti kibernetinio saugumo pajėgumus. ES tarptautinis įsipareigojimas kibernetiniais klausimais bus grindžiamas ES pagrindinėmis vertybėmis – žmogaus orumu, laisve, demokratija, lygybe, teisinės valstybės principais ir pagarba pagrindinėms teisėms.[56]

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.

Apibendrinant galima teigti, kad ES kibernetinio saugumo strategija yra išsamus strateginis dokumentas, kuriame reglamentuojami esminiai principai, tikslai, kibernetinio saugumo užtikrinimo lygiai bei valstybių narių ir Komisijos bendradarbiavimo mechanizmas.

2017 m. ES institucijos priėmė svarbų sprendimą, kad būtų sustiprintas tarpusavio bendradarbiavimas kovoje su kibernetiniais išpuoliais. 2017 m. buvo įsteigta nuolatinė Kompiuterinių incidentų tyrimo tarnyba[57] (CERT-EU), kuri apima visas ES institucijas, įstaigas ir agentūras. Šiuo metu veikianti darbo grupė buvo sustiprinta ir tapo nuolatine veiksminga tarnyba, atsakinga už tai, kad būtų užtikrintas koordinuotas ES atsakas į kibernetinius išpuolius prieš jos institucijas.

[56]Europos Parlamento ir Tarybos direktyva 2002/21/EB „Dėl elektroninių ryšių tinklų ir paslaugų bendrosios reguliavimo sistemos“, 2002 m.
[57]Europos Vadovų Taryba, „Kibernetinis saugumas: ES institucijos sustiprino bendradarbiavimą kovai su kibernetiniais išpuoliais“, 2017 m.

CERT-EU labai glaudžiai bendradarbiauja su ES institucijų vidaus IT saugumo tarnybomis ir palaiko ryšius su kompiuterinių incidentų tyrimo tarnybomis ir IT saugumo bendrovėmis valstybėse narėse ir kitose šalyse – keičiasi informacija apie grėsmes ir apie tai, kaip su jomis kovoti. Ji taip pat glaudžiai bendradarbiauja su atitinkamomis NATO tarnybomis.

2018 m. balandžio 16 d. Taryba priėmė išvadas dėl kibernetinės kenkimo veiklos,[58] šiose išvadose pabrėžta, kad svarbu užtikrinti visuotinę, atvirą, laisvą, stabilią ir saugią kibernetinę erdvę, kurioje visapusiškai galiotų žmogaus teisės ir pagrindinės laisvės bei teisinės valstybės principas.

Taryba pareiškė esanti labai susirūpinusi dėl to, kad padidėjo trečiųjų valstybių ir nevalstybinių subjektų gebėjimai ir noras siekti savo tikslų vykdant kibernetinę kenkimo veiklą. ES toliau stiprins savo kovos su kibernetinėmis grėsmėmis pajėgumus.

2019 m. Taryba priėmė reglamentą, dar žinomą kaip kibernetinio saugumo aktas, kuriuo:

- Sukuriama ES masto sertifikavimo sistemų sistema.ES masto kibernetinio saugumo sertifikavimas greitai bus teikiamas prie interneto prijungtiems prietaisams; tai leis vartotojams priimti išsamesne informacija pagrįstus sprendimus, o įmonėms bus lengviau parduoti savo išmaniuosius produktus visoje Europoje.

- Įsteigiama ES kibernetinio saugumo agentūra.Nuo įsteigimo 2004 m. Graikijoje įsikūrusi ENISA dirba ES tinklų ir informacijos saugumo srityje. Naujosiomis taisyklėmis šiai agentūrai bus suteikti nuolatiniai įgaliojimai ir apibrėžtas jos, kaip ES kibernetinio saugumo agentūros, vaidmuo. ENISA bus pavestos naujos užduotys padėti valstybėms narėms, ES institucijoms ir kitiems suinteresuotiesiems subjektams kibernetinių klausimų srityje. Ji rems ES politiką kibernetinio saugumo sertifikavimo srityje, pavyzdžiui, atlikdama pagrindinį vaidmenį rengiant sertifikavimo schemas. Ji propaguos naujos sertifikavimo sistemos diegimą, pavyzdžiui, sukurdama informuoti apie sertifikatus skirtą interneto svetainę. Taip pat agentūra reguliariai rengs ES lygio kibernetinio saugumo pratybas, įskaitant kas dvejus metus rengiamas stambaus masto visuotines pratybas.[59]

ES kibernetinė parengtis yra ypač svarbi tiek bendrajai skaitmeninei rinkai, tiek saugumo ir gynybos sąjungai. Privalu stiprinti Europos kibernetinį saugumą ir šalinti tiek civiliniams, tiek kariniams objektams kylančias grėsmes.

Vertinant kibernetines grėsmes yra susiduriama su keletu sunkumų. Pirmiausia, yra per mažai informacijos ir duomenų, kurie parodytų, kad išpuolis iš tiesų vyksta. Antra, beveik neįmanoma nustatyta, kas yra atsakingas už vykdomą ataką. Trečia, išteklių trūkumas, kurie padėtų tinkamai apsisaugoti nuo atakų ir grąžintų susiklosčiusią į prieš tai buvusią padėtį. Šalys turi galimybę prisiimti atsakomybę už įvykdytas atakas, tačiau tai gali iššaukti užpultos valstybės atsaką

[58]Europos Vadovų Taryba, pranešimas spaudai „Kibernetinė kenkimo veikla. Taryba priėmė išvadas“, 2018 m.
[59]Europos Vadovų Taryba, Europos Sąjungos Taryba, „Kibernetinis saugumas Europoje. Griežtesnės taisyklės ir geresnė apsauga“, https://www.consilium.europa.eu/lt/policies/cybersecurity/.

– kerštą. Kerštas galėtų būti apibūdintas, kaip savisauga jei ji būtų proporcinga įvykusiai atakai ir vykdoma tik atsiradus būtinybei. Tačiau į kibernetines grėsmes, kibernetines atakas ir net įprastus ginklus vis dar reaguojama labai santūriai.

3.2 Kibernetinis saugumas NATO darbotvarkėje

Kibernetinės grėsmės NATO saugumui tampa vis dažnesnės, sudėtingesnės ir darančios daug žalos. NATO tęsia prisitaikymą prie besikeičiančių kibernetinių grėsmių ir ieško būdų jų išvengti. NATO ir jos sąjungininkės vykdydamos pagrindines Aljanso užduotis – kolektyvinę gynybą, krizių valdymą ir bendradarbiavimo saugumą, pasikliauja stipriomis ir atspariomis kibernetinėmis priemonėmis. Aljansas turi būti pasirengęs ginti savo tinklus ir operacijas nuo didėjančių kibernetinių grėsmių ir atakų, su kuriomis susiduria, ir kurios tampa vis sudėtingesnės. Pabrėžiama, kad kibernetinė gynyba yra pagrindinė NATO kolektyvinės gynybos užduotis, o pagrindinis kibernetinės gynybos dėmesys yra skirtas kuo geriau apsaugoti savo elektroninius tinklus ir sustiprinti viso Aljanso atsparumą.

1994 m. po kibernetinių išpuolių Kosovo operacijų metu, NATO pradėjo pripažinti kibernetinę erdvę kaip kolektyvinės gynybos dalį. Tuo metu NATO informacinę erdvę atakavo serbų, kinų ir rusų įsilaužėliai, dėl to keletas vyriausybinių ir NATO tinklapių buvo neprieinami, nors pasisavinti svarbios informacijos įsilaužėliams ir nepavyko, tačiau NATO į šiuos išpuolius pažiūrėjo rimtai.[60] 2002 m. Prahoje buvo priimta kibernetinės gynybos programa. Svarbiausias programos tikslas buvo sukurti NATO reagavimo į kibernetinius incidentus pajėgumus.[61] Negana to 2006 m. NATO išreiškė norą plėtoti kibernetinio tinklo pajėgumus patikimai, saugiai ir nedelsiant dalytis informacija, duomenimis, žvalgybos informacija, kartu gerinant NATO pagrindinių informacinių sistemų apsaugą nuo kibernetinių išpuolių.[62]Nuo to laiko kibernetinio saugumo politika tapo vis svarbesniu NATO viršūnių susitikimų darbotvarkės objektu. 2008 m. buvo priimta pirmoji NATO kibernetinės gynybos politika.[63]Tais pačiai metais, Bukarešto viršūnių susitikime buvo pabrėžta būtinybė NATO ir šalims narėms apsaugoti pagrindines savo informacines sistemas. Taip pat Aljanso vadovybė įsteigė dvi pagrindines kibernetinės gynybos institucijas: Kibernetinės gynybos valdymo tarnybą ir Kibernetinės gynybos kompetencijos centrą, siekiant padėti valstybėms narėms tobulinti (koordinuoti ir peržiūrėti) savo nacionalinius kibernetinės gynybos pajėgumus ir vykdyti tinkamą kibernetinio saugumo rizikos valdymą.[64]Visų pirma, NATO reikia sukurti nuoseklią kibernetinio saugumo politiką siekiant išspręsti iškylančias grėsmes. 2010 m. buvo priimta NATO strateginė koncepcija, kurioje kibernetinio saugumo klausimai pripažinti kaip

[60]Justine Marie Chauvin, „NATO Cyber Defence Policy“, 2014 m. 44 p.
[61]J. Healey, Leendert van Bochoven, „NATO‘s Cyber Capabilities: Yesterday, Today, and Tomorrow“, 2011 m. 1 p.
[62]NATO, Riga Summit Declaration, 2006 m.
[63]Laura Brent, „NATO‘s role in cyberspace“, 2019 m.
[64]J. Healey, Leendert van Bochoven, „NATO‘s Cyber Capabilities: Yesterday, Today, and Tomorrow“, 2011 m. 2 p.

vienais svarbiausių kylančių saugumo iššūkių, ši koncepcija suteikė NATO platesnius įgaliojimus kas leido šiuos iššūkius spęsti sistemingiau.[65] Tais pačiais metais buvo pritarta Generalinio sekretoriaus siūlymui įsteigti kylančių saugumo iššūkių skyrių (ESCD), siekiant spręsti netradicinės rizikos ir iššūkių įvairovę. Šis skyrius susideda iš šešių skyrių ir vieno direktorato (Kovos su terorizmu skyrius, Kibernetinės gynybos skyrius, Energetinio saugumo skyrius, Masinio naikinimo ginklų neplatinimo skyrius, Strateginės analizės skyrius, Ekonomikos ir saugumo vertinimo skyrius ir Branduolinės politikos direktoratas).[66]

2011 m. buvo patvirtinta antroji NATO kibernetinės gynybos politika, koncepcija ir veiksmų planas, kurioje išdėstyta koordinuota kibernetinės gynybos vizija ir susijusių veiksmų planas jai įgyvendinti, kol kas tai yra pats svarbiausias Aljanso žingsnis kibernetinio saugumo srityje.[67] Šios politikos tikslai yra:

- integruoti kibernetinę gynybą į NATO planavimo procesus siekiant užtikrinti kolektyvinę gynybą ir krizių valdymą;
- kibernetinio turto apsauga ir gynyba;
- plėtoti patikimus kibernetinės gynybos pajėgumus ir centralizuoti NATO tinklų apsaugą;
- parengti būtiniausius nacionalinių tinklų kibernetinės gynybos reikalavimus;
- teikti pagalbą sąjungininkams siekiant minimalaus kibernetinės gynybos lygio ir sumažinti nacionalinių ypatingos svarbos infrastruktūros objektų pažeidžiamumą;
- bendradarbiauti su partneriais, tarptautinėmis organizacijomis, privačiu sektoriumi ir akademine bendruomene.[68]

2016 m. sąjungininkės dar kartą patvirtino NATO gynybinius įgaliojimus ir kibernetinę erdvę pripažino operacijų sritimi, kurioje NATO privalo gintis taip pat efektyviai kaip tai daro ore, sausumoje ir jūroje.[69] Siekiant kuo geriau užtikrinti Aljanso kibernetinį saugumą, sąjungininkės yra įpareigotos gerinti dalijimąsi informacija ir teikti visokeriopą pagalbą siekiant užkirsti kelią kibernetinėms atakoms, sušvelninti jas, o įvykus tokiai atakai, padėti atsigauti po jų.[70]

2019 m. siekiant dar labiau apsaugoti kibernetinę erdvę, sąjungininkai patvirtino NATO vadovą, kuriame išdėstytos priemonės, skirtos dar labiau sustiprinti NATO sugebėjimus reaguoti į reikšmingą, kenkėjišką elektroninę veiklą.

[65]Michael Rühle, „NATO and Emerging Security Challenges: Beyond the Deterrence Paradigm," American ForeignPolicy Interests: The Journal of the National Committee on American Foreign Policy 33, 2011 m. 281 p.
[66]NATO, EmergingSecurityChallengesDivision, https://esc.hq.nato.int/default.aspx
[67]J. Healey, Leendert van Bochoven, „NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow", 2011 m. 3 p.
[68]NATO, „Defending the networks. The NATO Policy on Cyber Defence", 2011 m. https://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf
[69]NATO, Warsaw Summit Communique, 2016 m. https://www.nato.int/cps/en/natohq/official_texts_133169.htm
[70]Laura Brent, „NATO's role in cyberspace", 2019 m.

Politiniu lygmeniu Aljansas toliau stiprina savo kibernetinį saugumą, gynybą ir atgrasymo strategijas, nuolat atnaujina veiksmų planus su konkrečiais tikslais ir terminais.

Kai ginkluotosios pajėgos, įskaitant priešiškai nusiteikusiose valstybėse, didina savo kibernetinius gebėjimus, NATO ir jos valstybės narės taip pat turi imtis atitinkamų veiksmų, parengti strategijas ir kibernetinio saugumo politiką kovai su grėsme, kovai prieš sudėtingus kibernetinius išpuolius. NATO kovai su kibernetinėmis atakomis remiasi bendrosiomis strategijomis, kuriomis vadovaujasi kovojant ir su kitais išpuoliais: atgrasymas neigimu ir atgrasymas bausmėmis. Atgrasymo neigimu strategijomis siekiama atgrasyti veiksmais, įtikinant priešininką, kad tai neatneš jam norimos naudos. Kitaip tariant besiginantis turi padaryti taip, kad toks puolimas atrodytų beprasmis, užpuolimas turėtų žlugti, arba bent nepadaryti žalos besiginančiai pusei.[71] Tokie kibernetiniai atgrasymai yra grindžiami stipriu kibernetiniu saugumu ir gynyba, kuri visų pirma yra nacionalinė atsakomybė.

Nors kibernetinis saugumas ir gynybos galimybės ir toliau tobulėja, tačiau dauguma ekspertų teigia, kad nusikaltimų kibernetinėje erdvėje nemažės. Turint pakankamai laiko, gerus įgūdžius ir išteklius, kibernetiniai nusikaltėliai gali vykdyti kibernetines atakas, ieškant tikslinės sistemos silpnųjų vietų, taip įgyjant prieigą prie jos ir gaunant norimos naudos. Būtent dėl šios priežasties Aljansas naudoja atgrasymo bausmėmis strategiją. Kitaip tariant, turima stengtis užkirsti kelią kibernetinėms atakoms, grasinant užpuolikams, kad tokia ataka atneš finansinių nuostolių, ir ekonominiais paskaičiavimais geriausias pasirinkimas yra apskritai nepulti.

NATO kibernetinėje strategijoje išskiriami šie būdai kaip sustiprinti kibernetinį saugumą ir gynybą:[72]

- įgyvendinti pagrindines kibernetinio saugumo priemones;
- padidinti situacijos suvokimą;
- paskatinti informacijos dalijasi;
- geresnės kibernetinių atakų aptikimo ir stebėjimo įrangos diegimas;
- investavimas į naujas technologijas;
- nuolatiniai darbuotojų mokymai;
- rengti kibernetinius mokymus ir pratybas;
- vykdyti reguliarų kibernetinį auditą;
- neskelbtinų failų šifravimas;

Taip pat NATO akcentuoja, kad vis glaudžiau susijusiame pasaulyje yra svarbus stiprus partnerių palaikymas tai ypač taikoma kibernetiniam saugumui ir gynybai. Todėl NATO bendradarbiauja su įvairiais partneriais, įskaitant pramonę, akademinę bendruomenę, šalis partneres

[71]J. S. Nye Jr., „DeterrenceandDissuasioninCyberspace“, 2017 m. 46 p.
[72]Susan DAVIS, NATO in the cyber age: strengthening security&defence, stabilising deterrence. 2019 m. 5 p.

ir kitas tarptautines organizacijas. Šioje srityje didelį vaidmenį vaidina pramonė, nes ji gali pateikti techninius sprendimus ir naujoves, investuoti į kibernetinio saugumo sprendimus ir saugoti išsamią informaciją apie kibernetines grėsmes. Be to, pramonė valdo arba naudoja didelę dalį sąjungininkų informacinių sistemų. NATO kibernetinio saugumo partneryste siekiama palengvinti keitimąsi informacija apie kibernetines grėsmes ir gerinti sąjungininkų galimybes aptikti, užkirsti kelią kibernetiniams incidentams ir atitinkamai į juos reaguoti. Ši partnerystė apima keletą prioritetinių sričių: tiekimo grandinės valdymas, geriausia praktika, sąmoningumo didinimas, švietimas, mokymai ir pratybos, naujovės.[73]

Kibernetinis saugumas ir gynyba labai dažnai yra NATO bendradarbiavimo komponentas su šalimis partnerėmis. Nors NATO bendradarbiauja su Europos saugumo ir bendradarbiavimo organizacija (ESBO) ir Jungtinėmis Tautomis, tačiau stipriausia tarptautinė partnerystė yra su Europos Sąjunga. Koordinavimas ir bendradarbiavimas kibernetinio saugumo ir gynybos srityje yra pagrindinė NATO ir ES strategijos sritis. Ši elektroninė partnerystė įgavo naują pagreitį 2016 m. kai Europos vadovų Tarybos pirmininkas, Europos Komisijos pirmininkas ir NATO generalinis sekretorius nusprendė išplėsti kibernetinį saugumą ir gynybą įtraukiant tai į misijas ir operacijas, pratybas, švietimą ir mokymąsi. Šiuo metu NATO ir ES įgyvendina 74 bendradarbiavimo pasiūlymus, o kibernetinis saugumas ir gynyba yra pagrindinis šių pasiūlymų pagrindas. NATO ir ES bendradarbiavimas apima šias konkrečias sritis:

- kibernetinės gynybos integraciją į planavimą;
- elektroninių mokslinių tyrimų ir technologinių naujovių skatinimas;
- dalintis gerąją krizių valdymo ir reagavimo patirtimi;
- grėsmių ir kenkėjiškų programų analizė;
- stiprinti bendradarbiavimą mokymų ir pratybų metu.[74]

2018 m. NATO ir ES ataskaitoje buvo pateikti pasiūlymai kaip pagerinti kibernetinę gynybą: keitimasis informacija, ypač koncepcijų, doktrinų ir teisės aktų klausimais, švietimo ir mokymo kursai, grėsmės rodiklių analizė, spartus grėsmės aptikimas ir vertinimas, krizių valdymas.[75]

Kalbant apie mokymus, 2017 m. ES kibernetinio saugumo specialistai pirmą kartą dalyvavo kibernetinio saugumo mokymuose „Cyber Coalition“, o 2018 m. „Locked Shields“. NATO krizių valdymo pratybos 2017 m. vyko lygiagrečiai su ES kibernetinio saugumo pratybomis. Tai leido abejoms organizacijoms įvertinti savo tarpusavio suderinamumą iškilus galimai grėsmei, o ypač reagavimą į kibernetines ir hibridines grėsmes.2019 m. „Locked Shields“ pristatė naujus

[73]DAVIS, Nato in the cyberage: strengthening security&defence, stabilising deterrence. 2019 m. 8 p.
[74]Ten pat, 9 p.
[75]Ten pat, 11 p.

iššūkius, technologijas ir specializuotas sistemas. Didžiausias dėmesys skiriamas realiems scenarijams, pažangiausioms technologijoms ir sudėtingų kibernetinių įvykių modeliavimui, įskaitant strateginių sprendimų priėmimo, teisinius ir komunikacijos aspektus.[76]

Jeigu pažiūrėtume iš šalies, kibernetinių atakų skaičiai ir grėsmės tikrai atrodo bauginančiai. Tačiau NATO stiprina kibernetinį saugumą, gynybą ir atgrasymo priemones. Nereikėtų pamiršti, kad kiekvienas sąjungininkas turi išlaikyti ir tobulinti tiek individualius, tiek kolektyvinius ryšius siekiant užkirsti kelią kibernetinėms grėsmėms. Šalys narės turi prisiimti atsakomybę, užtikrinant kibernetinį saugumą nacionaliniu lygmeniu vadovaujantis NATO gynybos planavimo procesu. NATO ir jos sąjungininkai ėmėsi reikšmingų strateginių, operacinių ir techninių žingsnių siekdami kovoti su kenkėjiška elektronine veikla. Nepaisant to, 2018 m. Briuselyje vykusiame aukščiausiojo lygio susitikime, sąjungininkų lyderiai perspėjo, kad kibernetinės grėsmės Aljanso saugumui tampa vis dažnesnės, sudėtingesnės, visa griaunančios ir priverstinės. Kibernetinių grėsmių pobūdis reikalauja, kad Aljansas nuolat vertintų ar tinkamai yra į jas reaguojama. Aiškiausias NATO, kaip Aljanso, tikslas kibernetinėje erdvėje buvo išsakytas Varšuvoje ir pakartotas Briuselyje: „Mes turime sugebėti veikti taip efektyviai elektroninėje erdvėje, kaip veikiame ore, sausumoje ir jūroje, kad sustiprintume ir palaikytume NATO bendroje Aljanso atgrasymo ir gynybos politikoje“.[77]

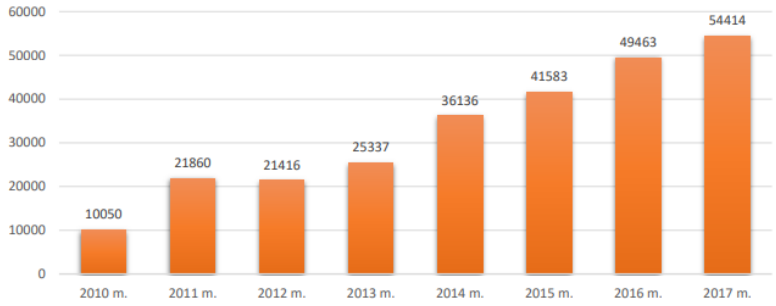
[76]CCDCOE, „Loecked Shields“, https://ccdcoe.org/exercises/locked-shields/
[77]NATO, Warsaw Summit Communique, 2016 m. https://www.nato.int/cps/en/natohq/official_texts_133169.htm

4. GRĖSMIŲ KIBERNETINIAM SAUGUMUI VERTINIMAS: LIETUVA

4.1 Kibernetinių incidentų ir kibernetinio šnipinėjimo analizė ir vertinimas

Lietuvoje vis daugiau visuomenės socialinių santykių perkeliama į virtualiąją erdvę – aktyviai panaudojami elektroniniai ryšiai ne tik informacijai gauti ar siųsti, bet ir elektroninės bankininkystės, elektroninio verslo ir elektroninės valdžios galimybėms realizuoti. Deja, šie pokyčiai skatina ir neteisėtas veikas elektroninėje erdvėje.

2017 metais CERT-LT ištyrė 54414 incidentų pagal pranešimus, gautus iš Lietuvos elektroninių ryšių paslaugų teikėjų, užsienio CERT tarnybų, atliekančių tarptautinius incidentų tyrimus, ir iš Lietuvos interneto naudotojų. Palyginti su 2016 metais (49463 atvejai), kibernetinių incidentų užregistruota dešimtadaliu daugiau. Iš žemiau pateiktos diagramos matome, kad kibernetinių incidentų skaičius CERT-LT duomenimis nuo 2015 m. tik augo.[78]



1 Pav. CERT-LT 2010-2017 m. apdorotų incidentų skaičius

Nacionalinio kibernetinio saugumo centro duomenimis, 2018 m. Lietuvoje buvo užregistruota 53183 kibernetinio saugumo incidentai, iš jų 29747 įrenginių saugumo spragos ir 10059 įsilaužimai į ryšių ir informacines sistemas ir jų užvaldymas.[79] Svarbu pabrėžti, kad, lyginant su ankstesniais metais, incidentai tapo sudėtingesni bei penktadaliu (21 proc.) didėjo įrenginių, turinčių saugumo spragų skaičius. Su kibernetinio saugumo iššūkiais susiduria tiek viešojo, tiek privataus sektoriaus subjektai. NKSC nustatė, kad 52 proc. interneto svetainių Lietuvoje yra pažeidžiamos, o Lietuvos banko 2018 m. atlikta finansų įstaigų apklausa atskleidė, kad Lietuvos finansų sistemai didžiausią riziką kelia kibernetinių išpuolių galimas poveikis.Nacionalinis kibernetinio saugumo centras 2018 m. užfiksavo 31 DDoS (daugybės užklausų siuntimas iš vieno, kelių ar daug įvairių interneto taškų į informacinius išteklius (interneto svetaines, registrus, valdymo ir vadovavimo tinklus). Kai užklausų srautas suintensyvėja, paslauga (interneto svetainė) teikiama su pertrūkiais arba tampa visiškai neprieinama.) kibernetinį incidentą.[80] Pagal svarbą, 20 iš jų buvo priskiriami vidutinei kategorijai. DDoS atakomis buvo taikomasi į Vidaus reikalų ministerijos, VĮ

[78]RRT, „2017 m. CERT-LT apdorojo 54414 kibernetinių incidentų“, 2018 m.
[79]G. Žintelis, NKSC 2018 metų ataskaitos išvados ir rekomendacijos, 2018 m. 4 p.
[80]NKSC, Nacionalinio kibernetinio saugumo būklės ataskaita, 2018 m. 36 p.

„Registrų centro", taip pat Lietuvos Respublikos Seimo ryšių ir informacinių sistemų teikiamų paslaugų prieinamumą.Pažymėtina, kad įrenginių, turinčių saugumo spragas, skaičius išaugo. Tokie įrenginiai gali būti užvaldyti ir įtraukti į Botnet (užvaldytų kompiuterių tinklai)tinklą, t. y. jais gali būti pasinaudota vykdant DDoS atakas. 2018 m. NKSC užfiksavo 28630 įrenginių, turinčių saugumo spragų. Palyginti su ankstesniais metais, ši tendencija nuo 2015 m. kasmet padidėjo penktadaliu (atitinkamai 2015 m. užfiksuota 18427, 2016 m. – 20490, o 2017 m. – 24612 įrenginių). Įrenginių, turinčių saugumo spragų, skaičiaus augimas susijęs su sparčiai populiarėjančiais išmaniaisiais telefonais, išmaniaisiais televizoriais ir pan.[81]

2018 m. Lietuvoje rezonansą kėlė hibridiniai incidentai, kai kibernetinės atakos buvo priderintos prie melagingų naujienų. 2018 m. vykę rezonansiniai kibernetiniai incidentai buvo susiję su ryšių ir informacinės sistemos (toliau – RIS) pažeidžiamumu atskleidimu, įdiegta kenkimo programine įranga, užvaldytais įrenginiais ir su RIS vykdytais kenkėjiškais veiksmais.[82] NKSC užfiksavo didelės reikšmės kibernetinius incidentus, kai pas kibernetinio saugumo subjektus buvo aptikta ilgą laiką veikusi pažangi šnipinėjimo įranga, sietina su užsienio valstybių žvalgybine veikla. Visuomenėje dažniausiai rezonansą kėlė kibernetiniai incidentai, savo pobūdžiu susiję su informacinėmis atakomis ir žinomų pažeidžiamumų išnaudojimu, nors dėl riboto poveikio pagal savo reikšmingumą nepriskirtini didelio poveikio arba pavojingiems kibernetiniams incidentams. Svarbus ir rezonansą nacionaliniu mastu sukėlęs kibernetinis incidentas 2018 m. susijęs su informacinės sistemos „e-sveikata" pažeidžiamumo atskleidimu. Asmuo, pasinaudojęs programavimo klaida, viešai atskleidė pažeidžiamumą ir gavo prieigą prie asmens duomenų. Šis incidentas iškėlė atsakingo informavimo problemą, kai apie pažeidžiamumus yra informuojamos ne atsakingos institucijos, o trečiosios šalys, kurios viešindamos informacinių sistemų pažeidžiamus ir (ar) jų išnaudojimo būdus gali sudaryti sąlygas piktavaliams prieiti prie RIS saugomų asmens duomenų. NKSC atkreipia dėmesį, kad aptikus saugumo spragą pirmiausia apie tai reikėtų pranešti sistemos valdytojui ir NKSC, nesistengti išnaudoti saugumo spragos pažeistoje sistemoje, nebandyti pakeisti duomenų ar kitaip ją paveikti, nenaudoti kibernetinio saugumo įrankių pažeidžiamumams išnaudoti.[83]

Kaip rodo incidentų statistika, Lietuvoje dvi didžiausios kibernetinio saugumo problemos yra kenkimo programinė įranga (kenkimo kodai) ir nesaugios informacinės sistemos, tarp jų ir interneto svetainės.[84] Minėtos saugumo problemos papildo viena kitą ir didina potencialią riziką interneto naudotojams. Vienais atvejais užvaldomos nesaugios interneto svetainės (turinio valdymo sistemos) ir į jas įkeliamas kenkimo kodas, skirtas kenkėjiškai programinei įrangai platinti.

[81]NKSC, Nacionalinio kibernetinio saugumo būklės ataskaita, 2018 m. 36 p.
[82]A. Balčiūnas, „Saugumo ataskaita: kibernetinės atakos prieš Lietuvą tampa vis sudėtingesnės", 2019 m.
[83]NKSC, Nacionalinio kibernetinio saugumo būklės ataskaita, 2018 m. 20 p.
[84]Verslo žinios, „Kibernetinis saugumas: buvo ir chuliganizmo, ir šnipinėjimo ir išpuolių energetikoje", 2018 m.

Kitais atvejais į užvaldytą svetainę įkeliama speciali valdymo konsolė, kuri leidžia piktavaliui vykdyti įvairesnę kenkėjišką veiklą – be jau minėto kenkėjiškos programinės įrangos platinimo, taip pat galima skenuoti ir atakuoti tinklus bei informacines sistemas, rinkti informaciją, valdyti kitus užvaldytus įrenginius ir pan.[85]

Dar viena svarbi grėsmė nukreipta prieš Lietuvą yra kibernetinis šnipinėjimas. Kibernetinis šnipinėjimas prieš Lietuvos valstybės institucijas, šalies kritinės infrastruktūros objektus, politikus, privatųjį sektorių išlieka grėsme šalies nacionaliniam saugumui. Lietuvos institucijų automatizuoto duomenų apdorojimo (toliau – ADA) sistemose ir tinkluose aptinkamos kibernetinio šnipinėjimo programos nuolat tobulinamos ir atnaujinamos. 2018 m. Lietuvos kibernetinėje erdvėje buvo nustatyta kenkėjiška veikla, priskiriama tiek valstybiniams, tiek nevalstybiniams veikėjams. Pasaulinėje kibernetinėje erdvėje didelį susirūpinimą keliantis Kinijos industrinis šnipinėjimas, Šiaurės Korėjos ir Irano veiksmai Lietuvos informaciniuose tinkluose vertinami kaip nekryptinga ar net atsitiktinė veikla.[86] Didžiausią grėsmę Lietuvos kibernetinei erdvei kelia Rusijos žvalgybos ir saugumo tarnybos – jos vykdo žvalgybą, rengia IT sistemų trikdymą ir prisideda vykdant įtakos operacijas.

Rusijos kibernetinio šnipinėjimo grupuočių veikla nustatoma beveik visose pasaulio šalyse, tačiau pagrindinis dėmesys yra skiriamas NATO ir ES valstybėms bei kitiems Rusijai geopolitiniu požiūriu aktualiems regionams. Rusijos kibernetinė veikla tampa vienu iš pagrindinių įrankių Rusijos geopolitiniams tikslams siekti ne tik konflikto, bet ir taikos metu. Rusijos kibernetinė veikla naudojama kaip atgrasymo elementas prieš valstybes, su kuriomis konfliktuojama. Vykdydama priešišką veiklą kibernetinėje erdvėje, Rusija neriboja savęs nei geografiniu, nei taikinių reikšmingumo požiūriu, tikėdamasi išvengti atsakomybės. Iki šiol iš kibernetinių operacijų Rusijos gaunama nauda atsvėrė galimą Vakarų valstybių atsaką.

Antrojo operatyvinio departamento duomenimis Lietuvoje nuolat fiksuojama Rusijos žvalgybos ir saugumo tarnybų programišių vykdoma žvalgybos veikla, nukreipta prieš Lietuvos informacines sistemas. Kibernetinio šnipinėjimo operacijose prieš Lietuvą naudojami technologiškai itin pažangūs kibernetiniai įrankiai, neaptinkami įprastomis sistemų apsaugos priemonėmis, todėl ilgą laiką užkrėstuose tinkluose veikia nepastebimai. Lietuvoje kibernetinį šnipinėjimą aktyviausiai vykdo GRU grupuotė Sofacy/APT28 ir FSB grupuotė Agent.btz/Snake. Jų pagrindinės informacijos rinkimo sritys – politinė, karinė ir ekonominė.[87] Vykdydamos žvalgybos veiklą, grupuotės prasiskverbia ne tik į valstybinių institucijų, bet ir privačių organizacijų ar asmenų informacines sistemas. Perimti duomenys įprastai naudojami vykdant įtakos operacijas ir

[85]LR RRT, 2017 m. veiklos ataskaita, 25 p.
[86]Daniel R. Coats, „World wide threat assessment of the US intelligence community“, 2019 m. 5 p.
[87]AOTD prie KAM, Grėsmių nacionaliniam saugumui vertinimas, 2019 m. 36 p.

prasiskverbimus į labiau apsaugotas, jautrią informaciją apdorojančias arba su kritine šalies infrastruktūra susijusias sistemas.[88]

Nacionalinio kibernetinio saugumo duomenimis elektroninių tinklų žvalgyba susijusi su informacijos apie kibernetinio saugumo subjektų ar paprastų naudotojų ryšių ir informacinės sistemos rinkimu. Populiariausias būdas – interneto skenavimo įrankiais, ieškant aktyvių, internetu prieinamų, paslaugų ir su jomis susijusių prievadų. Tokio pobūdžio elektroninių ryšių tinklų žvalgyba nebūtinai reiškia, kad bus vykdoma kenkėjiška veikla, tačiau dažniausiai tai yra pirmas žingsnis siekiant identifikuoti pažeidžiamas ryšių ir informacinės sistemos vietas ir pagal jas pritaikyti kenksmingos programinės įrangos platinimą. Skenuojant yra surenkama informacija apie prie interneto prijungtus organizacijų įrenginius, jų tipus, įgalintas paslaugas, pažeidžiamumus ar neuždarytus prievadus. Surinkus šią informaciją yra planuojamos tolesnės kibernetinės atakos arba – pasinaudojus viešai prieinama informacija ir įrankiais – bandoma įsilaužti į organizacijų infrastruktūrą. 2018 m. labiausiai buvo žvalgomi energetikos, krašto apsaugos, valstybės valdymo ir finansų sektoriuose ypatingos svarbos paslaugas teikiantys kibernetinio saugumo subjektai.[89]

Valstybiniam sektoriui didžiausią grėsmę kibernetinėje erdvėje kels Rusija. Atsižvelgiant į plėtojamus Rusijos pajėgumus ir sėkmingas operacijas kibernetinėje erdvėje, vertinama, kad Rusijos aktyvumas kibernetinėje erdvėje didės. Lietuvos valstybinio sektoriaus IT sistemos išliks prioritetiniu kibernetinio šnipinėjimo taikiniu, tačiau bus taikomasi ir į privačią kritinę infrastruktūrą: telekomunikacijų įmones, pramonės objektuose įrengtas SCADA (kompiuterizuota, tinklais valdoma programuojama pramoninių procesų valdymo sistema) sistemas ir kitus valstybinės reikšmės privačius objektus. Siekiant diskredituoti valstybę, kibernetinės atakos gali būti vykdomos po kiekvieno Rusijai neparankaus Lietuvos politinio sprendimo, viešo politinio pareiškimo ar Lietuvoje vykstančio didelės reikšmės tarptautinio renginio metu. Pažymėtina, kad kibernetinio šnipinėjimo grėsmė didės valstybės politikams bei stambaus verslo atstovams. Panaudodamos kibernetinę erdvę, Rusijos žvalgybos tarnybos ir toliau organizuos kibernetinio šnipinėjimo bei informacines operacijas prieš Lietuvos politikus, valstybės tarnautojus ir privačius asmenis, taip siekdamos paveikti Lietuvos vykdomą vidaus ir užsienio politiką.[90]

Prognozuojama, kad panašių atakų skaičius nemažės, o kibernetinė erdvė išliks viena pagrindinių veiklos erdvių,vykdant tiek įvairius išpuolius prieš nacionaliniam saugumui svarbius kritinės infrastruktūros objektus, tiek kibernetinį šnipinėjimą, siekiant rinkti įvairius duomenis,stebėti ir valdyti virusu užkrėstus kompiuterius. Todėl kibernetinio saugumo stiprinimas turi išlikti vienus varbiausiu valstybės prioritetu.[91]

[88]AOTD prie KAM, Grėsmių nacionaliniam saugumui vertinimas, 2019 m. 36 p.
[89]NKSC, Nacionalinio kibernetinio saugumo būklės ataskaita, 2018 m. 10 p.
[90]AOTD prie KAM, Grėsmių nacionaliniam saugumui vertinimas, 2017 m. 28 p.
[91]P.Saudargas, „Kibernetinių atakų Lietuvoje atvejai ir kaip į juos reaguojama“, 2016 m. 29 p.

4.2 Grėsmių kibernetiniam saugumui užkardymo galimybės ir priemonės

2018 m. buvo patvirtinta pirmoji Lietuvoje Nacionalinė kibernetinio saugumo strategija – esminis dokumentas, kuriame, atsižvelgiant į aplinkos analizės išvadas, Lietuvos ir Europos Sąjungos teisės aktus, gerąją kitų šalių patirtį bei viešojo ir privataus sektorių atstovų pasiūlymus, buvo įtvirtinti viešojo ir privataus sektorių, Lietuvos mokslo ir studijų institucijų penkerių metų tikslai ir uždaviniai kibernetinio saugumo srityje. Įgyvendinant strategiją yra siekiama stiprinti valstybės kibernetinį saugumą ir kibernetinių gynybos pajėgumų plėtrą, užtikrinti nusikalstamų veikų prevenciją, užkardymą ir tyrimą, skatinti kibernetinio saugumo kultūrą ir inovacijų plėtrą, stiprinti glaudų viešojo ir privataus sektorių, tarptautinį bendradarbiavimą ir užtikrinti tarptautinių įsipareigojimų kibernetinio saugumo srityje vykdymą.[92]

Kibernetiniai incidentai vis dažniau pažeidžia ne tik viešąjį ir privatų sektorius, bet ir žiniasklaidos priemones, kurios vaidina svarbų vaidmenį kuriant saugią kibernetinę erdvę ir objektyviai informuojant Lietuvos gyventojus.[93] 2018 m. Krašto apsaugos ministerija kartu su NKSC ir didžiausiais Lietuvos naujienų portalais bei agentūromis pasirašė bendradarbiavimo susitarimą,[94] kurio pagrindinis tikslas – efektyvinti bendradarbiavimą kibernetinio saugumo srityje, stiprinti visuomenės informavimo priemonių kibernetinį saugumą ir atsparumą kibernetinėms grėsmėms. Įgyvendinant bendradarbiavimo susitarimo nuostatas, 2018 m. Lietuvos kariuomenės Gedimino štabo batalione buvo surengti kibernetinio saugumo mokymai žurnalistams, kurie mokėsi, kaip kritiškai vertinti kibernetinę erdvę, atpažinti kibernetines grėsmes ir spręsti kibernetinius incidentus.

Nuo 2018 m. Krašto apsaugos ministerijos iniciatyva ir JAV pagalba pradėti vykdyti Regioninio kibernetinio saugumo centro steigimo darbai.[95] Šio būsimo centro tikslas – didinti Lietuvos kibernetinį atsparumą, dirbant su partneriais stiprinti Lietuvos kibernetinės gynybos specialistų gebėjimą laiku atpažinti ir užkirsti kelią mūsų regione vykstantiems kibernetiniams incidentams.

Atsižvelgiant į esamą kibernetinio saugumo būklę visų pirma reikia stiprinti valstybės kibernetinį saugumą ir kibernetinių gynybos pajėgumų plėtrą. To galima pasiekti kuriant sisteminį požiūrį į kibernetinį saugumą ir prevencinę veiklą (tobulinti kibernetinio saugumo rizikos nustatymo, vertinimo ir prognozavimo būdus). Taip pat didinti kibernetinio saugumo politikos formavimo ir įgyvendinimo efektyvumą. Šis uždavinys gali būti įgyvendinamas tobulinant kibernetinio saugumo teisinį reguliavimą, parengiant standartizuotus kibernetinio saugumo

[92]Lietuvos Respublikos nacionalinio saugumo strategija, 2018 m.
[93]LRV, „Kibernetinio saugumo tarybą papildys atstovai iš švietimo, žiniasklaidos, energetikos ir savivaldos sektorių“, 2019 m.
[94]NKSC, „Krašto apsaugos ministerija ir žiniasklaidos priemonės bendradarbiaus kibernetinio saugumo srityje“, 2018 m.
[95]R. Karoblis, „Krašto apsaugos sistemos plėtros programos įgyvendinimas“, 2019 m.

reikalavimus ir skatinant kibernetinio saugumo subjektus jais vadovautis, taip pat atnaujinant kibernetinio saugumo rizikos vertinimo sistemą, įvertinti kibernetiniam saugumui reikalingų lėšų kontrolę, nustatant jų skyrimo ir naudojimo pirmumą. Kitas svarbus dalykas stiprinant kibernetinį saugumą yra dalyvavimas nacionalinėse ir tarptautinėse kibernetinio saugumo pratybose. Privalu skatinti periodiškai rengti kompleksines nacionalines kibernetinio saugumo pratybas, dalyvauti Europos Sąjungos, NATO ir kitų šalių organizuojamose pratybose siekiant įgauti naujos patirties ir pasidalinti turima, atliekant situacijų valdymo, incidentų vertinimo, informacijos dalijimosi ar kitus veiksmus.[96] Taip pat reikėtų plėtoti valstybės kibernetinės gynybos pajėgumus, užtikrinant efektyvią Lietuvos kariuomenės bendradarbiavimą su valstybės civiliniais pajėgumais, plėtoti kibernetinės gynybos pajėgumus teikiant pagalbą kitoms valstybėms ir savivaldybių institucijoms/įstaigoms.

Visų antra, būtina užtikrinti nusikalstamų veikų kibernetinėje erdvėje prevenciją, užkardymą ir tyrimą. Būtina plėtoti valstybės pajėgumus ir gebėjimus kovoti su nusikalstamomis veikomis kibernetinėje erdvėje. Tobulinti teisinę sistemą, stiprinti teisėsaugos institucijų profesinius gebėjimus tirti nusikalstamas veikas kibernetinėje erdvėje, kurti tobulesnes analizės sistemas, diegti pažangius veiklos metodus ir procedūras, techninius įrankius, skirtus kovai su nusikalstamomis veikomis kibernetinėje erdvėje. Taip pat reikia stiprinti nusikalstamų veikų kibernetinėje erdvėje prevenciją ir kontrolę.[97] To galima pasiekti propaguojant visuomenės savisaugos kultūrą ir atsakingą elgesį kibernetinėje erdvėje, tobulinti teisėsaugos institucijų kovos su nusikalstamomis veikomis kibernetinėje erdvėje funkcijų vykdymą ir užtikrinti operatyvesnį bendradarbiavimą tiriant šias nusikalstamas veikas, plėtoti teisėsaugos institucijų efektyvų bendradarbiavimą su mokslo ir studijų institucijomis, viešojo ir privataus sektoriaus atstovais bei visuomene.[98]

Dar vienas svarbus aspektas siekiant užtikrinti kibernetinį saugumą yra kibernetinio saugumo kultūros ir inovacijų plėtros skatinimas.[99] Kibernetiniai incidentai šiuolaikiniame pasaulyje yra neišvengiami, nuo jų negalima apsisaugoti net ir taikant visas esamas technines kibernetinio saugumo priemones, todėl viešojo ir privataus sektorių atstovai turi rūpintis savo darbuotojų kibernetinės kultūros kėlimu. Svarbu plėtoti mokslinius tyrimus ir didelę pridėtinę vertę kuriančias veiklas kibernetinio saugumo srityje. Valstybė turi sudaryti palankias sąlygas kurti pažangius gebėjimus plėtojančias kibernetinio saugumo iniciatyvas, skatinti kibernetinio saugumo rinkos augimą, kibernetinio saugumo paslaugų eksportą į užsienio rinkas, plėtojant finansinių technologijų kibernetinio saugumo sektorių ir atliekant mokslinius tyrimus. Taip pat reikia ugdyti kibernetinio saugumo įgūdžius ir kvalifikaciją. Norint tai įgyvendinti, viešojo ir privataus sektoriaus

[96]LRV, „Dėl Nacionalinės kibernetinio saugumo strategijos patvirtinimo“, 2018 m. 5 p.
[97]LRV, „Dėl kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinis veiklos planas“, 2019 m.
[98]M. K. Daly, „Lawen for cement has to ge tserious about cybercrime“, 2018 m.
[99]Eva Short, „What is cyber security culture, and why is it important in the workplace?“, 2018 m.

atstovams bei mokslo ir studijų institucijoms reikia formuoti kibernetinio saugumo kompetencijų standartus, plėtoti šios srities mokymų, akreditavimo ir sertifikavimo sistemas, orientuotas į darbo rinkos poreikius, pritraukti ir ugdyti talentus, kuriant kibernetinio saugumo mokymų ir testavimo aplinką, apmokant naujokus ir sudarant persikvalifikavimo galimybes, tobulinant asmenų kibernetinio saugumo žinias. Žinoma reikėtų skatinti viešojo ir privataus sektoriaus bei mokslo ir studijų institucijų bendradarbiavimą, kuriant kibernetinio augumo srities inovacijas, tai padėtų kurti technines priemones, metodus ar kitus išteklius, siekiant išspręsti kibernetinio saugumo problemas ar vykdyti kibernetinio saugumo užduotis.[100]

Taip pat reikėtų stiprinti glaudų viešojo ir privataus sektoriaus bendradarbiavimą. Šiuolaikinėse valstybėse, kuriose gerai išvystyta plačiajuosčio ryšio infrastruktūra, viešojo sektoriaus atstovai nebegali toliau vieni kovoti su pavojingais ar didelės reikšmės kibernetiniais incidentais, o ypatingos svarbos informacinės infrastruktūros valdytojai – neretai privataus sektoriaus atstovai – patys ne visada gali suvaldyti kibernetinius incidentus, dažnai peržengiančius jų organizacijos ribas. Taigi viešojo ir privataus sektorių bendradarbiavimas tampa būtina sąlyga visapusiškam kibernetiniam saugumui užtikrinti. Būtina gerinti viešojo ir privataus sektorių bendradarbiavimo koordinavimą. Norint to pasiekti, reikia kurti tvarų viešojo ir privataus sektorių bendradarbiavimo kibernetinio saugumo srityje modelį, nustatant atsakomybę ir pajėgumus stiprinant valstybės kibernetinį saugumą,[101] efektyvinti viešojo ir privataus sektorių atstovų keitimąsi aktualia informacija apie kibernetines grėsmes, įvykusius incidentus, išmoktas pamokas, plėtoti komunikacijos metodus. Taip pat derėtų skatinti viešojo ir privataus sektorių atstovus tikrinti kibernetinio saugumo būklę ir taisyti kibernetinio saugumo spragas.

Siekiant stiprinti nacionalinį kibernetinį saugumą privalu plėtoti tarptautinį, tarpvalstybinį ir Baltijos regiono šalių bendradarbiavimą kibernetinio saugumo srityje. To galima pasiekti dalyvaujant ES, NATO, Jungtinių Tautų, Europos saugumo ir bendradarbiavimo organizacijos, Baltijos regiono ir kitų tarptautinių organizacijų veikloje. Reikia stiprinti tarptautinius kibernetinio saugumo pajėgumus ir gebėjimus. Taip pat plėtoti dialogą su JAV – kibernetinės gynybos srityje, siekti JAV dalyvavimo Lietuvos kibernetinio saugumo užtikrinimo projektuose, tik plėtojant dvišalį Lietuvos ir JAV politinio ir techninio lygmens bendradarbiavimą kibernetinės gynybos ir saugumo srityje dar labiau sustiprinsime mūsų šalies kibernetinę gynybą ir saugumą.[102]

Kibernetinis saugumas išlieka jautrus nacionalinio ir tarptautinio saugumo aspektu. Tą lemia ir iš pirmo žvilgsnio elementarios aplinkybės: visų pirma, virtuali erdvė nėra suvokiama kaip ta, kurią įmanoma kontroliuoti, todėl didelė dalis kompanijų nėra linkusios bendradarbiauti su

[100]Global Cyber Security Capacity Centre, „Cyber security Capacity review. Republic of Lithuania“, 2017 m. 47 p.
[101]AgnijaTumkevič, „Tarptautinio bendradarbiavimo ir konflikto potencialas kibernetinėje erdvėje“, 2019 m. 106 p.
[102]LR Vyriausybė, Nacionalinė kibernetinio saugumo strategija, 2018 m. 2-10 p.

valstybinėmis institucijomis, įvykus atakai ar vykdant prevencines priemones.[103] Antra, net jei nusikaltimas yra užfiksuojamas, globalūs tinklai yra dinamiški bei aprėpiantys gausybę informacijos, tad atsekti kaltuosius tampa sudėtinga, o atsekus – teisiškai sudėtinga nuteisti. Trečia, yra nelengva apibrėžti, ypač pinigine išraiška, kokią realią žalą išpuolis padarė.Siekiant sumažinti žalos dydį, rekomenduojama su svarbia informacija dirbančioms institucijoms bei pareigūnams elektroninius laiškus rašyti tik tekstine forma, be pridedamų dokumentų ar internetinių nuorodų, taip pat raginami nesiųsti rinkmenų į valstybes, kurios nėra laikomos iki galo draugiškomis – Kiniją, Rusiją, Iraną ar Šiaurės Korėją.[104]

Kad galėtume reaguoti į esminius informacijos ir ryšių technologijų pokyčius, paspartinti informacinės visuomenės plėtrą, būtina iniciatyvi politika. Kad esama teisinė sistema netrukdytų technologijų pažangai, o atvirkščiai – prie jos prisidėtų, būtina pakeisti teisės aktus: jie turi atitikti susiklosčiusius visuomeninius santykius ir tinkamai apsaugoti paslaugų gavėjus, didinti jų pasitikėjimą informacinėmis technologijomis, skatinti naudotis pažangiomis ir saugiomis informacinėmis technologijomis. Taip pat labai svarbu, kad būtų užtikrinta visapusiška valstybės informacinių išteklių apsauga, nes nuo stabilaus informacinių sistemų darbo priklauso valstybės gebėjimas veikti ir teikti būtinas viešąsias paslaugas piliečiams.Siekiant kuo geriau užtikrinti kibernetinį saugumą atsakingos institucijos turėtų nustatyti kibernetiniam saugumui reikalingų lėšų skyrimo ir panaudojimo prioritetus, užtikrinti įstaigų konsultavimą ir informavimą kibernetinio saugumo klausimais, skatinti tarptautinį bendradarbiavimą ir informacijos dalijimąsi.[105]

4.3 Sąveikos su ES ir NATO aspektai

Kibernetinį saugumą Lietuvoje reglamentuoja platus spektras tarptautinių teisės aktų. 2001 m. ES pasirašė konvenciją dėl elektroninių nusikaltimų, 2002 m. priimta direktyva „Dėl privatumo ir elektroninių ryšių“.[106] 2013 m. priimtas bendras komunikatas Europos Parlamentui ir Tarybai „Europos Sąjungos kibernetinio saugumo strategija, atvira, saugi ir patikima kibernetinė erdvė“. 2016 m. buvo priimtas Bendrasis duomenų apsaugos reglamentas ir ES direktyva „dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti“.[107] 2017 m. pateiktas bendras komunikatas Europos Parlamentui ir Tarybai „Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas“.[108]2015 metų pabaigoje Europos Parlamente ir Ministrų Taryboje sutarta dėl pirmųjų ES lygmens taisyklių, kurios turės užtikrinti

[103]Linas Kojala, „Virtualios erdvės saugumas – iššūkis ir JAV ir Europai“, 2016 m.
[104]Linas Kojala, „Virtualios erdvės saugumas – iššūkis ir JAV ir Europai“, 2016 m.
[105]Valstybinio audito ataskaita, Kibernetinio saugumo aplinka Lietuvoje“, 2015 m. 7 p.
[106]Europos Parlamento ir Tarybos direktyva 2002/58/EB, „Direktyva dėl privatumo ir elektroninių ryšių“, 2002 m.
[107]Europos Parlamento ir Tarybos direktyva 2016/1148, „Dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti“, 2016 m.
[108]Bendras komunikatas Europos Parlamentui ir tarybai, „Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas“, 2017 m.

minimalius kibernetinio saugumo reikalavimus bankams, energetikos, vandens įmonėms, taip pat įpareigos privačias kompanijas pranešti atitinkamoms institucijoms apie bandymus įsilaužti. Tikimasi, jog tai paskatins ES šalių bendradarbiavimą, paspartins keitimąsi informacija bei gerųjų praktikų įgyvendinimą. Prie to prisidės ir valstybės narės, kurios direktyvos įgyvendinimui turės paskelbti nacionalinę Elektroninių ryšių tinklų ir informacijos saugumo strategiją, taip pat paskirti kompetentingą instituciją, kuri prižiūrės priimtų sprendimų įgyvendinimą.[109]

Siekiant sustiprinti Europos Sąjungos kibernetinio saugumo ir gynybos pajėgumus bei efektyviau suvaldyti kibernetinius incidentus, peržengiančius valstybių sienas, būtina bendradarbiauti su kitomis Europos Sąjungos šalimis. Lietuvos Respublikos Krašto apsaugos ministerija 2017 m. inicijavo Europos Sąjungos nuolatinio struktūrizuoto bendradarbiavimo (PESCO) projektą „Kibernetinės greitojo reagavimo pajėgos ir tarpusavio pagalba kibernetinio saugumo srityje“, kuris buvo pradėtas įgyvendinti 2018 m. vasario mėnesį. PESCO yra ES Lisabonos sutartyje numatytas instrumentas, skirtas gilinti bendradarbiavimą saugumo ir gynybos srityje toms ES valstybėms narėms, kurių kariniai pajėgumai atitinka aukštesnius kriterijus ir kurios tarpusavyje yra susaistytos didesniais įsipareigojimais.[110]Projekto tikslas – sujungti ir panaudoti valstybių narių kibernetinės gynybos pajėgumus, žinias ir kompetencijas. Šešios šalys narės 2018 m., Europos Sąjungos užsienio reikalų tarybos susitikime Liuksemburge, pasirašė „Kibernetinio greitojo reagavimo pajėgų ir tarpusavio pagalbos kibernetinio saugumo srityje susitarimo memorandumą“. Prie pasirašiusiųjų – Lietuvos, Estijos, Ispanijos, Kroatijos, Olandijos ir Rumunijos – 2018 m. prisijungė ir Lenkija. Memorandumu šalys išreiškė politinę valią siekti glaudesnio bendradarbiavimo pagal projektą.[111]

2019 m. Amsterdame buvo rengiama Lietuvos vadovaujamo Europos Sąjungos kibernetinių greitojo reagavimo pajėgų ir tarpusavio pagalbos kibernetinio saugumo srityje projekto metinė konferencija. Lietuvos Krašto apsaugos viceministras teigia, kad „per pastaruosius metus kartu su projekto dalyviais ir partneriais pasiekėme didelę pažangą bendrų ES kibernetinių pajėgų sukūrimo kelyje. Tai tik patvirtina, kad galime praktiškai apjungti pajėgas kovai su grėsmėmis kibernetinėje erdvėje ir sustiprinti kolektyvinę gynybą šioje dimensijoje“. Vystant ES PESCO projektą per 2018 m. septynios ES šalys narės jau pasirašė ketinimų protokolą, įpareigojantį kurti bendras kibernetines pajėgas, o dar bent kelios šalys narės yra išreiškusios norą prisijungti ateityje. Paruošta teisinė bazė tokių ES kibernetinių pajėgų veikimui, nustatytos rolės ir procedūros, kurios buvo patikrintos per Lietuvoje vykusias kibernetinio saugumo pratybas „Kibernetinis skydas“. Pratybose dalyvavo ES šalių narių kibernetinio

[109]Europos Parlamento ir Tarybos direktyva 2018/1972, Europos elektroninių ryšių kodeksas, 2018 m. 16 p.
[110]LR KAM, Nuolatinis struktūrizuotas bendradarbiavimas (PESCO), 2017 m.
[111]Nacionalinio kibernetinio saugumo centras prie KAM, Nacionalinio kibernetinio saugumo būklės ataskaita, 2018 m. 48 p.

saugumo padalinių vadovai bei pirmoji ES kibernetinė greitojo reagavimo komanda, kurią metų trukmės rotacijai iki 2020 m. skiria Nyderlandai. Lietuvos, dar 2017 metais pasiūlyta iniciatyva, siekiama sukurti rotuojamas ES Kibernetines greitojo reagavimo komandas, kurias sudarytų projekte dalyvaujančių šalių kibernetinių incidentų tyrimų ir kitų saugumą užtikrinančių institucijų specialistai.Kibernetinio greitojo reagavimo komandos padės viena kitai užtikrinti aukštesnį kibernetinio atsparumo lygį ir bendrai reaguos į kibernetinius incidentus. Iš skirtingų Europos Sąjungos šalių kibernetinių ekspertų sudarytos komandos keisis, budės kas pusmetį. Komandos taip pat galės padėti kitoms valstybėms narėms ir Europos Sąjungos institucijoms, bendroms saugumo ir gynybos politikos operacijoms ir šalims partnerėms.[112]

Pagal 2016 m. NATO viršūnių susitikimo Varšuvoje priimtą sprendimą dėl kibernetinės erdvės pripažinimo penktuoju kariavimo domenu Lietuvos kariuomenė tapo pagrindiniu Lietuvos Respublikos kibernetinės erdvės gynybos subjektu. Kibernetinės gynybos stiprinimas siekiant apsisaugoti nuo besivystančių karinių kibernetinių grėsmių ir efektyvus kibernetinių incidentų valdymas yra viena iš būtinų sąlygų užtikrinant gyvybinius ir pirmaeilius valstybės nacionalinio saugumo interesus. Įgyvendinant Lietuvos kariuomenei keliamus uždavinius, bus plėtojami nacionaliniai kibernetinės gynybos pajėgumai, užtikrinantys Lietuvos kariuomenės sąveiką su valstybės civiliniais pajėgumais, taip pat Lietuvos kariuomenės gebėjimai užtikrinti patikimą agresorių atgrasymą kibernetinėje erdvėje, o nepavykus atgrasyti – savarankiškai ir kartu su sąjungininkais ginti Lietuvos Respubliką karinėmis kibernetinio saugumo priemonėmis.[113]

Dėl aukštos kompetencijos specialistų bendradarbiavimo ir keitimosi naudinga informacija bei tarptautinio bendradarbiavimo, galima būtų pabrėžti, kad 2010 m. Krašto apsaugos ministerija ir NATO Kibernetinės gynybos valdymo agentūra pasirašė dvišalį susitarimą dėl bendradarbiavimo kibernetinės gynybos srityje. Šiuo susitarimu siekiama pagerinti nacionalinių kibernetinės gynybos pajėgumų vystymą, sustiprinti bendradarbiavimą tarp Krašto apsaugos ministerijos ir NATO kibernetinės gynybos valdymo agentūros ir pagerinti kibernetinių atakų prognozavimo, aptikimo ir atsako į jas pajėgumus. Susitarime taip pat numatoma, kad, kibernetinės atakos atveju, Krašto apsaugos ministerija gali kreiptis į NATO Kibernetinės gynybos valdymo agentūrą prašydama atsiųsti NATO greitojo reagavimo kibernetinės gynybos specialistų komandą. Lietuva dalyvauja NATO Bendros kibernetinės gynybos kompetencijos centro, kuris įsikūręs Estijoje, veikloje. Šio centro veikloje taip pat dalyvauja Estija, Latvija, Lenkija, Vokietija, Italija, Vengrija, Slovakija, Ispanija, Nyderlandai ir JAV.[114]

Svarbu gerinti kibernetinio saugumo specialistų kompetenciją – nuolat savo gebėjimus išbandyti praktiškai. Dėl šios priežasties kibernetinio saugumo subjektai ir NKSC nuolat dalyvauja

[112]NKSC, Nacionalinio kibernetinio saugumo būklės ataskaita, 2018 m. 48 p.
[113]LR Vyriausybė, Nacionalinė kibernetinio saugumo strategija, 2018 m. 5 p.
[114]LR KAM, Kibernetinė gynyba ir energetinis saugumas, 2014 m.

tarptautinėse kibernetinio saugumo pratybose, tokiose kaip „Locked Shields 2018"[115], „Cyber Europe2018"[116] ir „Cyber Coalition 2018".[117] Pažymėtina, kad praėjusiais metais visose iš jų buvo imituojamos kibernetinės atakos prieš ypatingos svarbos infrastruktūrą, akcentuojama tarpusavio priklausomybė, ugdomi eskalavimo, grėsmių valdymo ir kibernetinių atakų priskyrimo gebėjimai. Visgi svarbiausios buvo pratybos „Kibernetinis skydas 2018", kurios 2018 m. buvo organizuotos kartu su Lietuvos kariuomenės pratybomis „Gintarinė migla 2018".[118] Šių pratybų metu kibernetinio saugumo subjektai ne tik tobulino gebėjimus atpažinti kibernetinius incidentus ir apie juos informuoti kompetentingas institucijas, tačiau praktiškai buvo išbandytos komandos iškvietimo procedūros, kurių metu projekto dalyviai realiu laiku vertino, kokiu būdu būtų galima suteikti pagalbą Lietuvai. Pratybų metu įgyta patirtis buvo perkelta į greitojo reagavimo pajėgų iškvietimo atmintines.[119]

ES taip pat didina bendradarbiavimą su NATO, ypač techniniame lygmenyje. 2016 m. pasirašytas susitarimas tarp organizacijų, kuriuo siekiama užtikrinti informacijos dalijimąsi, nes tai, anot NATO Komunikacijų ir informacijos agentūros vadovo Koeno Gijsberso, yra „esminė kibernetinės gynybos stiprinimo detalė". Nepaisant to, pripažįstama, kad nors kibernetinis saugumas įgyja vis didesnę svarbą, praktiniame lygmenyje valstybių bendradarbiavimas šiuo klausimu, dėl skirtingų teisės aktų, o kartais – ir politinių interesų, išlieka komplikuotas. Todėl itin svarbu užtikrinti, kad kibernetinis saugumas pasiektų deramą lygmenį nacionaliniu, o kartais – ir privačiu mastu. Atsižvelgiant į tai, kad kibernetiniai incidentai daro didelę žalą tiek nacionaliniu, tiek tarptautiniu lygmeniu, visos pasaulio valstybės, taip pat ir didžiosios tarptautinės organizacijos, pradedant Jungtinėmis Tautomis ir baigiant Šiaurės Atlanto Sutarties Asociacija (NATO), kibernetines grėsmės laiko prioritetu ir ieško būdų kaip efektyviai į jas reaguoti.[120]

[115]CCDCOE, „Locked Shields", https://ccdcoe.org/exercises/locked-shields/
[116]EuropeanUnionAgencyforcybersecurity, „Cyber Europe 2018", https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme/cyber-europe-2018.
[117]NATO, „NATO holas Cyber Coalition 2018", 2018 m.
[118]Nacionalinio kibernetinio saugumo centras, „Lietuvoje vyksta kibernetinio saugumo ir gynybos pratybos", 2018 m.
[119]NKSC, Nacionalinio kibernetinio saugumo būklės ataskaita, 2018 m. 49 p.
[120]Linas Kojala, „Virtualios erdvės saugumas – iššūkis ir JAV ir Europai", 2016 m.

Išvados

1. Nacionalinio saugumo sąvoka yra vartojama moksliniu, politiniu ir visuomeniniu požiūriu. Saugumo sąvoką yra sunku tiksliai apibrėžti, nes tiek visuomeniniu tiek politiniu požiūri ši sąvoka interpretuojama skirtingai. Nėra vieno, visuotinai priimto jos apibrėžimo. Kaip teigia Barry Buzan „pati saugumo sąvokos prigimtis neleidžia suformuluoti tikslaus jos apibrėžimo“, kadangi šis terminas yra plačiai naudojamas, kyla sunkumų norint nustatyti jo ribas.Išanalizavus pateiktus autorių apibrėžimus matome, kad saugumo sąvoka mokslinėje literatūroje nėra vienprasmiškai apibrėžta, nes dėl egzistuojančių skirtumų tarp šalių negalima tikėtis, kad būtų priimtas vieningas ir universalus apibrėžimas, nes kas tinka vienai valstybei, nebūtinai gali tikti kitai.

2. Nacionalinį saugumą veikia įvairūs valstybės ir visuomenės veiksniai. Vienas iš jų yra kibernetinis saugumas. Kibernetinio saugumo sąvoka šiais laikais tampa vis aktualesniu ir daugiau dėmesio sulaukiančiu reiškiniu. Kibernetinis saugumas yra plačiai naudojamas terminas, kurio apibrėžimai būna labai įvairūs, dažnai subjektyvūs, o kartais net neinformatyvūs. Visuotinai priimtos, trumpos ir aiškiai apibrėžtos sąvokos nebuvimas, kuriame būtų apibrėžtas kibernetinio saugumo daugialypiškumas, trukdo technologinei ir mokslinei raidai. Dėl kibernetinio saugumo specifiškumo, jo iki galo užtikrinti neįmanoma, o vis labiau tobulėjant technologijoms atsiranda naujų grėsmių darančių įtaką kibernetiniam saugumui.

3. Nacionalinis saugumas yra kiekvienos valstybės ir jos piliečių nepriklausomos egzistencijos pagrindas. Būtent todėl nacionalinio saugumo užtikrinimas yra aukščiausias kiekvienos valstybės vidaus ir užsienio politikos tikslas. Nacionalinis saugumas yra nepaprastai svarbus, nes tai yra saugumo nuo išorinių grėsmių pagrindas. Jei nebūtų nacionalinio saugumo į valstybę būtų galima lengvai ir greitai įsiveržti ir įveikti, paverčiant piliečius pavaldžiais kitai tautai. Kiekviena valstybė turi tam tikrą nacionalinio saugumo formą, dauguma turi nuolatinę kariuomenę, užtikrinančią nacionalinį saugumą, ar sąjungas su kitomis valstybėmis. Lietuva yra priėmusi ne vieną teisės aktą siekdama kuo geriau užtikrinti savo nacionalinį saugumą: Lietuvos Respublikos Konstituciją, Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymą, tarptautinės teisės principai ir normos, kiti šalies įstatymai. Taip pat Lietuva, vykdydama nacionalinio saugumo politiką, vadovaujasi nacionalinio saugumo strategija ir savo veiksmus derina su Europos Sąjungos bendros saugumo ir gynybos politikos strateginiais tikslais.

4. Pagrindiniai Lietuvos nacionalinio saugumo politikos tikslai yra apsaugoti gyvybinius ir pirmaeilius nacionalinius interesus, neutralizuoti pavojus bei grėsmes ir neleisti rizikos veiksniams virsti pavojais ar grėsmėmis. Dauguma rizikos veiksnių nacionaliniam saugumui yra tęstinio pobūdžio, juos visiškai panaikinti sunkiai įmanoma. Tik nuolatinės pastangos gali užtikrinti

minimalią jų tikimybę virsti grėsmėmis ir neleisti atsirasti nepalankiems padariniams ekonominiame,socialiniame, ekologiniame ir kt. sektoriuose.

5. Kibernetinis saugumas yra gana specifinis veiksnys ir jo iki galo užkardyti yra neįmanoma, būtinas tinkamas, detalus ir nuoseklus teisinis reguliavimas, siekiant kuo labiau sumažinti iškylančių grėsmių riziką. Lietuvoje svarbiausi teisiniai dokumentai užtikrinantis kibernetinį saugumą yra 2011 m. kibernetinio saugumo plėtros programa 2011-2019, 2018 m. Kibernetinio saugumo įstatymas ir Kibernetinio saugumo strategija.Šių teisinių dokumentų tikslas – plėtoti elektroninės informacijos saugą Lietuvoje, užtikrinti kibernetinį saugumą, nustatyti kibernetinio saugumo principus, kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijas, tarpinstitucinį bendradarbiavimą, stiprinti kibernetinių gynybos pajėgumų plėtrą, užtikrinti nusikalstamų veikų prevenciją, užkardymą ir tyrimą. Apžvelgus visus kibernetinį saugumą reglamentuojančius teisės aktus, galima teigti, kad iki 2011 m. kibernetinio saugumo užtikrinimui nebuvo skiriamas pakankamas dėmesys, ir tik patvirtinus 2011 m. kibernetinio saugumo plėtros programą 2011-2019, buvo padėtas tvirtas pagrindas teisiniam kibernetinio saugumo užtikrinimui Lietuvoje. Todėl galima teigti, kad tai paneigia ginamąjį teiginį apie tai, kad kibernetinio saugumo teisinio reglamentavimo trūkumas lemia kibernetinio saugumo problematiką Lietuvoje.

6. Atsižvelgiant į tai, kad kibernetinės atakos neturi sienų ir gali daryti žalą ne tik atskirai valstybei, bet ir Aljansui yra būtinas atitinkamas kibernetinio saugumo užtikrinimas ir Sąjungos mastu. Todėl kibernetinis saugumas akcentuojamas ne viename ES dokumente. 2013 m. ES kibernetinio saugumo strategija yra išsamus strateginis dokumentas, kuriame reglamentuojami esminiai principai, tikslai, kibernetinio saugumo užtikrinimo lygiai bei valstybių narių ir Komisijos bendradarbiavimo mechanizmas. Taip pat siekdama, kuo geriau užtikrinti kibernetinį saugumą ir apsaugoti vartotojus visoje ES, buvo įsteigta Europos tinklų ir informacijos saugumo agentūrą. ES taip pat pabrėžia, kad yra labai svarbus glaudesnis Sąjungos šalių bendradarbiavimas ir sklandus informacijos dalijimasis kovojant su nusikaltimais virtualioje erdvėje. ES kibernetinė parengtis yra ypač svarbi tiek bendrajai skaitmeninei rinkai, tiek saugumo ir gynybos sąjungai, todėl labai svarbu stiprinti Europos kibernetinį saugumą.Tai visiškai paneigia teiginį, kad kibernetinis saugumas ES nėra prioritetinis saugumo klausimas.

7. Kibernetinis saugumas aktualus ne tik ES, bet ir NATO. Atsižvelgiant į tai, kad kibernetinės grėsmės tampa vis sudėtingenės ir daro daug žalos, NATO turi būti pasirengusi ginti savo informacinius tinklus ir stiprinti Aljanso atsparumą kibernetinio saugumo atžvilgiu. 1994 m. po kibernetinių išpuolių Kosove, NATO pradėjo pripažinti kibernetinį erdvę kaip kolektyvinės gynybos dalį. NATO išreiškus norą plėtoti informacinių tinklų pajėgumus, saugiai dalintis informacija, duomenimis ar žvalgybos informacija, kibernetinio saugumo užtikrinimo siekimas

pakilo į aukštesnį lygį. Nuo to laiko kibernetinis saugumas tapo NATO viršūnių susitikimų dienotvarkės prioritetu. Siekdamas kuo geriau užtikrinti informacinę erdvę, politiniu lygmeniu Aljansas toliau stiprina savo kibernetinį saugumą, gynybą ir atgrasymo strategijas, nuolat atnaujina veiksmų planus su konkrečiais tikslais ir terminais.Tai visiškai paneigia teiginį, kad kibernetinis saugumas NATO dienotvarkėje nėra prioritetinis saugumo klausimas.

8. Kibernetinės grėsmės nemenką galvos skausmą kelia ne tik NATO ir ES, bet ir Lietuvai. Lietuvoje vis daugiau gyvenimo sričių perkeliant į virtualią erdvę, aktyviai naudojant elektroninius ryšius informacijai gauti ir siųsti,kyla grėsmės kibernetiniam saugumui, kibernetinės erdvės globalumas skatina neteisėtas veikas elektroninėje erdvėje. Kibernetiniai incidentai ir kibernetinis šnipinėjimas vienos iš nedaugelio grėsmių su kuriomis susiduria Lietuva. NKSC duomenimis kibernetinių incidentų skaičius lyginant su praėjusiais metais išaugo, o pačios grėsmės tapo sudėtingesnės. Dar viena svarbi grėsmė nukreipta prieš Lietuvą yra kibernetinis šnipinėjimas. Kibernetinis šnipinėjimas prieš Lietuvos institucijas ar šalies kritinę infrastruktūrą kelia grėsmę nacionaliniam saugumui. Didžiausią grėsmę Lietuvos kibernetinei erdvei kelia Rusijos žvalgybos ir saugumo tarnybos – jos vykdo žvalgybą, rengia IT sistemų trikdymą ir prisideda vykdant įtakos operacijas. Prognozuojama, kad kibernetinių incidentų ir kibernetinio šnipinėjimo atvejų tik daugės, todėl kibernetinis saugumas ir gynyba turėtų išlikti valstybės prioritetu.

9. Siekiant kuo geriau užtikrinti kibernetinį saugumą reikia stiprinti pačios valstybės kibernetinį saugumą ir gynybos pajėgumų plėtrą. To galima pasiekti, tobulinat kibernetinio saugumo rizikos nustatymo, vertinimo ir užkardymo būdus. Nereiktų pamiršti ir kibernetinių nusikaltimų prevencijos ir užkardymo galimybių, būtina plėtoti valstybės pajėgumus ir gebėjimus kovoti su kibernetiniais incidentais. Dar vienas aspektas, siekiant kuo geriau užtikrinti kibernetinį saugumą yra dalyvavimas nacionalinėse ir tarptautinėse kibernetinio saugumo pratybose. Periodiškai rengiamos kompleksinės nacionalinio kibernetinio saugumo pratybos, dalyvavimas ES ir NATO organizuojamose pratybose padės įgyti naujos patirties, pasidalinti pačių turimomis žiniomis, atliekant situacijų valdymo, incidentų vertinimo, informacijos dalijimosi ar kitus veiksmus. Taip pat atsakingos institucijos turėtų nustatyti kibernetiniam saugumui reikalingų lėšų skyrimo bei panaudojimo prioritetus, stengtis užtikrinti įstaigų konsultavimą ir informavimą kibernetinio saugumo klausimais, skatinti tarptautinį bendradarbiavimą ir informacijos dalijimąsi.

10. Norint kuo geriau užtikrinti ne tik nacionalinį, bet ir tarptautinį kibernetinį saugumą būtinas šalių, NATO ir ES bendradarbiavimas. Svarbu gerinti kibernetinio saugumo specialistų kompetenciją, dėl šios priežasties nuolat vyksta tarptautinės kibernetinio saugumo pratybos, kuriose mokomasi veikti kibernetinės atakos atveju, keičiamasi informacija ir turimomis žiniomis. Kuriami nauji kibernetinio saugumo projektai, atnaujinami tarptautiniai teisės aktai reglamentuojantys kibernetinį saugumą, Lietuvos iniciatyva kuriamos rotuojamos ES kibernetinės greitojo reagavimo

komandos. Atsižvelgiant į tai, kad kibernetiniai incidentai daro didelę žalą ir nuolatos tobulėja jų pobūdis, visos pasaulio valstybės, tai pat didžiosios organizacijos (ES, NATO), kibernetines grėsmes turi laikyti prioritetine sritimi ir ieškoti būdų kaip efektyviai į jas reaguoti.

Literatūros sąrašas

1. A. Petrauskaitė, R. Markelienė, R. Gedminienė, „Šalies saugumas ir gynyba“, Vilnius 2016 m.
2. Buzan B., Žmonės, valstybės ir baimės, Vilnius: Eugrimas, 1997 m.
3. Carson Zimmerman, 2014 m. Ten Strategies of a Worl-Class Cyber security Operations Center. The MITRE Corporation.
4. Council of Europe, 2001 m.. Convention on cyber crime. Budapest.
5. Dan Craigen, Nadia Diakun-Thibault, Randy Purse, „Defining Cybersecurity“, 2014 m.
6. Darius Štitilis, „Kibernetinio saugumo teisinis reguliavimas: kibernetinio saugumo strategijos“, 2013 m.
7. Deborah Bodeau, Richard Graubart, Cyber Resiliency Design Principle. The MITRE Corporation, 2017 m.
8. Dean C. Alexander, „Cyber threats against the North Atlantic Treaty Organization (NATO) and selected responses“,[žiūrėta: 2019 m. gruodžio 11 d.]. prieiga per interneta: <https://dergipark.org.tr/tr/download/article-file/89251>.
9. E.F. Chamorro, Dr. J.R.C.Fernandez, R.M. Lopez. S.L.Fernandez, „National Cyber Security, a commitment for everybody“, 2012 m.
10. E. Vareikis „Tarptautinis ir nacionalinis saugumas“. VDU leidykla, 2005 m.
11. E. Vareikis – „Kas yra krikščioniškoji demokratija (X). Karas ir saugumas“, 2015 m., [žiūrėta: 2019 m. balandžio 22 d.]. prieiga per internetą: <http://www.arche.lt/2015/11/egidijus-vareikis-kas-yra.html>
12. Erika Matulionytė „Grėsmių nacionaliniam saugumui nustatymas ir jų prevencijos galimybės“, Vilnius, 2008 m.
13. Europos Sąjungos kibernetinio saugumo strategija 2013 m.
14. Europos komisija, „Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas“, 2017 m.
15. Europos komisija, „ES padėtis 2017 m. Kibernetinis saugumas“, 2017 m.
16. Europos Parlamento ir Tarybos direktyva (95/46/EB) „Dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo“, 1995 m.
17. Europos Parlamento ir Tarybos direktyva 2002/58/EB „Dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje“, 2002 m.
18. Europos Parlamento ir Tarybos direktyva 2002/21/EB „Dėl elektroninių ryšių tinklų ir paslaugų bendrosios reguliavimo sistemos“, 2002 m.
19. Europian Commission, „BuildingstrongcybersecurityinEurope“, 2018 m.
20. Fred Kaplan, „Kibernetiniai karai“, 2018 m.

21. Held D., Mc Grew A. ir kt. Globaliniai pokyčiai: politika, ekonomika ir kultūra. Vilnius: Margi raštai, 2002 m.
22. Institute for security studies, „Riding the Digital wave: the impact of cyber capacity building on human development“, 2014 m.
23. I. Urmanavičiūtė, „Duomenų apsaugos priemonių kompiuterizuoto parinkimo ir įvertinimo metodika“, 2010 m.
24. ISACA, „Auditing Cyber Security: Evaluating Risk and Auditing Controls“, 2017 m. [žiūrėta: 2019 m. balandžio 18 d.]. Prieiga per internetą: <https://academy.crucialgroup.co.uk/docs/Auditing-Cyber-Security.pdf>
25. James A. Lewis, „CybersecurityandCriticalinfrastructureprotection“, Center for Strategic and International studies, 2006 m.
26. Jarno Limnell, Challenge for NATO – Cyber Article 5. Swedish Defence University, 2016 m.
27. J. Vaškūnas „Tautinė kultūra – pagrindinis šių laikų nacionalinio saugumo uždavinys“, 2019 m.
28. Jurgita Jakevičiūtė, „Paradigminės konstruktyvistų ir Neorealistų diskusijos saugumo objekto ir jam kylančių grėsmių prigimties Klausimais: bendros ES karinio saugumo Sistemos idėja“, Vilnius, 2011 m.
29. Justine Marie Chauvin, „NATO Cyber Defence Policy“, 2014 m.
30. Jason Healey, Leendert van Bochoven, „NATO‘s Cyber Capabilities: Yesterday, Today, and Tomorrow“, 2011 m.
31. J.Ann Tickner, Saugumo re-vizijos. Ken Booth, Steve Smith „Tarptautinių santykių teorija šiandien“ Vilnius, 2000 m.
32. Karpavičiūtė, I. „Saugumo sampratos kaita. Globalizacija ir transnacionalinių saugumo grėsmių išskyrimas“, 2004 m. [žiūrėta: 2019 m. balandžio 8]. Prieiga per internetą: http://vddb.laba.lt/fedora/get/LT-eLABa-0001:J.04~2004~ISSN_1822-9212.V_1.PG_21-39/DS.002.0.01.ARTIC.
33. Laimutis Telksnys, Vytautas Butrimas, Lukas Grinius, Romena Čiūtienė, Aleksandras Graželis, Linas Kojala, Paulius Saudargas, Jonas Kazimieras Švagžlys, Marius Laurinaitis, Konstantin Agafonov, Simonas Klimanskis: Kibernetinio saugumo apžvalga.
34. Lietuvos Respublikos vyriausybės nutarimas „Dėl duomenų apsaugos valstybės ir vietos savivaldos informacinėse sistemose“, 1997 m.
35. Lietuvos Respublikos vyriausybės nutarimas „Dėl informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo“, 2001 m.
36. Lorenzo Pupillo, EU Cybersecurityandtheparadoxofprogress. Brussels, 2018 m.

37. Martin C. Libicki, Cyber deterrence and cyber war“, 2009 m.
38. Matonytė, V. Morkevičius, A. Lašas, V. Jankauskaitė, „Grėsmių visuomenės gerovei suvokimas: socialinio optimizmo, socialinio ir institucinio pasitikėjimo bei pasitikėjimo savimi įtaka“, 2017 m.
39. Margarita Šešelgytė, „Europos saugumas: nauji iššūkiai ir bendradarbiavimo galimybės:, 2003 m.
40. Michael Rühle, „NATO and Emerging Security Challenges: Beyond the Deterrence Paradigm,” American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy 33, 2011 m.
41. Nacionalinio kibernetinio saugumo centras prie Krašto apsaugos ministerijos, 2017 metų nacionalinio kibernetinio saugumo būklės ataskaita.
42. National Institute of Standards and Technology. NISTIR 7298, revision 2, glossary of key information security terms. 2013 m.
43. Nort Atlantic Treaty Organization, NATO Cyber Defence. Public Diplomacy Division, 2017 m.
44. NATO, Riga Summit Declaration, 2006 m. [žiūrėta: 2019 m. gruodžio 18 d.]. Prieiga per internetą: <https://www.nato.int/cps/en/natohq/official_texts_37920.htm?selectedLocale=en>.
45. NATO, EmergingSecurityChallengesDivision, [žiūrėta: 2019 m. gruodžio 18 d.]. Prieiga per internetą: <https://esc.hq.nato.int/default.aspx>.
46. NATO, „Defending the networks. The NATO Policy on Cyber Defence“, 2011 m. [žiūrėta: 2019 m. gruodžio 18 d.]. Prieiga per internetą: <https://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf>.
47. Misha Glenny, „Nematoma rinka. Elektroniniai nusikaltimai ir Jūs“, 2011 m.
48. Paulauskas K. Saugumo studijų būklė ir raidos tendencijos. Lietuvos metinė strateginė apžvalga 2006 m. Vilnius: VU TSPMI, 2007 m.
49. PWC. „2015 Informationsecuritybreachessurvey“, 2015 m. [žiūrėta: 2019 m. balandžio 22 d.]. Prieiga per internetą: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/432412/bis-15-302-information_security_breaches_survey_2015-full-report.pdf>
50. Richard A. Kemmerer, „Cybers ecurity“, University of California, 2003 m.
51. Rytis Rainys, „Kibernetinio saugumo vertinimas Lietuvoje ir saugumo reikalavimai informacijos prieglobos teikėjams“, 2017 m.

52. Rolanda Kauzlauskaitė-Markelienė, Audronė Petrauskaitė „Pilietinė visuomenė ir nacionalinis saugumas: teorinė problemos apžvalga“, 2011 m.
53. Tomas Stamulis, „Kibernetinis saugumas. Ką saugom ir nuo ko saugom?“ 2015 m.
54. Saugi Europa geresniame pasaulyje. Europos saugumo strategija. 2003 m., [žiūrėta: 2019 m. balandžio 22 d.].Prieiga per internetą:<https://www.consilium.europa.eu/uedocs/cmsUpload/031208ESSIILT.pdf>
55. Shahri A, Ismail Z, Rahim N. „Security effectiveness in health information system: through improving the human factors by education and training“, Australian Journal of Basic and Applied Sciences 2012 m.
56. Straipsnis „Infografikas: didžiausios kibernetinės grėsmės“, 2015 m., [žiūrėta: 2018 m. lapkričio 26 d.]. Prieiga per internetą: <http://www.europarl.europa.eu/news/lt/headlines/society/20151207IFG06371/infografikas-didziausios-kibernetines-gresmes>.
57. Kaspersky Lab, „Whatis Cyber-Security?, [žiūrėta: 2019 m. balandžio 16 d.].Prieiga per internetą: <https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security>.
58. Laura Brent, „NATO‘s role in cyberspace“, 2019 m. [žiūrėta: 2019 m. gruodžio 11 d.]. Prieiga per internetą: <https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html>.
59. Lietuvos Respublikos vyriausybė, Nacionalinė kibernetinio saugumo strategija, 2018m. [žiūrėta: 2019 m. lapkričio 26 d.]. Prieiga per internetą: <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f?jfwid=dg8d31595>.
60. Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas, 1997 m., Nr. VIII-49. Aktuali redakcija nuo 2019-01-01.
61. Lietuvos Respublikos vyriausybė, „Dėl nacionalinio kibernetinių incidentų valdymo plano patvirtinimo“, 2018 m. [žiūrėta: 2018 m. lapkričio 26 d.]. Prieiga per internetą: <https://www.e-tar.lt/portal/lt/legalAct/2a916390c5b211e583a295d9366c7ab3/GSDjgmYIWG>
62. Lietuvos Respublikos Vyriausybė Dėl duomenų saugos valstybės ir savivaldybių informacinėse sistemose, 1997 rugsėjo 4 d. Nr. 952.
63. Lietuvos Respublikos užsienio reikalų ministerija, Europos saugumo ir bendradarbiavimo organizacija (ESBO), 2018 m.
64. Lietuvos Respublikos vyriausybė, nutarimas „Dėl Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepcijos patvirtinimo“, 2006 m.
65. Lietuvos Respublikos Vyriausybė, nutarimas „Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011-2019 metais programos patvirtinimo“. 2011 m.

66. Lietuvos Respublikos kibernetinio saugumo įstatymas, 2018-12-11 Nr. XII-1428.