MYKOLO ROMERIO UNIVERSITETAS

EKONOMIKOS IR VERSLO FAKULTETAS

TARPINSTITUCINIO BENDRADARBIAVIMO LIETUVOJE KIBERNETINIO SAUGUMO SRITYJE VERTINIMAS

Magistro baigiamasis darbas

Vadovas

Doc.dr. Marius Laurinaitis

VILNIUS, 2020

MYKOLO ROMERIO UNIVERSITETAS

EKONOMIKOS IR VERSLO FAKULTETAS

TARPINSTITUCINIO BENDRADARBIAVIMO LIETUVOJE KIBERNETINIO SAUGUMO SRITYJE VERTINIMAS

Kibernetinio saugumo valdymo magistro baigiamasis darbas

Studijų programa 6211LX066

Vadovas
doc.dr. M. Laurinaitis
2020 04

Recenzentas

Atliko
KSVvmis18-1 gr. stud.
Ž. Januško
2020 04 20

VILNIUS, 2020

TURINYS

ĮVADAS

1. TARINSTITUCINIO BENDRADARBIAVIMO KIBERNETINIO SAUGUMO SRITYJE TEORIJA....9

1.1. Kibernetinio saugumo koncepcija....9

1.2. Tarpinstitucinio bendradarbiavimo samprata....12

1.3. Tarpinstitucinio bendradarbiavimo ypatumai kibernetinio saugumo srityje....17

2. TARPINSTITUCINIO BENDRADARBIAVIMO KIBERNETINIO SAUGUMO SRITYJE TYRIMO METODOLOGIJA....23

2.1. Tarpinstitucinio bendradarbiavimo kibernetinio saugumo srityje tyrimo modelis....23

2.2. Tarpinstitucinio bendradarbiavimo kibernetinio saugumo srityje tyrimo metodikos pagrindimas....27

3. TARPINSTITUCINIO BENDRADARBIAVIMO LIETUVOJE KIBERNETINIO SAUGUMO SRITYJE ANALIZĖ....32

3.1. Nacionalinio kibernetinio saugumo centro tarpinstitucinio bendradarbiavimo formavimo procesų analizė....32

3.2. Valstybės institucijų tarpinstitucinio bendradarbiavimo formavimo procesų analizė....37

3.3. Tarpinstitucinio bendradarbiavimo Lietuvoje kibernetinio saugumo srityje ypatumai....50

IŠVADOS IR PASIŪLYMAI....58

LITERATŪRA....61

PRIEDAI....62

ANOTACIJA....70

ANNOTATION....71

SANTRAUKA....72

SUMMARY....74

PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ....76

LENTELĖS

1 lentelė. Kibernetinio saugumo apibrėžimai....9
2 lentelė. Kibernetinio saugumo koncepcijos veiksniai....11
3 lentelė. Tarpinstitucinio bendradarbiavimo būdai....13
4 lentelė. Bendradarbiavimo modeliai....14
5 lentelė. Tarpinstitucinio bendradarbiavimo neigiamos veiklos būsenos....15
6 lentelė. Koordinavimo modeliai....17
7 lentelė. Tarpinstitucinio bendradarbiavimo reglamentavimas kibernetinio saugumo srityje....18
8 lentelė. Tarpinstitucinio bendradarbiavimo principai....19
9 lentelė. Kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos....20
10 lentelė. Tarpinstitucinis bendradarbiavimas valdant ir tiriant kibernetinius incidentus....21
11 lentelė. Empirinio tyrimo metodai....26
12 lentelė. Tarpinstitucinio bendradrbiavimo kibernetinio saugumo srityje empirinio tyrimo etapai....27
13 lentelė. Klausimynas NKSC ekspertų apklausti....28
14 lentelė. Klausimynas valstybės institucijų ekspertų apklausti....30
15 lentelė. NKSC misija, pagrindiniai veiklos tikslai, teikiamos paslaugos, rekomendacijos....35
16 lentelė. LR aplinkos ministerija - YSI objekto sektoriai, subsektoriai ir paslaugos....38
17 lentelė. LR finansų ministerija - YSI objekto sektoriai, subsektoriai ir paslaugos....39
18 lentelė. LR energetikos ministerija - YSI objekto sektoriai, subsektoriai ir paslaugos....40
19 lentelė. LR susisiekimo ministerija - YSI objekto sektoriai, subsektoriai ir paslaugos....41
20 lentelė. LR sveikatos apsaugos ministerija - YSI objekto sektoriai, subsektoriai ir pasalugos....42
21 lentelė. LR ekonomikos ir inovacijos ministerija - YSI objekto sektoriai, subsektoriai ir paslaugos....43
22 lentelė. LR užsienio reikalų ministerija - YSI objekto sektoriai, subsektoriai ir paslaugos....44
23 lentelė. LR vidaus reikalų ministerija - YSI objekto sektoriai, subsektoriai ir paslaugos....45
24 lentelė. LR žemės ūkio ministerija - YSI objekto sektoriai, subsektoriai ir paslaugos....46
25 lentelė. LR Vyriausybė - YSI objekto sektoriai, subsektoriai ir paslaugos....47
26 lentelė. LR teisingumo ministerija - YSI objekto sektoriai, subsektoriai ir paslaugos....47
27 lentelė. LR krašto apsaugos ministerija - YSI objekto sektoriai, susektoriai ir paslaugos....48
28 lentelė. Ar vykdote tarpinstitucinį bendardarbiavimą su NKSC?....52
29 lentelė. Kaip vykdote tarpinstitucinį bendardarbiavimą su NKSC?....52
30 lentelė. Kokiais atvejais vykdomas tarpinstitucinis bendradarbiavimas su NKSC formaliuoju būdu?....53

31 lentelė. Kokiomis priemonėmis vykdote tarpinstitucinį bendradarbiavimą formaliuoju būdu su NKSC?.....53
32 lentelė. Kaip dažnai vykdomas tarpinstitucinis bendrdarbiavimas formaliuoju būdu su NKSC.....54
33 lentelė. Kokiais atvejais vykdomas tarpinstitucinis bendradarbiavimas su NKSC neformaliuoju būdu?.....54
34 lentelė. Kokiomis priemonėmis vykdote tarpinsitucinį bendradarbiavimą neformaliuoju būdu su NKSC?.....55
35 lentelė. Kaip dažnai vykdomas tarpinstitucinis bendradarbiavimas neformaliuoju būdu su NKSC?..55
36 lentelė. Jūsų nuomonė ar tarpinstitucinio bendradarbiavimo kokybė su NKSC tenkina Jūsų poreikius?.....56
37 lentelė. Neformaliojo būdo reglamentavimo poreikis tarpinstituciniame bendrdarbiavime.....56

PAVEIKSLAI

1 pav. Tyrimo modelis.....22

ĮVADAS

Temos aktualumas ir naujumas. Kibernetinio saugumo pasaulyje, kuriame vis labiau besikeičianti ir svaiginanti grėsmių aplinka didėja, tarpinstitucinis bendradarbiavimas šių dienų tampa aktuali tema. Kibernetinis saugumas yra vienas iš pagrindinių kiekvienos šiuolaikinės demokratinės valstybės vertybių. Šioje srityje rizikos elementų daugėja. Todėl nuolat kintančioje kibernetinio saugumo aplinkoje vienu iš svarbiausių prioritetų laikomas tarpinstitucinis bendradarbiavimas. Kai kurios kibernetinio saugumo partnerystės vystosi tarp vyriausybinių institucijų, o kai kurios iš jų yra tarp įmonių, kurios sprendžia saugumo klausimus. Tarpinstitucinio bendradarbiavimo kibernetinio saugumo srityje tema yra aktuali net tik kibernetinio saugumo valdymo institucijoms. Kibernetiniame saugume tarpinstitucinis bendradarbiavimas gali sudaryti galimybes apjungti kelių organizacijų pastangas ir siekti bendrai užsibrėžtų tikslų. Raišienė (2015) teigia, kad bendradarbiavimas tampa esmine strategija, siekiant šiuolaikinės visuomenės ir valstybės plėtros. Tad pagrįstai galima sakyti, kad tarpinstitucinio bendradarbiavimo nauda yra grindžiama tuo, jog visuomenės įtraukimas į kibernetinį saugumo procesą skatins ją tapti aktyviu veikėju, o ne tik pasyviu pagalbos gavėju. Taigi, tarpinstitucinis bendradarbiavimas gali būti galimybė užtikrinti visuomenės ir valstybės kibernetinį saugumą. Mokslininkės Jurkonienė ir Karčiauskienė (2017) atliktame tyrime nustatė, kad sėkmingam tarpinstituciniam bendradarbiavimui reikalinga ne tik keičiama strateginio planavimo metodika (teisės aktai), tačiau turi būti intensyviai skatinamas neformalus bendradarbiavimas. Dažniausiai tarpinstitucini bendradarbiavimą sudaro ne tik formalus bendradarbiavimas, kuris reglamentuoja procedūros apibrėžtos teisės aktuose, bet ir neformalus bendradarbiavimas, kuris nereglamentuotas ir kur procedūros nėra apibrėžtos teisės aktuose.

Tarpinstitucinis bendradarbiavimas ir jų klausimų koordinavimas yra iššūkis Lietuvos viešojo sektoriaus institucijoms. Pagrindinis tarpinstitucinio bendradarbiavimo įrankis Lietuvoje yra tarpinstitucinių programų (veiklos planų) rengimas ir įgyvendinimas. Vienas iš pagrindiniu teisės aktu kuriame akcentuojamas tarpinstitucinis bendradarbiavimas yra Lietuvos Respublikos nutarimas “Dėl vystomojo bendradarbiavimo tarpinstitucinio veiklos plano patvirtinimo“ (2016 m. rugsėjo 21 d. Nr. 937), kurio siekiama stiprinti tarpinstitucinį vystomojo bendradarbiavimo veiklos koordinavimą ir užtikrinti nepertraukiamą ir veiksmingą Lietuvos vystomojo bendradarbiavimo veiklą. Pasak Puškorių (2007) bendradarbiavimas yra ypatingos veiklos rūšys kur veikla atliekama dalyvaujant keliems vykdytojams, valdymo subjektams, institucijoms, sistemoms ar net valstybėms.

Lietuvoje tarpinstitucinis bendradarbiavimas kibernetinio saugumo srityje yra dar pakankamai nauja tema. Nėra daug mokslinių straipsnių lietuvių kalba bei tyrimų nagrinėjančių tarpinstitucinio bendradarbiavimo sąveiką kibernetinio saugumo srityje, sėkmės prielaidas, veiksnius ar problemas.

Abipusis pasitikėjimas ir neformalaus tarpinstitucinio bendradarbiavimo nauda gali padėti efektyviai ir laiku identifikuoti kibernetinius incidentus, užkirsti kelią jų atsiradimui, plitimui, valdyti kibernetinių incidentų sukeltas pasekmes. Taigi siekiant garantuoti galimybę visuomenei saugiai naudotis informacinių ir ryšių technologijų teikiamomis galimybėmis, tarpinstitucinis bendradarbiavimas tampa būtina sąlyga visapusiškam kibernetiniam saugumui užtikrinti.

Atsižvelgiant į tai, kad nėra pakankamai ištyrinėtas tarpinstitucinis bendradarbiavimas kibernetinio saugumo srityje, kuris lemia kibernetinio saugumo užtikrinimą, pasirinkta magistro darbo tema – Tarpinstitucinio bendradarbiavimo Lietuvoje kibernetinio saugumo srityje vertinimas.

Tyrimo problema – nėra aiškių kriterijų, kuriais remiantis vertinti tarpinstitucinį bendradarbiavimą kibernetinio saugumo srityje.

Tyrimo objektas – tarpinstitucinis bendradarbiavimas Lietuvoje kibernetinio saugumo srityje.

Tyrimo hipotezė - poreikis reglamentuoti Lietuvos Respublikos teisės aktuose neformalųjį tarpinstitucinį bendradarbiavimą kibernetinio saugumo srityje.

Tyrimo tikslas – išnagrinėjus mokslinius požiūrius, praktinius aspektus į tarpinstitucinį bendradarbiavimą kibernetinio saugumo srityje ir parengus tyrimo metodologiją ištirti ir apibrėžti Lietuvos tarpinstitucinio bendradarbiavimo kibernetinio saugumo srityje ypatumus.

Tyrimo uždaviniai:

1) Pateikti tarpinstitucinio bendradarbiavimo kibernetinio saugumo srityje teorinius aspektus;
2) Parengti teikti tarpinstitucinio bendradarbiavimo kibernetinio saugumo srityje tyrimo metodologija;
3) Išanalizuoti tarpinstitucinį bendradarbiavimą Lietuvoje kibernetinio saugumo srityje.
4) Atsižvelgiant į atliktą tyrimą prireikus pateikti pasiūlymus dėl tarpinstitucinio bendradarbiavimo Lietuvoje kibernetinio saugumo srityje tobulinimo.

Tyrimo metodika. Analizuojant tarpinstitucinį bendradarbiavimą kibernetinio saugumo srityje buvo naudota sisteminė, apibendrinimo, lyginamoji ir aprašomoji mokslinės literatūros analizė bei teisės dokumentų turinio analizė, kurios tikslas buvo atskleisti kibernetinio saugumo tarpinstitucinio bendradarbiavimo teisinį reguliavimą Lietuvoje.

1. TARPINSTITUCINIO BENDRADARBIAVIMO KIBERNETINIO SAUGUMO SRITYJE TEORIJA

1.2. Kibernetinio saugumo koncepcija

Informacinių ir ryšių technologijų naudojimo eksponentinis augimas nuo XX a. antrosios pusės smarkiai įtakojo visuomenės raidos tendencijas. Šiuolaikinės informacinės ir ryšių technologijos iš esmės išplėtė galimybes ir padidino sąveikos metodų efektyvumą tarp geografiškai nutolusių subjektų, institucijų iš įvairių visuomenės ir ekonomikos sričių. Taigi dėl didėjančio informacinių ir ryšių technologijų vartotojų skaičiaus ir jų priklausomybė elektroninė erdvė tampa labiau pažeidžiama ir kibernetinis saugumas yra laikomas esminiu valstybės saugumo elementu.

Kibernetinio saugumo sritis neturi būti laikoma atskira valstybės problema arba atskiras vienos ar kelių visuomenės elementų problema. Dėl pasaulinės reikšmės, kibernetinis saugumas yra visuomenės reiškinys. Jis turi būti grindžiamas kompleksiniu požiūriu, reikalaujančiu intensyviai bendrai naudoti informaciją ir koordinuoti veiklą tiek nacionaliniu, tiek tarptautiniu lygiu. Kuriant kibernetinį saugumą būtina siekti, kad valstybės, viešojo ir privataus sektorių, taip pat nacionalinių ir tarptautinių institucijų civiliniai ir saugumo vienetai bendradarbiautų. Saugumo incidentų ir įvykių valdymas priklauso ne tik nuo viešojo sektoriaus gebėjimų, bet ir labai priklauso nuo konstruktyvaus veikėjų, veikiančių ne viešajame sektoriuje. Tinkamą ir veiksmingą kibernetinės erdvės apsaugą turi užtikrinti atitinkamos institucijos, atsakingos už atskirų sektorių infrastruktūrą nacionaliniu lygmeniu ir už tarptautinį infrastruktūros eksploatavimą.

Mokslo literatūroje trūksta universalios kibernetinio saugumo sąvokos. Taip pat pasitelkus į pastarųjų metų mokslinę literatūrą pastebėta, kad kalbama ne tik apie patį kibernetinį saugumą kaip reiškinį bet kaip apie visuma tarpusavyje susijusiu ir vieną kitą palaikančiu institucijų, nevyriausybinių organizacijų, apie kibernetinio saugumo organizaciją, politiką, apie kibernetinio saugumo formavimo proceso principus (žr.1 lent.).

1 lentelė. Kibernetinio saugumo apibrėžimai

Autorius	Apibrėžimas
Kemmerer, 2003	Kibernetinis saugumas tai yra gynybinių metodų visuma, kurie naudojami aptikti ir užkirsti kelią būsimiems elektroninės erdvės atakoms bei įsibrovimams.
Lewis, 2006	Kibernetinis saugumas tai kompiuterinių tinklų apsauga ir jose esančios informacijos nuo įsilaužimo ar veiklos sutrikdymo. ***1 lentelės tęsinys kitame puslapyje***

Amoroso, 2006	Kibernetinis saugumas apima rizikų mažinimą kenkėjiškų išpuolių programinei įrangai, kompiuteriams ir tinklams. Tai apima įrankius, naudojamus pažeidimams aptikti, sustabdyti virusus, užkirsti kelią kenkėjiškoms prieigoms, užtikrinti autentiškumą, sustiprinti užšifruotus ryšius.
ITU, 2009	Kibernetinis saugumas yra technologijų, saugumo koncepcijų, saugumo garantijų, gairių, rizikos valdymo metodų, veiksmų, mokymo, politikos, geriausių priemonių ir praktikos rinkinys, kuris gali būti naudojamos kibernetinei aplinkai ir organizacijai bei naudotojo turtui apsaugoti.
CNSS, 2010	Gebėjimas apsaugoti ar ginti kibernetinės erdvės naudojimą nuo kibernetinių išpuolių.
Government of Canada, 2014	Technologijų, procesų, gerosios praktikos į reagavimą, bei mažinimo priemonių, skirtų tinklams, kompiuteriams, programoms ir duomenims apsaugoti nuo žalingos ir įtartinos prieigos užtikrinant konfidencialumą, vientisumą ir prieinamumą.
Canongia & Mandarino, 2014	Kibernetinis saugumas tai yra menas užtikrinti tautos informacinės visuomenės egzistavimą ir tęstinumą, garantuojant ir saugant kibernetinėje erdvėje informaciją, turtą ir ypatingos svarbos infrastruktūrą.
Oxford University press, 2014	Kibernetinis saugumas yra apsauga nuo nusikalstamo ar neteisėto elektroninių duomenų naudojimo ar priemonių, kurių buvo imtasi siekiant šio tikslo.
DHS, 2009	Kibernetinis saugumas tai yra veikla - procesas, gebėjimai ir pajėgumai saugant valstybės ryšių sistemas ir juose esanti informacija nuo žalingo, neteisėto naudojimo, pakeitimo ar eksploatavimo.

Šaltinis: parengta autorės, remiantis nurodytais šaltiniais

Kibernetinis saugumas yra naujai ir plačiai vartojamas terminas, kurio apibrėžimai yra labai skirtingi, dažnai subjektyvi, o kartais ir neinformatyvūs. Trumpo, plačiai priimtino apibrėžimo nebuvimas, apimančio daugialypį kibernetinį saugumą, kliudo technologinei ir mokslinei pažangai. Sustiprinant daugiausia techninę kibernetinio saugumo požiūrį, atskiria disciplinas, kurios turėtų veikti kartu, siekiant išspręsti sudėtingas kibernetinio saugumo problemas. Taigi mokslininkai skirtingai apibrėžia kibernetinį saugumą ir diskutuoja dėl sąvokos turinio. ***Apibendrinant*** galima laikytis nuomonės, kad kibernetinis saugumas yra veiksmų visumą, kur pasitelkiant į išteklius, bendradarbiavimą, procesus ir struktūras, palaikoma ir apsaugoma kibernetinė erdvė nuo organizuotu kibernetinių atakų, nusikaltimų.

Nagrinėjant kibernetinio saugumo koncepciją, svarbu išanalizuoti kokie veiksniai įtakoja į kibernetinio saugumo užtikrinimą (žr. 2 lent.).

2 lentelė. Kibernetinio saugumo koncepcijos veiksniai

Politikos principai ir veikla	Technologijų charakteristikos	Socialinės naudos
• Pagerintas bendradarbiavimas tarp istitucijų • Tarptautinis bendradarbiavimas • Viešojo ir privataus sektoriaus bendradarbiavimas su įvairiais suinteresuotais subjektais • Lankstumas •Įvairių sričių rizikos modeliai • Gebėjimas spręsti incidentus •Pagrindinių demokratijos vertybių pagrindas • Atskaitomybė • Tinkamo vystymosi ir derinimo teisines sistemas, pvz., siekiant kovoti su elektroniniais nusikaltimais • Savireguliavimas	• Būdingas sudėtingumas • Universalus ryšiai • Bendra infrastruktūra • Pasaulinė sąveika • Atvirumas • Naujų standartų taikymas • Gebėjimas greitai prisitaikyti ir diegti inovacijas	• Stiprus ir platus ekonominis poveikis • Produktyvumo didinimas • Universali ir visame pasaulyje įvairi vartotojų bazė • Greita naudojimo modelių raida • Plati nauda, susijusi su galimybe gauti išsilavinimą, mokymus, bendra informacija •Platus naujo bendravimo modeliai.

Šaltinis: parengta autorės pagal Vishik, Matsubara ir Plonk, 2016

Apibendrinant kibernetinio saugumo koncepciją galima teigti, kad kibernetinis saugumas yra sudėtingas iššūkis, reikalaujantis tarpinstitucinio bendradarbiavimo. Pagrindinis bruožas yra tas, kad atskiros kibernetinio saugumo sudedamosios dalys turi skirtingų savininkų, administratorių, operatorių ir naudotojų. Jie turi savo socialinę naudą, skirtingas technologijas, bet vadovaujasi vieningais politikos principais ir taisyklėmis užtikrinant kibernetinį saugumą. Nesilaikant tokių minimalių saugumo taisyklių, apsaugos metodų ir minimalių saugumo priemonių kibernetinio saugumo srityje ar jų nebuvimo, padidėja naudojamos elektroninės informacijos, ryšių ir kontrolės sistemų pažeidžiamumo lygis.

1.2. Tarpinstitucinio bendradarbiavimo samprata

Tarpinstitucinio bendradarbiavimo poreikis siekiant palaikyti ir stiprinti kibernetinį saugumą yra akivaizdus. Nuolat kintančioje sudėtingoje kibernetinio saugumo aplinkoje vienu iš svarbiausių institucijų prioritetų laikomas bendradarbiavimas. Todėl svarbu užtikrinti, kad Lietuvoje kibernetiniame saugume veikiančios, saugumą užtikrinančios institucijos siektų ir gebėtų veikti kartu. Didelis dėmesys turi būti skiriamas tarpinstituciniam bendradarbiavimui, kuris taptu esmine strategija, siekiant užtikrinti šiuolaikinės visuomenės ir valstybės kibernetinį saugumą. Tarpinstitucinis bendradarbiavimas yra pagrindinis produktyvumo didinimo veiksnys, nes jis sukuria didesnę vertę ir efektyvius rezultatus siekiant bendro tikslo. Iš tiesų tarpinstitucinis bendradarbiavimas yra esminė savybė kuria institucijos siekia savo vidaus departamentuose, suinteresuotosioms šalims ar visoms kitoms organizacijoms. Esančios tarpinstitucinės bendradarbiavimo pastangos labiausiai naudingos norint užtikrinti saugią elektroninę erdvę.

Lietuvoje tarpinstitucinis bendradarbiavimas kibernetinio saugumo srityje yra dar pakankamai nauja tema. Nėra mokslinių straipsnių lietuvių kalba bei tyrimų nagrinėjančių tarpinstitucinio bendradarbiavimo samprata kibernetinio saugumo srityje, sėkmės prielaidas, veiksnius ar problemas. Europos šalių mokslininkai straipsnių, tiesiogiai nagrinėjančių šį temą taip pat nėra paskelbę. Tačiau tiek Lietuvoje, tiek Europos šalyse tarpinstitucinis bendradarbiavimas kibernetinio saugumo srityje yra minimas teisės aktuose.

Tarpinstitucinis bendradarbiavimas ir jų klausimų koordinavimas yra iššūkis Lietuvos viešojo sektoriaus institucijoms. Pagrindinis tarpinstitucinio bendradarbiavimo įrankis Lietuvoje yra tarpinstitucinių programų (veiklos planų) rengimas ir įgyvendinimas. Vienas iš pagrindiniu teisės aktu kuriame akcentuojamas tarpinstitucinis bendradarbiavimas yra Lietuvos Respublikos nutarimas “Dėl vystomojo bendradarbiavimo tarpinstitucinio veiklos plano patvirtinimo“, kurio siekiama stiprinti tarpinstitucinį vystomojo bendradarbiavimo veiklos koordinavimą ir užtikrinti nepertraukiamą ir veiksmingą Lietuvos vystomojo bendradarbiavimo veiklą. Pasak Puškorių (2007) bendradarbiavimas yra ypatingos veiklos rūšys kur veikla atliekama dalyvaujant keliems vykdytojams, valdymo subjektams, institucijoms, sistemoms ar net valstybėms.

Mokslininkės Jurkonienė ir Karčiauskienė (2017) atliktame tyrime nustatė, kad sėkmingam tarpinstituciniam bendradarbiavimui reikalinga ne tik keičiama strateginio planavimo metodika (teisės aktai), tačiau turi būti intensyviai skatinamas neformalus bendradarbiavimas. Taigi tarpinstitucini bendradarbiavimą sudaro ne tik formalus bendradarbiavimas, kuri reglamentuoja procedūros apibrėžtos teisės aktuose, bet ir neformalus bendradarbiavimas, kuris nereglamentuotas ir kur procedūros nėra apibrėžtos teisės aktuose. Išanalizavus mokslinėje literatūroje tarpinstitucinio bendradarbiavimo būdus, galima išskirti du (žr. 3 lent.).

3 lentelė. Tarpinstitucinio bendradarbiavimo būdai

Būdas / Reglamentavimas	Teisės aktai/Tinklai
1. ***Formalus*** bendradarbiavimas / ***reglamentuotas***	***Teisės aktai.*** Nustatyta tvarka reguliuoja ir tvarko.
2.*Neformalus* bendradarbiavimas / ***nereglamentuotas***	***1.Koordinatorių tinklas.*** Paskatina glaudesnį tarpinstitucinį bendradarbiavimą, skatinant neformalią tinklaveiką. Koordinatorių tinklas, neformaliu tinklu orientuotas į neformalaus horizontalaus bendradarbiavimo vystymą, bendradarbiavimo kultūros plėtojimą. Tinklo susitikimuose gvildenamos kiekvienos institucijos problemos, dalijamasi gerosiomis patirtimis, keliamos kompetencijos, stiprinami ryšiai ir bendradarbiavimas, formuojama konsensuso kultūra, informuojama apie kitų institucijų įsipareigojimus ir siekius. Organizuojamų mokymų metu keliamos koordinatorių kompetencijos įvairiais viešojo valdymo klausimais, didelį dėmesį skiriant lyderystei.
	2. Strategų tinklas. Didina institucijų strateginio planavimo ekspertų kompetencijas ir įsitraukia į tarpinstitucinių klausimų sprendimą. Neformalus strategų tinklas leidžia sustiprinti strategų vaidmenį, apibrėžiant horizontalaus pobūdžio problemas ir nustatant jų sprendimo būdus. Dalyvavimas tinkle leidžia įtvirtinti bendrus tarpinstitucinių klausimų sprendimo standartus ir praktikas. Strateginio planavimo ekspertų ankstyvas įsitraukimas į tarpintiticinių klausimų sprendimą sudaro sąlygas atsakingai įvertinti atitinkamų ministerijų indėlį.
	3. Pažangos gildija. Tarpinstitucinių klausimų/problemų sprendimas. Pažangos gildija (savo srities ekspertai, praktikai ir akademikai) jungia savo srities ekspertus, formuojant neformalų žinių ir ekspertizės tinklą. Gildijos veikla nukreipta į realių problemų sprendimą, analizuojant egzistuojančius iššūkius ir įsitraukiant į sprendimų paieškas.

Šaltinis: parengta autorės pagal Jurkonienė ir Karčiauskienė, 2017

Dažniausiai tarpinstitucinis bendradarbiavimas vyksta darbo grupėse, komitetuose, formalių ir neformalių ryšių pagrindu. Neformalus bendradarbiavimas itin svarbus ir skiriasi priklausomai nuo politikos lygmens. Neformalių mechanizmų dėka formalūs susitikimai tampa efektyvesniais, tačiau svarbūs sprendimai tvirtinami oficialioje aplinkoje. Konfliktų sprendimas pradedamas ir dažniausiai užbaigiamas administraciniame lygmenyje, dažniausiai pasitelkiant neformalų bendradarbiavimą, kaip pirmiausią sprendimo būdą. Raišienė konstatuoja, jog esminiai bendradarbiavimo kaip veiklos

organizavimo bruožai yra lankstumas, dalyvavimas ir tarpusavio priklausomybės ryšių horizontalumas (Raišienė, 2015).

Nagrinėjant teorinius aspektus tarpinstitucinio bendradarbiavimo, svarbu išanalizuoti kokie modeliai sudaro bendradarbiavimą. Dėl sudėtingo būdo daugiasluoksnio institucijų bendradarbiavimo, sunku išskirti vyraujančius modelius. Tačiau mokslininkai Smith ir Katz (2000) pateikia tris skirtingus bendradarbiavimo modelius, kurie parodo pagrindinius tarpusavio bendradarbiavimo skirtumus, struktūrą, veikimo būdus (žr. 4 lent.).

4 lentelė. Bendradarbiavimo modeliai

Modelis	Pagrindiniai požymiai	Privalumai
1. Partnerystė	- Formalizuotas tinklas, teikiantis koordinuotą bendrą strategiją plėtrą. - Struktūros skiriasi, bet paprastai gali būti oficialios valdybos ar bendrovės, atsakingos už partnerystės strategijos įgyvendinimas. - Tiksliniai finansavimo šaltiniai: finansavimo įstaigos, mokslinių tyrimų taryba, labdaros organizacijosfondai, Europos fondai, taip pat privataus sektoriaus pramonės finansavimas.	- Institucinių sutelktumas. - Prieiga prie išorinių išteklių. - Gebėjimas strategiškai dirbti. - Sinergijas tarp partnerių. - Teigiamas poveikis bendram tikslui. - Pasiekti misiją ir strategiją. - Nauda bendradarbiaujant su kitais partneriais. - Žmogiškųjų išteklių įgūdžių ugdymas.
2. Komanada	- Bendradarbiavimas orientuotas į apimantį įvairių specialistų sektorius. - Komandos, kuriose dalyvauja universitetai, mokslinių tyrimų centrai, verslo atstovai, vyriausybės institucijos. - Simbioziniai santykiai su finansavimo srautais. - Specialistai orientuoti į rezultatus, problemos ir užduočių sprendimą. - Paprastai struktūrizuojamos ir yra atsakingi už užduočių atlikima.	- Tinkamų įgūdžių, patirties plėtra. - Žinių, supratimo ir mokslinių tyrimų darbotvarkės gerinimas. - Stabilus egzistavimas, tačiau bendradarbiavimas paprastai turi gyvavimo ciklą, kuris apsaugo nuo osifikacijos - Aukštasis universiteto ir vartotojo sąsajos. - Aukšto lygio pažangiausi tyrimai, kurie gali būti naudingi visuomenei. ***4 lentelės tęsinys kitame puslapyje***

3. Aktyvus bendradarbiavimas	- Sėkmingas bendradarbiavimas yra „iš apačios į viršų“, remiantis asmeniniais santykiais, pasitikėjimu ir sugebėjimu dirbti kartu. - Nėra oficialios struktūros bendradarbiavimui, nors dažnai iš pradžių vystosi iš formalaus bendradarbiavimo į glaudžius santykius. - Gyvavimo ciklas gali būti nepaprastai ilgalaikis ir gebantis nuolatos atsinaujanti, kai keičiasi nariai. - Užduotys orientuotos į didelę diskreciją nustatyti, pasiekti tikslus.	- Disciplininio vystymosi raktas – intelektualus smalsumas. - Stipri asmeniniai ir bendri pajėgumus. - Suteikia gyvybingumą, reikalingą tarpinstitucinių tinklų augimui ir išlaikymui. - Didelės asmeninės investicijos į bendradarbiavimo kūrimą.

Šaltinis: parengta autorės pagal Smith ir Katz, 2000

Pateiktuose modeliuose galima matyti, kad institucijų vadovai siekia bendravimo norint užmegzti partnerystės ryšius ir bendradarbiaujant pasiekti nustatytus tikslus. Dauguma institucijų teikia šių modelių variantus. Dažnai visi trys egzistuoja nevienodai ir tarpusavyje persipina. Bendradarbiavimo modeliai supaprastina ir apibendrina bendradarbiavimo veiklos sudėtingumą. Taip pat modeliai apibūdina pagrindines kiekvieno bendradarbiavimo rūšies charakteristikas ir suteikia daugiau galimybių sistemingai vertinti santykius tarp skirtingų institucijų ir atitinkamai jų indėlio siekiant numatyto tikslo.

Tarpinstitucinio bendradarbiavimo koordinavimas yra daug iššūkių keliantis tikslas. Kaip rodo patirtis, tarpinstitucinį bendradarbiavimą varžo institucijų darbo krūvis, tikslų nenuoseklumas, bendravimo ir socialinių įgūdžių stoka, nepakankamai dėmesio skiriama tarpinstituciniams susitikimams. Tarptautiniu mastu stokojama tarpinstitucinių, kompleksinių programų efektyvumo vertinimo. Pasak Guy (1998) tarpinstitucinio bendradarbiavimo koordinavimas gali būti apibūdinamas kaip rezultatas, kuriame dėl jo koordinavimo nebuvimo pasireiškė neigiamos bendradarbiavimo veiklos būsenos (žr. 5 lent.).

5 lentelė. Tarpinstitucinio bendradarbiavimo neigiamos veiklos būsenos

Dubliavimas	Spraga	Nenuoseklumas
Kelios institucijos, padaliniai atlieka tą pačią ar panašią užduotį, funkciją.	Nė viena institucija neatlieka reikalingos užduoties	Skiriasi viešųjų institucijų politiniai tikslai ir jos tarnauja skirtingoms grupėms

Šaltinis: parengta autorės pagal Tarpinstitucinio bendradarbiavimo analizė atlikimo, analogiškos patirties ES šalyse ir esamos teisinės bazės Lietuvoje įvertinimo galutinė ataskaita, 2012

Kaip matome 5 lentelėje neigiamos tarpinstitucinio bendradarbiavimo veiklos rezultatas gali atsirasti dėl institucijų biurokratijos, blogo veiksmų koordinavimo, išteklių trūkumo ir žmogiškųjų išteklių motyvacijos nebuvimas.

Apibendrinant galima teigti, kad formalus bendradarbiavimas yra vienas iš pagrindinių tarpinstitucino bendradarbiavimo būdu, kurio procedūros reglamentuotos ir apibrėžtos teisės aktuose. Tačiau stiprinantis tarpinstitucinį bendradarbiavimą kibernetinio saugumo srityje yra neformalus bendradarbiavimo būdas, kuris paskatina glaudesnį tarpinstitucinį bendradarbiavimą ir neformalia tinklaveiką. Jo koordinavimas yra daug iššūkių keliantis tikslas. Kaip rodo patirtis, tarpinstitucinį bendradarbiavimą varžo institucijų darbo krūvis, tikslų nenuoseklumas, bendravimo ir socialinių įgūdžių stoka, nepakankamai dėmesio skiriama tarpinstituciniams susitikimams, stokojama tarpinstitucinių, kompleksinių programų efektyvumo vertinimo.

1.3. Tarpinstitucinio bendradarbiavimo ypatumai kibernetinio saugumo srityje

Virtualusis pasaulis jungia organizacijos kritine infrastruktūra tiek viešajame, tiek privačiuose sektoriuose. Visame pasaulyje institucijos naudoja ryšių tinklą ir interneto paslaugas savo veiklai ir bendradarbiavimui. Ryšių tinklas įgalina institucijų narius bendradarbiauti tarpusavyje ir prieiti prie interneto. Todėl, be abejonės, sudėtinga kibernetinė ataka, sklindanti iš vieno tinklo segmento gali sukelti krizę, kuri gali paveikti įvairius suinteresuotuosius subjektus tiek institucijose, tiek už jų ribų – privačiame sektoriuje. Taigi, koordinuotas tarpinstitucinis bendradarbiavimas, norint labiau apsaugoti tinklą ir išlaikyti saugų internetą, reikalauja bendrų pastangų.

Tarpinstitucinis bendradarbiavimas Lietuvoje kibernetinio saugumo srityje yra didelis iššūkis. Įvairiose valstybėse taikomi skirtingi politikos koordinavimo modeliai. Jie priklauso nuo strateginio planavimo sistemų, Vyriausybės (politinių) prioritetų, bendradarbiavimo kultūros ir kitų veiksnių. Tarpinstitucinis koordinavimas yra daug iššūkių keliantis tikslas, nes dažniausiai tarpinstitucinį bendradarbiavimą varžo institucijų darbo krūvis, tikslų nenuoseklumas ir nepakankamai teikiama pirmenybė tarp jų, bendravimo ir socialinės rinkodaros įgūdžių stoka, nepakankamai dėmesio skiriama tarpinstituciniams susitikimams. Siekiant įvertinti, kaip sudaromos ir įgyvendinamos tarpinstitucinės programos ir koks tarpinstitucinio bendradarbiavimo modelis yra efektyviausias, galima apžvelgti naudojamus tarpinstitucinio bendradarbiavimo koordinavimo modelius. Taip pat šitie modeliai gali būti naudojami nagrinėti tarpinstitucinio bendradarbiavimo rezultatyvumą ir efektyvumą (žr. 6 lent.).

6 lentelė. Koordinavimo modeliai

Hierarchinis	Vadybinis (rinkos)	Tinklų
- Administravimas grindžiamas hierarchija, rašytinėmis taisyklėmis (svarbiausia koordinavimo priemonė yra teisės aktų projektų derinimas ir jų svarstymas Vyriausybėje).	- Vadyba grindžiama programomis, kurios turi tikslus, priemones, biudžetą, atsakingas institucijas ir asmenis.	- Valdymas grindžiamas įvairių suinteresuotųjų grupių dalyvavimu tinkle, įrodymais apie problemas ir jų sprendimo būdus.

Šaltinis: parengta autorės pagal Tarpinstitucinio bendradarbiavimo analizės atlikimo, analogiškos patirties ES šalyse ir esamos teisinės bazės Lietuvoje įvertinimo galutinė ataskaita, 2012

Remiantis LR Kibernetinio saugumo įstatymu, LR Nacionaliniu kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio veiklos plano patvirtinimo nutarimo ir išnagrinėjus koordinavimo modelius galima daryti išvada, kad Lietuvoje tarpinstituciniame bendradarbiavime kibernetinio saugumo srityje vyrauja mišrus: **hierarchinis/tinklų modelis**. Taigi koordinavimo

priemonė yra teisės aktai, o valdymas grindžiamas suinteresuotųjų grupių tinkle pagal veiklos planą. Teisinis reglamentavimas tarpinstitucinio bendradarbiavimo Lietuvoje kibernetinio saugumo srityje (žr. 7 lent.).

7 lentelė. Tarpinstitucinio bendradarbiavimo reglamentavimas kibernetinio saugumo srityje

Teisės aktai	Tarpinstitucinio bendradarbiavimo veikimo planas
LR Kibernetinio saugumo įstatymas / Nr. XII-1428	IV skyrius. 14 straipsnis. Tarpinstitucinis bendradarbiavimas valdant ir tiriant kibernetinius incidentus.
Nacionalinė kibernetinio saugumo strategija / PATVIRTINTA LR Vyriausybės 2018 m. rugpjūčio 13 d. Nutarimu Nr. 818	32.3. *Trečiasis trečiojo tikslo uždavinys* – skatinti viešojo ir privataus sektorių bei mokslo ir studijų institucijų bendradarbiavimą, kuriant kibernetinio saugumo srities inovacijas. 36.Viešojo ir privataus sektorių bendradarbiavimo įgyvendinimui užtikrinti naudojamas Kibernetinio saugumo informacinis tinklas. 38.1. *Pirmasis ketvirtojo tikslo uždavinys* – gerinti viešojo ir privataus sektorių bendradarbiavimo koordinavimą. Šis uždavinys bus įgyvendinamas kuriant tvarų viešojo ir privataus sektorių bendradarbiavimo kibernetinio saugumo srityje modelį, nustatant atsakomybę ir pajėgumus stiprinant valstybės kibernetinį saugumą, efektyvinant viešojo ir privataus sektorių atstovų keitimąsi aktualia informacija apie kibernetines grėsmes, įvykusius kibernetinius incidentus, išmoktas pamokas, plėtojant ankstyvojo perspėjimo sistemą, kuriant naujus arba tobulinant esamus komunikacijos metodus ir procesus.
Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinis veiklos planas/ PATVIRTINTA LR Vyriausybės 2019 m. liepos 3 d. Nutarimu Nr. 709	2019–2021 m. tikslai, uždaviniai, priemonės, asignavimai ir dalyvaujančios institucijos. Lietuvos Respublikos krašto apsaugos ministerija, Vidaus reikalų ministerija, Lietuvos Respublikos Vyriausybės kanceliarija, Policijos departamentas, Lietuvos Respublikos teisingumo ministerija, Teisingumo ministerija, Lietuvos Respublikos ryšių reguliavimo tarnyba, Lietuvos Respublikos švietimo, mokslo ir sporto ministerija, Lietuvos Respublikos užsienio reikalų ministerija.

Šaltinis: parengta autorės pagal LR teisės aktus, 2019

Kaip matome 7 lentelėje numatytose teisės aktuose ypatingai dėmesys tarpinstituciniam bendradarbiavimui skiriamas valdant ir tiriant kibernetinius incidentus, o būtent trijų institucijų saveika:

Nacionalinio kibernetinio saugumo centro, Lietuvos policijos (Lietuvos kriminalinės policijos biuro Sunkaus ir organizuoto nusikalstamumo 5-oji valdyba) ir Valstybinės duomenų apsaugos inspekcijos. Bendradarbiavimo įgyvendinimui užtikrinti naudojamas kibernetinio saugumo informacinis tinklas. Tačiau kaip kitos institucijos bendradarbiauja nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucini veiklos plane yra nenumatytos, o tiesiog įvardijama kokia institucija už ką yra atsakinga, kur kreiptis esant būtinumui, akcentuojami tikslai, uždaviniai ir priemonės.

Tarpinstitucinio bendradarbiavimo poreikis siekiant palaikyti ir stiprinti kibernetinį saugumą yra akivaizdus. Išnagrinėjus 7 lentelėje teisės aktus reglamentuojančius tarpinstitucinį bendradarbiavimą kibernetinio saugumo srityje galima apžvelgti literatūroje pateiktus tarpinstitucinio bendradarbiavimo principus ir jų ypatumus (žr. 8 lent.)

8 lentelė. Tarpinstitucinio bendradarbiavimo principai

Principas	Specifikacija
Planavimo principas	Skirtingos specializacijos atstovai, vykdantys savo profesines funkcijas, bendradarbiaudami siekia bendro tikslo. Šiam tikslui pasiekti yra kuriami bendri planai, programos, kuriamos priemonės.
Funkcijų ir vaidmenų pasidalinimo principas	Kiekvienas atstovas tarpinstitucinį darbą papildo savo kompetencija ir sprendžia problemas tik savo kompetencijos ribose bei susilaiko nuo sau nebūdingų funkcijų prisiėmimo.
Sisteminio požiūrio principas	Kompleksinis situacijos projektavimas, siekiant konkrečių problemų sprendimo. Įvairių sričių specialistai susirenka tam, kad padėdami vieni kitiems pasiektų tikslą – bendros problemos kompleksinį sprendimą.
Informavimo principas	Bendradarbiaujant sukuriama galimybė susipažinti su kitų institucjų veikla, jos specifika bei kita aktualia informacija ir dalintis svarbia informacija.
Išteklių optimizavimo principas	Derinami skirtingų institucijų/organizacijų/įstaigų veiklos prioritetai, telkiami ir efektyviai išnaudojami žmogiškieji bei materialiniai ištekliai.

Šaltinis: parengta autorės pagal Miginis ir Ulozas, 2014

Apžvelgus tarpinstitucinio bendradarbiavimo principus (8 lent.) ir remiantis teisės aktais reglamentuojančius tarpinstitucinį bendradarbiavimą kibernetinio saugumo srityje galima daryti prielaidą, kad šiuo metu vyrauja **informavimo principas**. Bendradarbiaujant sukuriama galimybė susipažinti su kitų institucjų veikla, jos specifika bei kita aktualia informacija ir dalintis svarbia informacija.

Pagal Lietuvos Respublikos kibernetinio saugumo įstatymo nuostatas, užtikrinant kibernetinį saugumą tarpinstitucinis bendradarbiavimas vyksta tarp Lietuvos Respublikos krašto apsaugos ministerijos, Nacionalinio kibernetinio saugumo centro, Valstybinės duomenų apsaugos inspekcijos, Lietuvos policijos ir kitu institucijų, kurių funkcijos yra susijusios su kibernetiniu saugumu (pavyzdžiui

Ryšių reguliavimo tarnyba, toliau – RRT). Kibernetinio saugumo tarybą analizuoja kibernetinio užtikrinimo būklę Lietuvoje ir teikia pasiūlymus dėl būklės gerinimo. Ją sudaro politiką formuojančių ir įgyvendinančių institucijų nariai, IT verslo atstovai, mokslo ir akademinės bendruomenės atstovai, ypatingos svarbos informacinės infrastruktūros valdytojai, viešųjų ryšių tinklų atstovai ir kt. Tarybai vadovauja Krašto apsaugos ministerijos atstovas (žr. 9 lent.).

9 lentelė. Kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos

Lietuvos Respublikos Vyriausybė Tvirtina planus Formuoja strateginius tikslus ir priemones Steigia Kibernetinio saugumo Tarybą			
Lietuvos Respublikos krašto apsaugos ministerija Formuoja kibernetinio saugumo politiką Organizuoja, kontroliuoja, koordinuoja politikos įgyvendinimą			
Kibernetinio saugumo taryba	**Nacionalinis kibernetinio saugumo centras**	**Valstybinės duomenų apsaugos inspekcija**	**Policija**
- Teikia pasiūlymus dėl kibernetinio saugumo užtikrinimo būklės gerinimo. - Analizuoja kibernetinio saugumo užtikrinimo tobulinimo tendencijas. - Teikia kibernetinio saugumo dalyviams rekomendacijas dėl kibernetinio saugumo stiprinimo.	- Įgyvendina kibernetinio saugumo politiką. - Atlieka rizikos kibernetinėje erdvėje bei kibernetinių incidentų analizę. - Diegia ir valdo technines kibernetinio saugumo priemones valstybės informaciniuose ištekliuose ir ypatingos svarbos informacinėse infrastruktūrose. - Duoda nurodymą viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjui. - Bendradarbiauja su tarptautinių organizacijų kompetentingomis institucijomis.	- Įgyvendina kibernetinio saugumo politiką asmens duomenų apsaugos srityje.	- Vykdo kibernetinių incidentų, galimai turinčių nusikalstamų veikų požymių, užkardymą ir atlieka jų tyrimą. - turi teisę, be teismo sankcijos duoti nurodymą viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjui, elektroninės informacijos prieglobos paslaugų teikėjui ir skaitmeninių paslaugų teikėjui. - 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

Šaltinis: parengta autorės pagal LR Kibernetinio saugumo įstatymą, 2018

Vienas iš pagrindinių tarpinstitucinio bendradarbiavimo ypatumu yra informacijos keitimasis. Nacionalinis kibernetinio saugumo centras yra viena iš pagrindiniu informacijos keitimosi institucijų, kurios pagrindinis tikslas yra informacijos apie kibernetinius incidentus dalijimasis ir bendradarbiavimas tarp kibernetinio saugumo informacinio tinklo narių. "Kibernetinio saugumo informacinio tinklo paskirtis – dalytis informacija apie galimus ir įvykusius kibernetinius incidentus, taip pat rekomendacijomis, nurodymais, techniniais sprendimais ir kitomis priemonėmis, užtikrinančiomis kibernetinį saugumą ir kibernetinio saugumo informacinio tinklo narių tarpusavio bendradarbiavimą kibernetinio saugumo srityje (Lietuvos Respublikos kibernetinio saugumo įstatymas, 2018). Subjektai, kurie atitinka Kibernetinio saugumo informacinio tinklo nuostatuose nurodytus reikalavimus gali sužinoti skelbiama aktualia kibernetinio saugumo subjektų paskirtų asmenų, padalinių, atsakingų už kibernetinio saugumo organizavimą ir kibernetinių incidentų valdymą, kontaktinė informacija.

Tarpinstitucinis bendradarbiavimas valdant ir tiriant kibernetinius incidentus vyksta tarp Nacionalinio kibernetinio saugumo centro, policijos ir Valstybinės duomenų apsaugos inspekcijos (žr. 10 lent.).

10 lentelė. Tarpinstitucinis bendradarbiavimas valdant ir tiriant kibernetinius incidentus

Nacionalinis kibernetinio saugumo centras	
Lietuvos Policija	**Valstybinė duomenų apsaugos inspekcija**
Konsultuojasi ir bendradarbiauja tiriant kibernetinius incidentus, keičiasi su kibernetinių incidentų tyrimu susijusia informacija, reikalinga pagal kompetenciją šių institucijų funkcijoms atlikti. Prireikus apie kibernetinių incidentų tyrimą gali būti pranešama kitiems kriminalinės žvalgybos subjektams ir (arba) žvalgybos institucijoms.	***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.

Šaltinis: parengta autorės pagal LR Kibernetinio saugumo įstatymą, 2018

Kaip matome 10 lentelėje tarpinstitucinis bendradarbiavimas tarp Nacionalinio kibernetinio saugumo centro, Lietuvos policijos ir Valstybinės duomenų apsaugos inspekcijos bendradarbiavimas vyksta tiriant kibernetinius incidentus, apsikeičiant aktualią informaciją. Nacionalinis kibernetinio saugumo centras (toliau – NKSC) prie Krašto apsaugos ministerijos (toliau – KAM) yra pagrindinė Lietuvos kibernetinio saugumo institucija, atsakinga už vieningą kibernetinių incidentų valdymą, kibernetinio saugumo reikalavimų įgyvendinimo stebėseną ir kontrolę, ypatingos svarbos informacinės

infrastruktūros kibernetinį saugumą ir informacinių išteklių akreditaciją. Keitimasis informacija yra vienas iš pagrindiniu veiksniu tarpinstituciniame bendradarbiavime. Patvirtintuose NKSC nuostatuose yra numatyti šie pagrindiniai institucijos veiklos tikslai:

- įgyvendinti nacionalinę kibernetinio saugumo politiką;
- atlikti Saugumo priežiūros tarnybos funkcijas;
- atlikti Nacionalinės komunikacijų apsaugos tarnybos funkcijas;
- vykdyti informacijos sklaidos, tyrimų ir analizės kibernetinio saugumo klausimais veiklą.

Nuo 2018 m. pradžios Nacionalinis kibernetinio saugumo centras „vieno langelio "(vieną patogią fizinę ar elektroninę vietą, kur galima gauti visas ar dalį institucijų teikiamų viešąsias/administracines paslaugas) principu teikia pagalbą valstybės institucijoms, verslui ir gyventojams. NKSC savo kompetencijos ribose drauge su valstybės įstaigomis ir organizacijomis bei kitais ūkio subjektais sprendžia valstybės informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros kibernetinio saugumo klausimus. Tarpinstitucinio bendradarbiavimo valdant ir tiriant kibernetinius incidentus tvarka nustatoma Nacionaliniame kibernetinių incidentų valdymo plane.

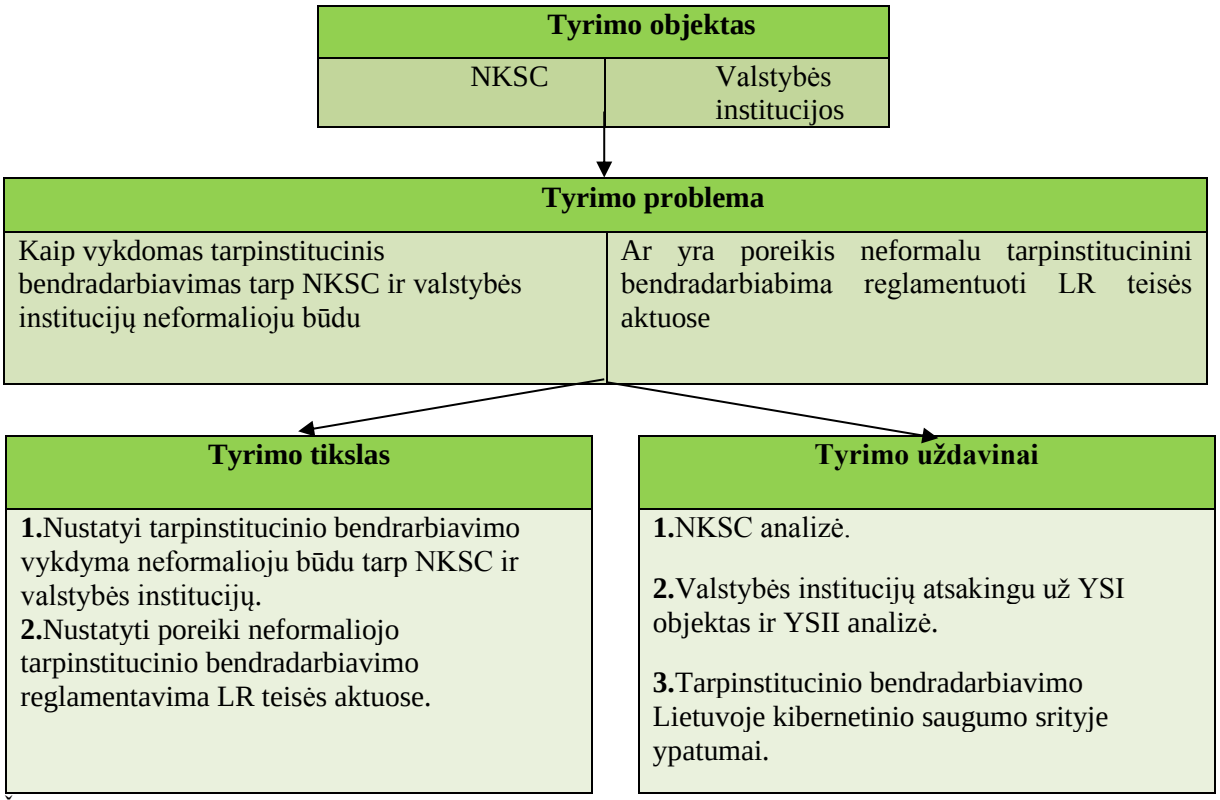
Apibendrinant galima teigti, kad pagrindinis ir esminis ypatumas tarpinstituciniame bendradarbiavime kibernetinio saugumo srityje yra visavertė partnerystė grindžiama informacijos keitimusi. Šiuo metu vyrauja **informavimo principas** kur bendradarbiaujant sukuriama galimybė susipažinti su kitų institucjų veikla, jos specifika bei kita aktualia informacija ir dalintis svarbia informacija. Nacionalinis kibernetinio saugumo centras yra viena iš pagrindiniu informacijos keitimosi institucijų, kurios pagrindinis tikslas yra informacijos apie kibernetinius incidentus dalijimasis ir bendradarbiavimas tarp kibernetinio saugumo informacinio tinklo narių. Kitos institucijos tik nukreipiamos incidento atveju. Apie jų bendradarbiavimą teisės aktuose nėra numatyta. Lietuvoje tarpinstituciniame bendradarbiavime kibernetnio saugumo srityje vyrauja **mišrus: hierarchinis/tinklų modelis**. Koordinavimo priemonė yra teisės aktai, o valdymas grindžiamas suinteresuotųjų grupių tinkle pagal veiklos planą. Tarpinstitucinio bendradarbiavimo valdant ir tiriant kibernetinius incidentus tvarka nustatoma Nacionaliniame kibernetinių incidentų valdymo plane.

2.TARPINSTITUCINIO BENDRADARBIAVIMO KIBERNETINIO SAUGUMO SRITYJE TYRIMO METODOLOGIJA

2.1. Tarpinstitucinio bendradarbiavimo kibernetinio saugumo srityje tyrimo modelis

Metodinėje darbo dalyje buvo pastebėta, jog teisės aktuose nėra išsamiai reglamentuotas tarpinstitucinis bendradarbiavimas įvairiais lygiais. Sėkmingam tarpinstituciniam bendradarbiavimui reikalinga ne tik keičiama strateginio planavimo metodika (teisės aktai), tačiau turi būti intensyviai skatinamas neformalus bendradarbiavimas, kuri sudaro ne tik formalus bendradarbiavimas reglamentuojamas procedūromis apibrėžtomis teisės aktuose, bet ir neformalus bendradarbiavimas, kuris nereglamentuotas ir procedūros nėra apibrėžtos teisės aktuose. Šioje srityje rizikos elementų daugėja. Todėl nuolat kintančioje kibernetinio saugumo aplinkoje vienu iš svarbiausių prioritetų laikomas tarpinstitucinis bendradarbiavimas.

Atsižvelgiant į tai, kad nėra pakankamai ištyrinėtas tarpinstitucinis bendradarbiavimas kibernetinio saugumo srityje, kuris lemia kibernetinio saugumo užtikrinimą, pasirinkta tyrimo tema – Tarpinstitucinio bendradarbiavimo Lietuvoje kibernetinio saugumo srityje vertinimas.



Šaltinis: sudaryta autorės

1 pav. Tyrimo modelis

Tyrimo objektas – Nacionalinio kibernetinio saugumo centras (toliau NKSC) ir valstybės institucijos atsakingos už ypatingos svarbos infrastruktūros objektus (toliau YSI objektas) ir ypatingos svarbos informacinę infrastruktūrą (toliau YSII).

Tyrimo problema – nėra aiškių kriterijų, kuriais remiantis vertinti tarpinstitucinį bendradarbiavimą kibernetinio saugumo srityje:

1) Kaip vykdomas tarpinstitucinis bendradarbiavimas tarp NKSC ir valstybės institucijomis;
2) Ar yra poreikis neformalu tarpinstitucini bendradarbiavimą reglamentuoti LR teisės aktuose.

Tyrimo hipotezė – poreikis reglamentuoti Lietuvos Respublikos teisės aktuose neformalųjį tarpinstitucinį bendradarbiavimą kibernetinio saugumo srityje.

Tyrimo tikslas – išnagrinėjus mokslinius požiūrius, praktinius aspektus į tarpinstitucinį bendradarbiavimą kibernetinio saugumo srityje ir parengus tyrimo modelį, metodologiją ištirti ir apibrėžti Lietuvos tarpinstitucinio bendradarbiavimo kibernetinio saugumo srityje ypatumus.

Tyrimo uždaviniai- tikslui pasiekti darbe sprendžiami uždaviniai:

1) Išanalizuoti Nacionalinio kibernetinio saugumo centro (toliau NKSC) tarpinstitucinio bendradarbiavimo formavimo procesus su kitomis Lietuvos valstybės institucijomis kibernetinio saugumo srityje;
2) Išanalizuoti valstybės institucijų atsakingu už ypatingos svarbos infrastruktūros objektus ir ypatingos svarbos informacinės infrastruktūros tarpinstitucinio bendradarbiavimo formavimo procesus su NKSC užtikrinant kibernetinį saugumą YSI objektu ir YSII;
3) Nustatyti tarpinstitucinio bendradarbiavimo Lietuvoje kibernetinio saugumo srityje ypatumus ir vyraujančius tarpinstitucinio bendradarbiavimo būdus.

Tyrimo imtis:

NKSC. Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (NKSC) yra pagrindinė Lietuvos kibernetinio saugumo institucija, atsakinga už vieningą kibernetinių incidentų valdymą, kibernetinio saugumo reikalavimų įgyvendinimo stebėseną ir kontrolę, ypatingos svarbos informacinės infrastruktūros kibernetinį saugumą ir informacinių išteklių akreditaciją.

Valstybės institucijos. Tyrimo metu remiantis LR nutarimu dėl ypatingos svarbos informacinės infrastruktūros identifikavimo metodikos patvirtinimu (2016 m. liepos 20 d. Nr. 742) buvo parinktas valstybės institucijų sąrašas atsakingu už ypatingos svarbos infrastruktūros objektus ir ypatingos svarbos informacinės infrastruktūros, nuo kurių priklauso kertinės valstybės funkcijos. Jų nepasiekiamumas gali turėti skaudžių pasekmių visos visuomenės saugumui, ekonomikai ir gerbūviui. Taigi pagal LR kibernetinio saugumo įstatymą**, ypatingos svarbos informacinė infrastruktūra (YSII)** tai yra elektroninių ryšių tinklas ar jo dalis, informacinė sistema ar jos dalis, informacinių sistemų grupė ar pramoninių procesų valdymo sistema ar jos dalis, nepaisant to, ar jos valdytojas yra privatus ar viešojo administravimo subjektas, kuriuose įvykęs kibernetinis incidentas gali padaryti didelę žalą

nacionaliniam saugumui, šalies ūkiui, valstybės ir visuomenės interesams. Remiantis LR Vyriausybės nutarimu dėl ypatingos svarbos informacinės infrastruktūros identifikavimo metodikos patvirtinimo, **ypatingos svarbos infrastruktūros objektas (YSI objektas)** tai yra institucija ar jos struktūrinis padalinys, įmonė, įrenginys ar įrenginio dalis, nepaisant to, ar jo valdytojas yra privatus ar viešojo administravimo subjektas, teikiantis ypatingos svarbos paslaugas, kurio neveikimas ar veiklos sutrikdymas gali padaryti didelę žalą nacionaliniam saugumui, šalies ūkiui, valstybės ar visuomenės interesams. Tyrimo metu bus nagrinėjamos dešimt valstybės institucijų sąrašų**:**

1. Lietuvos Respublikos aplinkos ministerija;
2. Lietuvos Respublikos energetikos ministerija;
3. Lietuvos Respublikos finansų ministerija;
4. Lietuvos Respublikos susisiekimo ministerija;
5. Lietuvos Respublikos sveikatos apsaugos ministerija;
6. Lietuvos Respublikos ūkio ministerija;
7. Lietuvos Respublikos užsienio reikalų ministerija;
8. Lietuvos Respublikos vidaus reikalų ministerija;
9. Lietuvos Respublikos žemės ūkio ministerija;
10. Lietuvos Respublikos Vyriausybės kanceliarija.

Remiantis LR teisės aktais vis dar nėra paskelbtas LR YSI objektų, YSII sąrašas ir už jos atsakingų valstybės institucijų. Nuo 2018 m. liepos 5 d. yra derinamas LR vyriausybės nutarimo projektas dėl Lietuvos Respublikos ypatingos svarbos infrastruktūros objektų, ypatingos svarbos technologijų, ypatingos svarbos išteklių tiekimo saugumo, neskelbtinos informacijos ir gebėjimo kontroliuoti neskelbtiną informaiją, kuriame turi būti pridedamas Lietuvos Respublikos ypatingos svarbos infrastruktūros objektų, ypatingos svarbos technologijų sąrašas.

Metodinėje darbo dalyje buvo nustatyta, jog egzistuoja du tarpinstitucinio bendradarbiavimo būdai. Vienas yra **formalus bendradarbiavimas** reglamentuotas teisės aktais ir **neformalus bendradarbiavimas** – nereglamentuotas teisės aktais. Mokslininkai pabrėžia, kad sėkmingam tarpinstituciniam bendradarbiavimui turi būti intensyviai skatinamas neformalus bendradarbiavimas. Siekiant įvertinti tarpinstitucinį bendradarbiavimą Lietuvoje kibernetinio saugumo srityje buvo apžvelgti Nacionalinio kibernetinio saugumo centro ir valstybės institucijų bendradarbiavimo formavimo sąlygojantys veiksniai, kurie yra reikalingi atlikti empirinio tyrimo uždavinius. Tai yra:

1) Išanalizuoti Nacionalinio kibernetinio saugumo centrą (toliau NKSC);
2) Išanalizuoti valstybės institucijos atsakingos už ypatingos svarbos infrastruktūros objektus ir ypatingos svarbos informacinės infrastruktūros;
3) Tarpinstitucinis bendradarbiavimas Lietuvoje kibernetinio saugumo srityje ypatumai.

Siekiant suprasti tiriamuosius reiškinius bei pateikti interpretacinį, holistinį (ne kaip atskirų kintamųjų pasekmė) bet kaip Lietuvos valstybinių institucijų bendradarbiavimo visumą ir Nacionalinio kibernetinio saugumo centro bendradarbiavimo formavimo patirtį buvo pasitelkta į empirinio tyrimo metodus.

Tyrimo metodika. Analizuojant tarpinstitucinį bendradarbiavimą kibernetinio saugumo srityje buvo naudota sisteminė, apibendrinimo, lyginamoji, turinio ir aprašomoji mokslinės literatūros analizė, loginis analitinis metodas bei teisės dokumentų turinio analizė, kurios tikslas buvo atskleisti kibernetinio saugumo tarpinstitucinio bendradarbiavimo ypatumus Lietuvoje (žr. 11 lent.).

11 lentelė. Empirinio tyrimo metodai

Tyrimo metodas	Naudojimo tikslas
Dokumentų analizės metodas	Pasitelkiant dokumentų analizės metodu renkami duomenys bus tekstai, teisės aktai, veiklos ataskaitos, reglamentavimai, kurie atliekame darbe naudojami kaip pagrindiniai informacijos šaltiniai. Metodo pagalba analizuojama NKSC ir valstybinių institucijų bendradarbiavimo formavimo sąlygojantys veiksniai. Dokumentų analizės metodas bus vienas iš pagrindinio empirinio tyrimo matmeniu, kuris sujungs teorinę ir analitinės tyrimo dalys. Šis metodas bus naudojamas tiriant tarpinstitucinio bendradarbiavimo Lietuvoje kibernetinio saugumo srityje ypatumus kartu siekiant identifikuoti neformalaus tarpinstitucinio bendradarbiavimo būdo egzistenciją.
Loginis analitinis metodas	Loginio analitinio metodo pagalba bus siekiama sukonkretinti, suprasti, įvertinti tarpinstitucinį bendradarbiavimą Lietuvoje kibernetinio saugumo srityje ir atskleisti jo naudą.
Sisteminės analizės metodas	Pasitelkiant į sisteminės analizės metodo pagalbą bus nagrinėjamas bendradarbiavimas Lietuvos valstybės institucijų kaip kibernetinio saugumo dalis. Taip pat atskleista kaip ir kokiu bendradarbiavimo būdu valstybės istitucijos sąveikauja tarpusavyje užtikrinant kibenetinį saugumą ir tai savo ruožtu leis išryškinti kompleksinį tyrimo objekto charakterį.

Šaltinis: parengra autorės

Analizė bus pasitelkta į tarpinstitucinio bendradarbiavimo formavimo procesus būtent neformaliuoju būdu, kadangi šis bendradarbiavimo būdas gali padėti efektyviai ir laiku identifikuoti kibernetinius incidentus, užkirsti kelią jų atsiradimui, plitimui, valdyti kibernetinių incidentų sukeltas pasekmes. Neformalaus tarpinstitucinio bendradarbiavimo poreikis norint palaikyti ir stiprinti kibernetinį saugumą yra aktualus. Siekiant garantuoti galimybę visuomenei saugiai naudotis informacinių ir ryšių technologijų teikiamomis galimybėmis, tarpinstitucinis bendradarbiavimas tampa būtina sąlyga visapusiškam kibernetiniam saugumui užtikrinti.

Medžiaga ir metodai: mokslinės literatūros analizė, ekspertinio tyrimo duomenų analizė ir teisinių dokumentų analizė.

2.2. Tarpinstitucinio bendradarbiavimo kibernetinio saugumo srityje tyrimo metodikos pagrindimas

Tarpinstitucinio bendradarbiavimo Lietuvoje kibernetinio saugumo srityje empirinis tyrimas, susideda iš trijų etapu. Kiekviename etape tam, kad tyrimas vyktu kryptingai buvo iškelti tikslai ir parinktos vertinimo priemonės ir kriterijai (žr. 12 lent.).

12 lentelė. Tarpinstitucinio bendradarbiavimo kibernetinio saugumo srityje empirinio tyrimo etapai

Etapai	Tikslai	Apimtis, rodikliai
1.NKSC tarpinstitucinio bendradarbiavimo formavimo procesų analizė	1.Išanalizuoti NKSC tarpinstitucinio bendradarbiavimo formavimo pricesų ypatumus 2.Išanalizuoti NKSC tarpinstitucinio bendradarbiavimo skatinančios priemonės	-Teisinis reglamentavimas; -Nuostatai; - Veiklos ataskaitos.
2.Valstybės institucijų bendradarbiavimo formavimo procesų analizė	1.Išanalizuoti valstybės institucijų bendradarbiavimo formavimo procesų ypatumus kibernetinio saugumo srityje 2.Išanalizuoti valstybės institucijų bendradarbiavimo skatinančios priemonės	1. LR aplinkos ministerija; 2. LR energetikos ministerija; 3. LR finansų ministerija; 4. LR susisiekimo ministerija; 5. LR sveikatos apsaugos ministerija; 6. LR ūkio ministerija; 7. LR užsienio reikalų ministerija; 8. LR vidaus reikalų ministerija; 9. LR žemės ūkio ministerija; 10. LR Vyriausybė; 11. LR teisingumo ministerija; 12. LR krašto apsaugos ministerija.
3.Tarpinstitucinio bendradarbiavimo Lietuvoje kibernetinio saugumo srityje ypatumai	1.Išanalizuoti tarpinstitucinio bendradarbiavimo ypatumus ir nustatyti vyraujantį taristitucinį bendradarbiavimo būdą Lietuvoje kibernetinio saugumo srityje	- NKSC (ekspertas) -Valstybės institucijos, atsakingos už YSI objektus ir YSII (atsakingas asmuo).

Šaltinis: parengta autorės

Pirmame etape bus analizuojami NKSC tarpinstitucinio bendradarbiavimo ypatumai ir skatinančios priemonės pasitelkiant į teisini reglamentavimą ir veiklos ataskaitos.

Antrame etape bus analizuojamos dvylika institucijų atsakingu už ypatingos svarbos infrastruktūros objektus ir ypatingos svarbos informacinė infrastruktūra tarpinstitucinio bendradarbiavimo ypatumai ir skatinančios priemonės pasitelkiant į institucijų veiklos planus ir bendra teisinį reglamentavimą.

Trečiame etape:

1. ***Siekiant nustatyti tarpinstitucinį bendradarbiavimą NKSC su kitomis valstybės institucijomis*** bus panaudotas ekspertų vertinimo metodas. Ekspertų metodas pasirinktas, siekiant pateikti kokiu būdu formaliuoju ar neformaliuoju NKSC ir valstybės institucijos vykdo tarpinstitucinį bendradarbiavimą. Ekspertinė apklausa padės tiesiogiai išsiaiškinti sėkmingiausia tarpinstitucinio bendradarbiavimo būdą, nes pasak Tidiko (2003) ekspertas yra asmuo, kuris dėl savo profesinės patirties turi didžiausią kompetenciją ir patikimiausią bei pakankamai išsamią informaciją apie tiriamą problemą.

Pastaruoju metu vienas populiariausių empirinio tyrimo metodų yra apklausa. Ekspertiniam vertinimui pasirinktas metodas – ***apklausos anketavimo būdu***. Remiantis Cohen, Manion ir Morrison (2007) yra manoma, kad tinkamai anketai būdingos tokios savybės, kaip aiškumas, nedviprasmiškumas, patikimumas kuri tuo pačiu turi skatinti eksperto norą bendradarbiauti. Anketavimas yra standartizuotas metodas su griežtomis taisyklėmis. Anketa sudaryta ir iš atvirų klausimų kurie skirti norint išgryninti ekspertų nuomonę. Klausimai tarpusavyje susijusę ir į kuriuos reikia gauti apklausiamų respondentų atsakymus. Taigi apklausa vyks raštu sudarant anketavimą. Šio tipo apklausose ekspertui elektroniniu paštu siunčiamas klausimynas anketa ir prašoma ją užpildyti. Šiame tyrime ekspertų bus paprašyta atsakyti į žemiau pateiktus klausimus (žr. 13 lent.).

13 lentelė. Klausimynas NKSC ekspertų apklausti

Nr.	Klausimas	Tikslas
1.	***Ar vykdote tarpinstitucinį bendradarbiavimą su valstybės institucijomis atsakingomis už YSI objektus ir YSII?***	Nustatyti ar vyksta tarpinstitucinis bendradarbiavimas su valstybės institucijomis.
2.	***Kokiais atvejais vykdote tarpinstitucini bendradarbiavimą su valstybės institucijomis atsakingomis už YSI objektus ir YSII?***	Nustatyti kokiais atvejais vyksta tarpinstitucinis bendradarbiavimas užtikrinant kibernetinį saugumą.
3.	***Kokiais būdais vykdote tarpinstitucinį bendradarbiavimą: formaliuoju (reglamentuoja teisės aktai), neformaliuoju (pagal poreikį, nereglamentuojamas) ar mišriuoju?***	Nustatyti vyraujanti tarpinstitucinio bendradarbiavimo būdą.
4.	***Kaip dažnai vykdote tarpinstitucinį bendradarbiavimą su valstybės institucijomis atsakingomis už YSI objektus ir YSII?***	Nustatyti tarpinstitucinio bendradarbiavimo dažnumą.

13 lentelės tęsinys kitame puslapyje

5.	***Kokiomis priemonėmis vykdote tarpinstitucinį bendradarbiavimą: jeigu vykdote formaliuoju būdu*** *(susitikimai, el. paštas, telefonu, konferencijos, mokymai, vaizdo pokalbiai ar kita-nurodyti)* ***jeigu vykdote neformaliuoju būdu*** *(susitikimai, el. paštas, telefonu, konferencijos, mokymai, vaizdo pokalbiai ar kita- nurodyti)****?***	Nustatyti vyraujančia priemonę vykstančiame tarpinstituciniame bendradarbiavime.
6.	***Jeigu nevykdote neformaliuoju būdu tarpinstitucinio bendradarbiavimo tai Jūsų nuomonė toks bendradarbiavimo būdas yra naudingas LR užtikrinant kibernetinį saugumą? Pagrįskite savo atsakymą.***	Nustatyti naudą tarpinstitucinio bendradarbiavimo neformaliuoju būdu.
7.	***Jūsų nuomonė ar yra poreikis reglamentuoti neformalųjį būdą tarpinstitucinio bendradarbiavimo LR teisės aktuose?***	Nustatyti poreikį neformaliojo būdo reglamentavimą LR teisės aktuose.

Šaltinis: parengta autorės

Remiantis pagal Kardelį (2002) bendraisiais anketos reikalavimas buvo panaudoti ***aprašomieji klausimai***. Tokie klausimai dažniausiai reikalauja duomenų, apibūdinančių tiriamą sistemą. Tyrimo metu tiriant tarpinstitucinį bendradarbiavimą kibernetinio saugumo srityje aprašomieji klausimai padės atskleisti vykstančius procesus, susijusius su tarpinstitucinių bendradarbiavimų ir nustati kokių būdu jis vykdomas. Klausimai sudaryti motyvuotai, yra konkretūs, logiškai paaiškina dėl ko atliekamas tyrimas, todėl eksperto pastangos atsakyti į klausimus yra minimalios.

Analizuojant eksperto apklausos rezultatus pasitelkiama į turinio analizės metodą:

1) vertinami eksperto atsakymai ir išskiriami esminiai aspektai, remiantis išskirtais raktiniais žodžiais;
2) atliekamas elementų identifikavimas;
3) prasminių priemonių suskirstymas į kategorijas;
4) išskiriami principai ir būdai;
4) turinio duomenų interpretavimas.

Tyrimui naudojamos apklausos formos pateiktos 1 priede.

2. Siekiant nustatyti tarpinstitucinį bendradarbiavimą valstybės institucijų atsakingu už YSI objektus ir YSII su NKSC bus taip pat bus panaudotas ekspertų vertinimo metodas ir pasirinktas – ***apklausos anketavimo būdas.*** Anketa sudarys uždari ir atviri klausimai kurių pagalbą bus norima išgryninti ekspertų nuomonę. Klausimai tarpusavyje susiję ir į kuriuos reikia gauti apklausiamų respondentų atsakymus. Pasak Kardelį (2002) kuo mažiau respondentui tenka rašyti, tuo daugiau jis tiki, kad bus išlaikytas anonimiškumas. Anketa su uždarais klausimais buvo sudaryta remiantis Kardelio (2002) bendrais anketos reiklavimais kur didelis dėmesys nukreiptas į apimtį, nes didelė apimtis respondentą atbaido ir iš anksto nustato atmestinį anketos pildymą, apipavidalinimą, klausimų kompoziciją (paprastumas, aiškumas, tikslumas). Taigi apklausa vyks raštu per internetą. Šio tipo

apklausose ekspertui elektroniniu paštu siunčiamas klausimynas ir prašoma jį užpildyti. Šiame tyrime ekspertų bus paprašyta atsakyti į žemiau pateiktus klausimus (žr. 14 lent.).

14 lentelė. Klausimynas valstybės institucijų ekspertų apklausti

Nr.	Klausimas	Tikslas
1.	***Ar vykdote tarpinstitucinį bendradarbiavimą su NKSC?*** *a)* ***taip*** *b)* ***ne***	Nustatyti ar vyksta tarpinstitucinis bendradarbiavimas kibernetinio saugumo srytyje.
2.	***Kaip vykdote tarpinstitucinį bendradarbiavimą su NKSC?*** ***a) formaliuoju būdu*** ***b) neformaliuoju būdu*** ***c) mišriu (derinant formalųjį ir neformalųjį bendradarbiavimo būdą)***	Nustatyti vyraujanti tarpinstitucinio bendradarbiavimo būdą kibernetinio saugumo srityje.
3.	***Kokiais atvejais vykdomas tarpinstitucinis bendradarbiavimas su NKSC formaliuoju būdu?*** ***a) incidentų atvejais*** ***b) prevenciškai*** ***c) mokymai*** ***d) kiti (nurodyti konkrečius atvejus)***	Nustatyti vyraujanti atvejį tarpinstitucinio bendradarbiavimo formaliuoju būdu.
4.	***Kokiomis priemonėmis vykdote tarpinstitucinį bendradarbiavimą formaliuoju būdu su NKSC?*** ***a) susitikimai*** ***b) telefono pokalbiai*** ***c) el. paštu*** ***d) kitos priemonės (nurodyti konkrečias priemonės)***	Nustatyti vyraujanti priemonė tarpinstitucinio bendradarbiavimo formaliuoju būdu.
5.	***Kaip dažnai vykdomas tarpinstitucinis bendradarbiavimas formaliuoju būdu su NKSC?*** ***a) 1-3 mėn*** ***b) 3-6 mėn*** ***c) 6-12 mėn*** ***d) 12 mėn. ir daugiau***	Nustayti laiko intervalą ir dažnumą tarpinstitucinio bendradrbiavimo formaliuoju būdu.
6.	***Kokiais atvejais vykdomas tarpinstitucinis bendradarbiavimas su NKSC neformaliuoju būdu?*** ***a) incidentų atvejais*** ***b) prevenciškai*** ***c) mokymai*** ***d) kiti (nurodyti konkrečius atvejus)***	Nustatyti vyraujanti atvejį tarpinstitucinio bendradarbiavimo formaliuoju būdu. ****14 lentelės tęsinys kitame puslapyje***

7.	***Kokiomis priemonėmis vykdote tarpinstitucinį bendradrbiavimą neformaliuoju būdu su NKSC?*** ***a) susitikimai*** ***b) telefono pokalbiai*** ***c) el. paštas*** ***d) kitos priemonės (nurodyti konkrečias priemonės)***	Nustatyti vyraujanti priemonė tarpinstitucinio bendradarbiavimo formaliuoju būdu.
8.	***Kaip dažnai vykdomas tarpinstitucinis bendradarbiavimas neformaliuoju būdu su NKSC?*** ***a) 1-3 mėn*** ***b) 3-6 mėn*** ***c) 6-12 mėn*** ***d) 12 mėn. ir daugiau***	Nustatyti laiko intervalą ir dažnumą tarpinstitucinio bendradarbiavimo neformaliuoju būdu.
9.	***Jūsų nuomonė ar tarpinstitucinio bendradarbiavimo kokybė su NKSC tenkina Jūsų poreikius?*** ***a) tenkina*** ***b) netenkina*** ***c) iš dalies tenkina***	Nustatyti valstybės institucijų tarpinstitucinio bendradrabiavime su NKSC kokybės rodiklį.
10.	***Jūsų nuomonė ar yra poreikis reglamentuoti neformalią būdą tarpinstitucinio bendradarbiavimo LR teisės aktuose užtikrinant kibernetinį saugumą?***	Atskleisti valstybės institucijų poreikį nefarmliuoju būdo tarpinstitucinio bendradrbiavimo reglamentavimą LR teisės aktuose užtikrinant kibernetinį saugumą.

Šaltinis: parengta autorės

Analizuojant valstybės institucijų eksperto apklausos rezultatus bus pasitelkta į turinio analizės metodą:

1) vertinami eksperto atsakymai ir išskiriami esminiai aspektai, remiantis išskirtais raktiniais žodžiais;

2) atliekamas elementų identifikavimas;

3) prasminių priemonių suskirstymas į kategorijas;

4) išskiriami principai ir būdai;

4) turinio duomenų interpretavimas.

Tyrimui naudojamos apklausos formos pateiktos 2 priede.

Formuojant anketos uždarius ir atvirus klausimus buvo stengiamasi, kad eksperto pastangos atsakyti būtų minimalios, o klausimai būtų konkretūs su suprantamais atsakymų variantais. Tinkamai suformuota anketos apimtis kuri sudaryta iš 7 – 10 klausimų leidžia ekspertui noriai pateikti atsakymus į klausimus. Taip pat buvo išlaikytas respondentų anonimiškumas.

Medžiaga ir metodai: Mokslinės literatūros analizė, ekspertinio tyrimo duomenų analizė ir teisinių dokumentų analizė.

3. TARPINSTITUCINIO BENDRADARBIAVIMO LIETUVOJE KIBERNETINIO SAUGUMO SRITYJE ANALIZĖ

3.1. NKSC tarpinstitucinio bendradarbiavimo formavimo procesų analizė

Nacionalinis kibernetinio saugumo centras (toliau NKSC) yra pagrindinė Lietuvos kibernetinio saugumo institucija, atsakinga už:

- ✓ vieningą kibernetinių incidentų valdymą;
- ✓ kibernetinio saugumo reikalavimų įgyvendinimo stebėseną;
- ✓ kontrolę;
- ✓ informacinių išteklių akreditavimą;
- ✓ ypatingos svarbos informacinės infrastruktūros valdytojų ir kitų kibernetinio saugumo subjektų kibernetinio saugumo užtikrinimą.

Remiantis NKSC prie Krašto apsaugos ministerijos (toliau KAM) nuostatais galima išskirti ***pagrindinius NKSC veiklos tikslus ir funkcijos*** kuriais pagalbą NKSC įgyvendina nacionalinę kibernetinio saugumo politiką, atlieka Saugumo priežiūros tarnybos ir Nacionalinės komunikacijų apsaugos tarnybos funkcijas,

vykdo informacijos sklaidos, tyrimų ir analizės kibernetinio saugumo klausimais veiklą. Pagal savo kompetenciją rengia, teikia pasiūlymus, krašto apsaugos ministrui dėl organizacinių ir techninių kibernetinio saugumo reikalavimų valstybės informaciniams ištekliams ir ypatingos svarbos informacinei infrastruktūrai ir atlieka jų atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams stebėseną. Taip pat valdo kibernetinio saugumo informacinį tinklą, rengia gynybos planus ir tipinius kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus. Reaguoja į kibernetinius incidentus valstybės informaciniuose ištekliuose, ypatingos svarbos informacinėse infrastruktūrose ir juose diegia, valdo technines kibernetinio saugumo priemones. Vykdo žinybinių saugumo priežiūros tarnybų apskaitą, teikia metodines rekomendacijas ir koordinuoja jų veiklą. Tvirtina kriptografinius metodus, produktus, konsultuoja, analizuoja nacionalinę kibernetinio saugumo situaciją ir rengia nacionalinio kibernetinio saugumo būklės ataskaitas. Vykdo informacijos sklaidą kibernetinio saugumo klausimais ir teikia konsultacijas, rekomendacijas valstybės informacinių išteklių valdytojams ir ypatingos svarbos infrastruktūros valdytojams kibernetinio saugumo klausimais.

Pagal Lietuvos Respublikos (toliau LR) KAM ministro įsakymą dėl NKSC prie KAM nuostatų ir struktūros patvirtinimo galima išskirti ***pagrindinės NKSC teisės***. Taigi vykdydamas nustatytas funkcijas NKSC turi teisę gauti iš LR institucijų ir jų padalinių dokumentus ir informaciją, kuri būtina funkcijoms vykdyti. Taip pat rengti, dalyvauti rengiant teisės aktų, projektus susijusių su jų veikla ir

teisės aktų nustatyta tvarka savo vardu sudaryti sandorius. Teikti siūlymus krašto apsaugos ministrui ar jo įgaliotam asmeniui dėl veiklos tobulinimo ir pagal kompetenciją ***bendradarbiauti su Lietuvos Respublikos institucijomis*** ir organizacijomis ir jose atstovauti.

Nuo 2017 m. gruodžio 19 d. seimas priėmė Kibernetinio saugumo įstatymo pataisas, kuriomis konsoliduota informacinių išteklių saugumo sritis, o nuo 2018 m. pradžios NKSC „vieno langelio“ principu teikia pagalbą tiek valstybės institucijoms, tiek verslui ir gyventojams. Savo kompetencijos ribose drauge su valstybės įstaigomis ir organizacijomis bei kitais ūkio subjektais sprendžia valstybės informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros kibernetinio saugumo klausimus.

NKSC naudodamasis įdiegtomis techninėmis stebėsenos priemonėmis pateikė nacionalinio kibernetinio saugumo būklės ataskaita už 2017 metus kur užfiksavo daugiausia ***žalingos programinės įrangos*** veikimo atvejų daugiausiai:

- ✓ energetikos daugiau negu 26 proc. visų užfiksuotų atvejų;
- ✓ viešojo saugumo ir teisinės tvarkos daugiau negu 22 proc.;
- ✓ užsienio reikalų ir saugumo politikos sektoriuje daugiau negu 21 proc.

Remiantis nacionalinio kibernetinio saugumo būklės ataskaita už 2018 metus daugiausiai ***kenkimo programinės įrangos*** aptikta:

- ✓ valstybės valdymo - 39 proc.;
- ✓ energetikos - 20 proc.;
- ✓ užsienio reikalų ir saugumo politikos sektoriuje daugiau negu 19 proc.

Tokio masto incidentų statistika signalizuoja didelį kibernetinio saugumo iššūkį, tenkantį Lietuvos elektroninei erdvei, piliečiams, valstybės institucijom ir verslui. Todėl NKSC kartu su Europos nacionalinių fondų šio metu vykdo projektą *„Kompleksiniai kibernetinės saugos mokymai valstybės ir savivaldybių institucijų ir įstaigų darbuotojams“* kurio tikslas stiprinti informacinės visuomenės saugumą, suteikiant valstybės tarnybos ir savivaldos darbuotojams žinių kibernetinio saugumo srityje, kad jie gebėtų įvertinti kibernetinio saugumo rizikas ir taikyti efektyvias kibernetinio saugumo priemones savo informacinių sistemų apsaugai ir tokiu būdu prisidėti prie saugios informacinės visuomenės kūrimo proceso Lietuvos valstybiniame sektoriuje. O 2019 m. spalio 22- 24 dienomis, NKSC prie Krašto apsaugos ministerijos (toliau KAM) bendradarbiaudamas su Kauno technologijos universitetu surengė kasmetines nacionalines kibernetinio saugumo pratybas „Kibernetinis skydas 2019“. Remiantis pratybų „KIBERNETINIS SKYDAS 2019“ ataskaita visuomenei, pratybomis buvo siekiama formuoti praktinius pratybų dalyvių kibernetinio saugumo įgūdžius, patikrinti kibernetinių incidentų valdymo procedūras, ***gerinti bendradarbiavimą tarp kibernetinius incidentus valdančių ir tiriančių institucijų*** ir kibernetinio saugumo subjektų. Remiantis ataskaita į pratybas buvo kviečiami dalyvauti:

- ✓ valstybės informacinių išteklių valdytojai ir tvarkytojai;

- ✓ ypatingos svarbos informacinės infrastruktūros valdytojai;
- ✓ viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų;
- ✓ elektroninės informacijos prieglobos paslaugų ir skaitmeninių paslaugų teikėjai;
- ✓ kibernetinius incidentus valdančios ir (ar) tiriančios institucijos (Nacionalinis kibernetinio saugumo centras, Valstybinė duomenų apsaugos inspekcija, Lietuvos policija);
- ✓ pavojingo kibernetinio incidento valdymą koordinuojančios institucijos (LR Vyriausybės kanceliarija, LR Seimo kanceliarija, LR Prezidento kanceliarija, LR valstybės saugumo departamentas, LR Krašto apsaugos ministerija).

Tačiau pagal NKSC pratybų ataskaitą dalyvavo tik pusė LR ministerijų, o joms pavaldžių įstaigų dalyvavimas nesiekia 50 procentų. Toks LR ministerijų dalyvių skaičius ***byloja apie menką tarpinstitucinį bendradarbiavimą kibernetinio saugumo srityje***, nes vienas iš pagrindinių pratybų tikslų gerinti bendradarbiavimą tarp kibernetinius incidentus valdančių ir tiriančių institucijų ir kibernetinio saugumo subjektų. Remiantis Kibernetinio saugumo įstatymu IV skyriu 14 str. yra reglamentuojama, kad NKSC vykdo formalio būdo tarpinstitucinį bendradarbiavimą tik su policiją tiriant kibernetinius incidentus, apsikeičiant su kibernetinių incidentų tyrimu susijusia informacija, reikalinga pagal kompetenciją šių institucijų funkcijoms atlikti, o reikalui esant gali būti vykdomas bendradarbiavimas su kriminalinės žvalgybos subjektais ir žvalgybos institucijomis. Tiriant kibernetinius incidentus, susijusius su asmens duomenų ir privatumo apsaugos pažeidimais, NKSC bendradarbiauja su Valstybinė duomenų apsaugos inspekcija apsikeičiant informacija, reikalinga teisės aktų nustatytomis funkcijomis, susijusiomis su asmens duomenų ir privatumo apsaugą pažeidžiančių kibernetinių incidentų tyrimui atlikti. Taip pat yra paminėta, kad tarpinstitucinio bendradarbiavimo valdant ir tiriant kibernetinius incidentus tvarka nustatoma Nacionaliniame kibernetinių incidentų valdymo plane, tačiau šito plano galiojanti suvestinė redakcija baigė galioti ir negalioja nuo 2019 m. sausio 1 d.

NKSC siekiant apjungti savo teikiamus resursus, paslaugas vienoje erdvėje ir užtikrinti efektyvų kibernetinio saugumo informacijos dalinimąsi tarp kibernetinio saugumo subjektų tai yra užtikrinti viešojo ir privataus sektorių bendradarbiavimo įgyvendinimą naudojimąsi tinklu yra sukūręs - ***Kibernetinio saugumo informacinį tinklą.*** Remiantis Nacionalinė kibernetinio saugumo strategiją, IV skyriaus ketvirtuojų strategijos tikslu, vienas iš tinko tikslų yra dalytis informacija apie galimus ir įvykusius kibernetinius incidentus. Taip pat rekomendacijomis, nurodymais, techniniais sprendimais ir kitomis priemonėmis, užtikrinančiomis kibernetinį saugumą ir tinklo narių bendradarbiavimą kibernetinio saugumo srityje. Tinkle būtina įdiegti priemones, užtikrinančias efektyvų ir abipusį pasitikėjimą skatinantį tinklo narių bendravimą.

Taigi Nacionalinis kibernetinio saugumo centras savo kompetencijos ribose drauge su valstybės institucijomis ir organizacijomis bei kitais ūkio subjektais sprendžia valstybės informacinių išteklių (toliau VII) ir ypatingos svarbos informacinės infrastruktūros (toliau YSII) kibernetinio saugumo

klausimus. Remiantis NKSC oficialiąją internetinę svetainę buvo nustatyti pagrindiniai veiklos tikslai, teikiamos paslaugos (žr. 15 lent.).

15 lentelė. NKSC misija, pagrindiniai veiklos tikslai, teikiamos paslaugos, rekomendacijos

Nacionalinis kibernetinio saugumo centras Prie Krašto apsaugos ministerijos yra pagrindinė Lietuvos kibernetinio saugumo institucija, atsakinga už vieningą kibernetinių incidentų valdymą, kibernetinio saugumo reikalavimų įgyvendinimo stebėseną ir kontrolę, ypatingos svarbos informacinės infrastruktūros kibernetinį saugumą ir informacinių išteklių akreditaciją.			
Misija	**Pagrindiniai veiklos tikslai**	**Teikiamos paslaugos**	**Rekomendacijos**
Būti kibernetinio saugumo kompetencijos centru siekiant, kad interneto vartotojai bendraudami, mokydamiesi ir dirbdami kibernetinėje erdvėje jaustųsi saugiai.	-Įgyvendinti nacionalinę kibernetinio saugumo politiką. -Atlikti saugumo priežiūros tarnybos funkcijas. -Atlikti nacionalinės komunikacijų apsaugos tarnybos funkcijas. -Vykdyti informacijos sklaidos, tyrimų ir analizės kibernetinio saugumo klausimais veiklą.	-Asmenų konsultavimas ir įstatymų nustatytos informacijos teikimas. -Asmenų skundų nagrinėjimas. -Kriptografinės priemonės patvirtinimo pažymos išdavimas. -Leidimo apdoroti įslaptintą informaciją išdavimas. -Pažymų, dokumentų kopijų, išrašų, kuriais patvirtinamas tam tikras juridinis faktas, išdavimas	-Interneto svetainių apsauga -Mobiliųjų įrenginių apsauga -Ransomware -Sinkhole HTTP -Conficker, Conflicker, -Downadup SSL v3.0 protokolo saugumo spraga -SSDP DDoS -NetBIOS DDoS -NTP Version spraga -Open Resolver

Šaltinis: parengta autorės pagal www.nksc.lt

Kaip matome 15 lentelėje surinkti duomenys iš oficialios Nacionalinio kibernetinio saugumo centro svetainės parodo, kad nei tiksluose nei misijoje nėra minima apie tarpinstitucinį bendradarbiavimą ir jo vystymą, tačiau svetainėje yra pateiktas projektas kuris vykdomas kartu su Europos nacionalinių fondų *„Kompleksiniai kibernetinės saugos mokymai valstybės ir savivaldybių institucijų ir įstaigų darbuotojams“* kurio tikslas stiprinti informacinės visuomenės saugumą, suteikiant valstybės tarnybos ir savivaldos darbuotojams žinių kibernetinio saugumo srityje, kad jie gebėtų įvertinti kibernetinio saugumo rizikas ir taikyti efektyvias kibernetinio saugumo priemones savo informacinių sistemų apsaugai ir tokiu būdu prisidėti prie saugios informacinės visuomenės kūrimo proceso Lietuvos valstybiniame sektoriuje.

Apibendrinant NKSC tarpinstitucinio bendradarbiavimo formavimo procesų analizė galima daryti išvada, kad tarpinstitucinis bendradarbiavimas formuojasi ne tik remiantis teisės aktais kuriuose reglamentuotas bendradarbiavimas įvykus incidentams. NKSC įžvelgia neformaliojo bendradarbiavimo būdo poreikį, kuris padės stiprinti informacinės visuomenės saugumą, suteikiant valstybės tarnybos ir savivaldos darbuotojams žinių kibernetinio saugumo srityje, kad jie gebėtų įvertinti kibernetinio saugumo rizikas ir taikyti efektyvias kibernetinio saugumo priemones savo informacinių sistemų apsaugai ir tokiu būdu prisidėti prie saugios informacinės visuomenės kūrimo proceso Lietuvos valstybiniame sektoriuje. Tokiu būdu ***NKSC*** dalyvauja valstybės institucijų mokymų organizavime (*„Kibernetinis skydas 2019“, „Kompleksiniai kibernetinės saugos mokymai valstybės ir savivaldybių institucijų ir įstaigų darbuotojams*“) ir ***vykdo neformalųjį tarpinstitucinį bendradarbiavimą.***

3.2. Valstybės institucijų tarpinstitucinio bendradarbiavimo formavimo procesų analizė

Gyvenant skaitmeninėje, informacinių technologijų eroje, Lietuvai būtina priimti naujus iššūkius, nes yra aktyviai naudojamasi informacinių ir ryšių technologijų teikiamomis galimybėmis. Puikiai išplėtotą plačiajuosčio ryšio infrastruktūrą, tampa patraukli ne tik pavieniams asmenims, bet ir organizuotoms grupuotėms. Lietuva nuolat susiduria su įvairaus tipo kibernetiniais incidentais, skirtais valstybės informaciniams ištekliams ir ypatingos svarbos informacinei infrastruktūrai pažeisti. Remiantis Lietuvos Respublikos (toliau LR) valstybės saugumo departamento ir Antrojo operatyvinių tarnybų departamento prie Krašto apsaugos ministerijos (2018) ataskaitą (*Grėsmių nacionaliniam saugumui vertinimas)* taip pat Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos (2018) ataskaitą (*Nacionalinio kibernetinio saugumo būklės ataskaita*) prognozuojama, kad ateityje kibernetinių incidentų nukreiptu prieš nacionalinį saugumą ir visuomenę ir jos gerbuvį, skaičius ir mastas gali didėti.

Vertinant tarinstitucinio bendradarbiavimo Lietuvoje kibernetinio saugumo srityje buvo parinktos valstybės institucijos atsakingos už ypatingos svarbos infrastruktūros objektus (toliau YSI objektai) ir ypatingos svarbos informacines infrastruktūras (toliau YSII). Remiantis LR Kibernetinio saugumo įstatymu ir ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką pateiktomis YSI objekto ir YSII apibrėžimais galima pamatyti jų teikiančia svarbą:

- ***ypatingos svarbos informacinė infrastruktūra*** – ryšių ir informacinė sistema ar jos dalis, ryšių ir informacinių sistemų grupė, kurioje įvykęs kibernetinis incidentas gali padaryti didelį neigiamą poveikį nacionaliniam saugumui, valstybės ūkiui, valstybės ir visuomenės interesams;
- ***ypatingos svarbos infrastruktūros objektas*** – infrastruktūros objektas, teikiantis ypatingos svarbos paslaugą, kurios neveikimas ar veikimo sutrikimas padarytų didelį neigiamą poveikį nacionaliniam saugumui, šalies ūkiui, valstybės ar visuomenės interesams.

Tam, kad ypatingos svarbos infrastruktūros objektai galėtų teikti kokybiškas paslaugas, jie tampa vis labiau priklausomi nuo informacinių ir ryšio technologijų. Jiems kyla vis naujos grėsmės. Šių ypatingos svarbos infrastruktūros objektų kibernetinio saugumo užtikrinimas yra svarbus uždavinys ir aukščiausio lygio prioritetas tiek valstybėms, tiek institucijoms, organizacijoms, valdančioms ypatingos svarbos infrastruktūros objektus. Todėl norint pasiekti šio uždavinio rezultatą svarbų vaidmenį atlieka tarpinstitucinis bendradarbiavimas bei įvairių sričių specialistų maksimalus koordinavimas. Taigi ypatingos svarbos informacinių struktūrų saugumo ir atsparumo stiprinimas yra ilgalaikis tikslas, kurio strategiją ir priemones reikia reguliariai vertinti.

Analizuojant valstybės institucijų tarpinstitucinio bendradarbiavimo formavimo procesus, buvo remiamasi LR Kibernetinio saugumo įstatymu ypatingos svarbos informacinės infrastruktūros

identifikavimo metodikos 1 priedu, kur pateiktas valstybės institucijų atsakingu už ypatingos svarbos infrastruktūros objektus ir ypatingos svarbos informacinių infrastruktūrų sąrašas:

1. Lietuvos Respublikos aplinkos ministerija;
2. Lietuvos Respublikos energetikos ministerija;
3. Lietuvos Respublikos finansų ministerija;
4. Lietuvos Respublikos susisiekimo ministerija;
5. Lietuvos Respublikos sveikatos apsaugos ministerija;
6. Lietuvos Respublikos ūkio ministerija;
7. Lietuvos Respublikos užsienio reikalų ministerija;
8. Lietuvos Respublikos vidaus reikalų ministerija;
9. Lietuvos Respublikos žemės ūkio ministerija;
10. Lietuvos Respublikos Vyriausybė;
11. Lietuvos Respublikos teisingumo ministerija;
12. Lietuvos Rrespublikos krašto apsaugos ministerija.

Kiekviena iš aukščiau minėtu valstybės institucijų yra atsakinga už tam tikrą ypatingos svarbos infrastruktūros objektą ir ypatingos svarbos informacinės infrastruktūras. Taigi pagal Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką 1 priedą, **Lietuvos Respublikos aplinkos ministerija** atsakinga už (žr. 16 lent.).

16 lentelė. LR aplinkos ministerija - YSI objekto sektoriai, subsektoriai ir paslaugos

Atsakinga institucija	Sektorius	Subsektorius	Paslaugos
Lietuvos Respublikos aplinkos ministerija	Geriamojo vandens tiekimo, paskirstymo ir tvarkymo sektorius	Geriamojo vandens subsektorius	Geriamojo vandens laikymo, tiekimo ir kokybės užtikrinimo paslauga
		Nuotekų subsektorius	Nuotekų surinkimo ir tvarkymo paslauga
	Aplinkos sektorius	Oro taršos ir meteorologinio stebėjimo subsektorius	Oro taršos stebėjimo ir ankstyvo perspėjimo paslauga
			Meteorologinio stebėjimo ir ankstyvo perspėjimo paslauga
		Paviršinių ir jūros vandenų stebėjimo subsektorius	Paviršinių vandenų (upių, ežerų) stebėjimo ir ankstyvo perspėjimo paslauga
			Jūros užterštumo stebėjimo ir kontrolės paslauga
			Vandens lygio reguliavimo, hidrotechninių įrenginių eksploatavimo paslauga
		Miškininkystės subsektorius	Valstybinių miškų valdymo paslauga

Šaltinis: parengta autorės pagal Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką, 1 priedas, 2018

Analizuojant Lietuvos Respublikos aplinkos ministerijos nuostatus buvo pastebėta, kad tarpinstitucinis bendradarbiavimas formaliuoju būdu nėra reglamentuotas nei su viena valstybės institucija. Tačiau II skyriuje kur yra apibrėžtos aplinkos ministerijos veiklos tikslai ir funkcijos 9.9 punkte sakoma, kad aplinkos ministerija pagal kompetenciją organizuoja ir koordinuoja mokslinius tyrimus, taikomųjų mokslo programų ir projektų finansavimą, koordinuoja jų įgyvendinimą, skatina inovacijas. Taigi galima daryti prielaida dėl aplinkos ministerijos vykdomo neformaliojo būdu tarpinstitucinio bendradarbiavimo.

Lietuvos Respublikos finansų ministerija. Nemaža dalis kibernetinių atakų vyksta finansinių paslaugų sektoriuje. Dėl naujų kibernetinių grėsmių nuolat keičiama ir pildoma teisinio reguliavimo praktika. Kiekvienais metais finansinių paslaugų sektoriuje sukuriamas duomenų kiekis sparčiai didėja. Reguliuotojų reikalavimai dėl kibernetinio saugumo ir duomenų apsaugos griežtėja, o tai sukelia papildomą administracinę ir atitikties naštą tiek privačiam, tiek viešam sektoriui. Remiantis Ypatingos svarbos informacinės infrastruktūros identifikavimo metodikos 1 priedu, galima išskirti šiuos Lietuvos Respublikos finansų ministerijos sektorius, subsektorius ir paslaugas (žr. 17 lent.).

17 lentelė. LR finansų ministerija – YSI objekto sektoriai, subsektoriai ir paslaugos

Atsakinga institucija	Sektorius	Subsektorius	Paslaugos
Lietuvos Respublikos finansų ministerija	Finansų sektorius	Kredito įstaigų subsektorius	Kredito įstaigų finansinė paslauga
		Finansinių rinkų infrastruktūros subsektorius	Paslauga, susijusi su mokėjimų ir vertybinių popierių atsiskaitymų sistemų veikla
			Paslauga, susijusi su prekybos vietų ir reguliuojamos rinkos veikla
			Centrinių vertybinių popierių depozitoriumų paslauga

Šaltinis: parengta autorės pagal Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką, 1 priedas, 2018

Analizuojant Lietuvos Respublikos finansų ministerijos nuostatus buvo pastebėta, kad tarpinstitucinis bendradarbiavimas formaliuoju būdu nėra reglamentuotas nei su viena valstybės institucija. Taip pat finansų ministerijos nuostatuose veiklos tikslai ir funkcijos nėra kalbama apie neformaliojo būdo tarpinstitucinį bendradarbiavimą.

Lietuvos respublikos energetikos ministerija. Pramoniniai kibernetiniai incidentai yra vieni iš pavojingiausių. Jie gali sukelti gamybos prastovas, apčiuopiamus finansinius nuostolius ir turi sunkias pasekmes ypač incidentas įvykus kritiniuose, tokiuose kaip energetika, sektoriuose. Remiantis "Kaspersky" 2019 m. pirmojo pusmečio statistika, kuri buvo gauta iš jų automatiškai apdorojamų saugumo technologijų, parodė, kad per stebėtą laikotarpį „Kaspersky" produktai kenkėjišką veiklą

aptiko beveik pusėje (41,6 proc.) energetikos sektoriaus ICS kompiuterių. Taip pat buvo užblokuota daugybė įprastų kenkėjiškų programų, kurios nebuvo skirtos ICS tipo įrangai. Todėl remiantis Europos Sąjungos (toliau ES) Komisijos rekomendaciją (2019/553) dėl energetikos sektoriaus kibernetinio saugumo ES valstybėms narėms, būtina vystyti tarpinstitucinį bendradarbiavimą, keitimąsi informaciją kibernetinio saugumo klausimais. Taigi ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką 1 priede, išskiria šiuos Lietuvos Respublikos energetikos ministerijos sektorius, subsektorius ir paslaugas (žr. 18 lent.).

18 lentelė. LR energetikos ministerija – YSI objekto sektoriai, subsektoriai ir paslaugos

Atsakinga institucija	Sektorius	Subsektorius	Paslaugos
Lietuvos Respublikos energetikos ministerija	Energetikos sektorius	Elektros energijos subsektorius	Elektros energijos gamybos paslauga Elektros energijos perdavimo paslauga Elektros energijos skirstymo paslauga Elektros energijos tiekimo paslauga
		Naftos ir naftos produktų subsektorius	Naftos gavybos paslauga Naftos perdirbimo ir apdorojimo paslauga Naftos perdavimo vamzdynais paslauga Naftos ir naftos produktų laikymo paslauga (taip pat ir valstybės atsargų saugojimas)
		Gamtinių dujų subsektorius	Gamtinių dujų perdavimo paslauga Gamtinių dujų skirstymo paslauga Gamtinių dujų ir suskystintųjų gamtinių dujų laikymo paslauga Gamtinių dujų perdirbimo ir apdorojimo (taip pat ir gamtinių dujų suskystinimo) paslauga Suskystintųjų gamtinių dujų pakartotinio dujinimo paslauga Gamtinių dujų ir suskystintųjų gamtinių dujų tiekimo paslauga
		Centralizuoto šildymo subsektorius	Centralizuoto šilumos tiekimo paslauga Centralizuotos šilumos gamybos paslauga

Šaltinis: parengta autorės pagal Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką, 1 priedas, 2018

Analizuojant Lietuvos Respublikos energetikos ministerijos nuostatus buvo pastebėta, kad tarpinstitucinis bendradarbiavimas formaliuoju būdu reglamentuojamas tarptautiniu mastu. Remiantis LR energetikos nuostatais, veiklos tikslai ir funkcijos, II skyrio 11.3. punktu reglamentuoja, kad energetikos ministerija dalyvauja rengiant energetinio bendradarbiavimo su užsienio valstybėmis sutartis, kitus su tuo susijusius dokumentus, dalyvauja konsultacinėse konferencijose ir derybose su tarptautinėmis organizacijomis, siekdama plėsti Lietuvos ir užsienio valstybių bendradarbiavimą ir spręsti energetikos sektoriui aktualias problemas, dalyvauja rengiant dvišalių ir daugiašalių Lietuvos ir

užsienio valstybių bendradarbiavimo komisijų posėdžius. Taip pat pastebėta, kad energetikos ministerija remiantis nuostatais vykdo ir neformalųjį tarpinstitucinį bendradarbiavimą tai yra dalyvauja įgyvendinant ilgalaikes valstybės saugumo stiprinimo programas energetikos srityje, rengia projektus, teikia jį Vyriausybei. Kartu su kitomis ministerijomis ir institucijomis organizuoja ir koordinuoja programos įgyvendinimą.

Lietuvos Respublikos susisiekimo ministerija, remiantis 2020–2022 metų strateginiu veiklos planu kurio siekiama, kad būtų sukurta darni, saugi, konkurencinga ir didelę pridėtinę vertę kurianti susisiekimo sistema, kuri atitiktų gyventojų ir verslo lūkesčius ir tenkintų jų poreikius:

1. *Transporto ir ryšių politikos įgyvendinimas;*
2. *Susisiekimo valstybinės ir vietinės reikšmės keliais užtikrinimas;*
3. *Susisiekimo vandens keliais užtikrinimas;*
4. *Susisiekimo geležinkeliais užtikrinimas;*
5. *Susisiekimo oro transportu užtikrinimas.*

Taigi įgyvendinant strateginį veiklos plano tikslą, susisiekimo sistema turi užtikrintų kokybišką, saugų, nepertraukiamą ir darnų visuomenės narių judumą, prekių transportavimą ir aukštos kokybės logistikos paslaugas ir tame nemažai dalyvauja kibernetinis saugumas. Jį įgyvendinti LR susisiekimo ministerija galės tik glaudžiai bendradarbiaujant su kitomis institucijomis formaliuoju ir neformaliuoju būdu. Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką 1 priede, išskiria šiuos Lietuvos Respublikos susisiekimo ministerijos sektorius, subsektorius ir paslaugas (žr. 19 lent.).

19 lentelė. LR susisiekimo ministerija – YSI objekto sektoriai, subsektoriai ir paslaugos

Atsakinga institucija	Sektorius	Subsektorius	Paslaugos
Lietuvos Respublikos susisiekiko ministerija	Transporto ir pašto sektorius	Oro transporto subsektorius	Skrydžių valdymo ir navigacijos paslauga; Oro uostų paslauga; Oro susisiekimo paslauga.
		Geležinkelių transporto Subsektorius	Keleivių ir bagažo vežimo geležinkeliais paslauga; Krovinių vežimo geležinkeliais paslauga; Geležinkelių infrastruktūros plėtros, valdymo ir priežiūros paslauga.
		Vandens transporto subsektorius	Uostų paslauga; Laivybos saugos, kontrolės ir valdymo paslauga; Keleivių ir krovinių vežimo vandens transportu paslauga.
		Kelių transporto subsektorius	Susisiekimo kelių transportu paslauga; Kelių tinklo planavimo, kontrolės ir priežiūros paslauga; Intelektinių transporto sistemų paslauga.
	Informacinių technologijų ir elektroninių ryšių sektorius	Elektroninių ryšių subsektorius	Fiksuotojo ir judriojo telefono ryšio, duomenų perdavimo paslauga; Interneto prieigos paslauga; Radijo ir televizijos programų perdavimo ir transliavimo (retransliavimo) paslauga.

Šaltinis: parengta autorės pagal Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką, 1 priedas, 2018

Analizuojant Lietuvos Respublikos susisiekimo ministerijos nuostatus buvo pastebėta, kad tarpinstitucinis bendradarbiavimas pagal nuostatuose 8.1.1. punktą byloja apie neformalųjį bendradarbiavimo būdą tai yra dalyvauja įgyvendinant kitų institucijų parengtas strategijas ir programas. Apie formalųjį tarpinstitucinį bendradarbiavimą LR susisiekimo ministerijos nuostatuose yra reglamentuojama tarptautiniu mastu tai yra pagal 9.16. punktą, susisiekimo ministerija pagal kompetenciją bendradarbiauja su užsienio valstybių atitinkamomis institucijomis ir tarptautinėmis organizacijomis, atstovauja jose Lietuvos Respublikai.

Lietuvos Respublikos sveikatos apsaugos ministerijos valdomų ir Valstybės įmonės Registrų centro tvarkomų elektroninės sveikatos sistemos informacinių sistemų duomenų saugos nuostatai reglamentuoja Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos ir Išankstinės pacientų registracijos informacinės sistemos elektroninės informacijos saugos kibernetinio saugumo politiką. Remiantis Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką 1 priede, išskiria šiuos Lietuvos Respublikos sveikatos apsaugos ministerijos sektorius, subsektorius ir paslaugas (žr. 20 lent.).

20 lentelė. LR sveikatos apsaugos ministerija – YSI objekto sektoriai, subsektoriai ir paslaugos

Atsakinga institucija	Sektorius	Subsektorius	Paslaugos
Lietuvos Respublikos sveikatos apsaugos ministerija	Sveikatos priežiūros sektorius	Sveikatos priežiūros infrastruktūros subsektorius	Skubiosios medicinos pagalbos paslauga; Stacionarinio gydymo paslauga; Ambulatorinio gydymo paslauga; Vaistinių preparatų, medicinos priemonių (prietaisų), kraujo ir kraujo komponentų tiekimo ir laikymo paslauga; Infekcinių ligų atvejų, protrūkių ir (ar) epidemijų kontrolės paslauga.

Šaltinis: parengta autorės pagal Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką, 1 priedas, 2018

Analizuojant Lietuvos Respublikos sveikatos apsaugos ministerijos nuostatus buvo pastebėta, kad ypatingas dėmesys, atskiru teisės aktu, skiriamas tarpinstitucinio bendradarbiavimo LR sveikatos apsaugos ministerijos valdomų ir valstybės įmonių registro centrų tvarkomų elektroninės sveikatos sistemos informacinių sistemų duomenų saugai kur nuostatuose 13.2.5. punkte yra kalbama apie formalųjį tarpinstitucinį bendradarbiavimą. Apie būtinumą koordinuoti elektroninės informacijos saugos kibernetinių incidentų tyrimą savo organizacijose ir bendradarbiauti su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugos kibernetinius incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos kibernetiniais incidentais. Tačiau apie prevencijos tarpinstitucinio bendradarbiavimo priemonės užtikrinant kibernetinį saugumą nėra minima.

Analizuojant LR sveikatos apsaugos ministerijos nuostatus yra pastebėta, kad ministerija vykdo bendradarbiavimą tarptautiniu mastu tai yra organizuoja ir koordinuoja tarptautinį bendradarbiavimą sveikatos srityje. Taip pat vykdo formaliuoju būdu bendradarbiauja su valstybės ir savivaldybių institucijomis ir įstaigomis, nevyriausybinėmis organizacijomis, profesinėmis sąjungomis.

Lietuvos Respublikos ūkio ministerija šiuo metu yra pervadinta į Lietuvos Respublikos ekonomikos ir inovacijų ministeriją. Pagal Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką 1 priede, išskiria šiuos Lietuvos Respublikos ūkio ministerijos sektorius, subsektorius ir paslaugas (žr. 21 lent.).

21 lentelė. LR ekonomikos ir inovacijų ministerija – YSI objekto sektoriai, subsektoriai ir paslaugos

Atsakinga institucija	Sektorius	Subsektorius	Paslaugos
Lietuvos respublikos ekonomikos ir inovacijų ministeriją	Informacinių technologijų ir elektroninių ryšių sektorius	Skaitmeninės infrastruktūros subsektorius	Interneto duomenų srautų mainų taško (IXP) paslauga; Domenų vardų sistemos (DNS) paslauga; Aukščiausio lygio domenų vardų registro (lt. domeno) paslauga.
		Informacinių technologijų subsektorius	Duomenų centrų ir (arba) debesijos paslauga
	Pramonės sektorius	Cheminės, branduolinės ir kitos didesnės rizikos pramonės subsektorius	Pavojingų medžiagų gamybos, laikymo ir atliekų tvarkymo paslauga; Didelės rizikos pramoninių objektų saugumo užtikrinimo paslauga; Statinių ir kitų objektų sprogdinimo paslauga.
		Karinės pramonės subsektorius	Karinės įrangos, ginklų ir šaudmenų gamybos paslauga.
	Valstybės valdymo sektorius	Valstybės valdžios funkcijų vykdymo subsektorius	Ypatingos svarbos valstybės informacinių išteklių valdymo ar tvarkymo paslauga.

Šaltinis: parengta autorės pagal Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką, 1 priedas, 2018

Analizuojant Lietuvos Respublikos ekonomikos ir inovacijų ministerijos nuostatus buvo pastebėta, kad ministerija daugiausiai bendradarbiauja su verslininkus vienijančiomis organizacijomis, visuomeninėmis patariamosiomis institucijomis ir kitomis suinteresuotomis šalimis, analizuodama ir vertindama verslo sąlygas Lietuvoje, spręsdama smulkiojo ir vidutinio verslo subjektų problemas. Taip pat užtikrina viešųjų paslaugų smulkiajam ir vidutiniam verslui prieinamumą, bendradarbiaujant su savivaldybių institucijomis ir asocijuotomis verslo struktūromis. Kaip matome ekonomikos ir inovacijų

ministerija savo dėmesį nuostatuose labiau akcentuoja į privatų sektorių. Šiek tiek yra minimą apie savivaldybės institucijas, tačiau tik tiek kiek liečia privatųjį sektorį. Nepaisant to ekonomikos ir inovacijų ministerija pagal nuostatuose 9.7. punktą koordinuoja Europos Sąjungos, bendradarbiaudama su kitomis valstybės institucijomis dėl Lietuvos geresnio reglamentavimo iniciatyvų, skirtų ūkio subjektų administracinei ir kitai reguliavimo naštai mažinti, teisės aktams supaprastinti, teisinio reguliavimo kokybei ir verslo sąlygoms gerinti, įgyvendinimą. Taigi galima daryti išvadą, kad LR ekonomikos ir inovacijų ministerija vykdo formalųjį tarpinstitucinį bendradarbiavimą, tačiau nuostatuose apie bendradarbiavimą užtikrinant kibernetinį saugumą Lietuvoje nėra minima.

Lietuvos Respublikos užsienio reikalų ministerija remiantis Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką 1 priede, išskiria šiuos Lietuvos Respublikos užsienio reikalų ministerijos sektorius, subsektorius ir paslaugas (žr. 22 lent.).

22 lentelė. LR užsienio reikalų ministerija – YSI objekto sektoriai, subsektoriai ir paslaugos

Atsakinga institucija	Sektorius	Subsektorius	Paslaugos
Lietuvos Respublikos užsienio reikalų ministerija	Užsienio reikalų ir saugumo politikos sektorius	Užsienio reikalų ir saugumo politikos įgyvendinimo subsektorius	Užsienio reikalų ir saugumo politikos įgyvendinimo paslauga

Šaltinis: parengta autorės pagal Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką, 1 priedas, 2018

Pagrindinis Užsienio reikalų ministerijos ir diplomatinių atstovybių veiklos tikslas – užtikrinti Lietuvos valstybės ir jos žmonių saugumą bei gerovę. Atstovauti ir ginti Lietuvos interesus tarptautiniuose formatuose, taip pat telkti bei puoselėti lietuvybę užsienyje. Vertinant tai, kad mes gyvename informacinių technologijų eroje, užsienio reikalų ministerijos ataskaitoje (2019 m.) pateiktoje 2020 metais vasario mėnesio, nėra minima apie kibernetinio saugumo užtikrinimo tarpinstitucinio bendradarbiavimo priemonės, pasiektus tikslus ir jų vertinimą.

Analizuojant Lietuvos Respublikos užsienio reikalų ministerijos nuostatus buvo pastebėta, kad ministerija savo veiklos tiksluose ir funkcijose vykdo koordinavimą tarp valstybės ir užsienio institucijų, o pasak Uwe, P. (2003) ***koordinavimo procesai yra neformalus tarpinstitucinio bendradarbiavimo būdas***. Taigi LR užsienio reikalų ministerija teikia valstybės institucijoms ir įstaigoms pasiūlymus dėl ekonominio saugumo užtikrinimo priemonių, tarpininkauja užmezgant ir palaikant Lietuvos Respublikos ir užsienio valstybinių institucijų ir nevyriausybinių organizacijų ryšius.

Lietuvos Respublikos vidaus reikalų ministerija formuoja valstybės politiką viešojo saugumo: viešosios tvarkos, vidaus tarnybos, priešgaisrinės bei civilinės saugos ir gelbėjimo darbų, valstybės

sienos apsaugos, ginklų, šaudmenų, sprogmenų ir specialiųjų priemonių apyvartos, saugomo asmens statusą turinčių asmenų apsaugos srityse,. Taip pat organizuoja, koordinuoja ir kontroliuoja jos įgyvendinimą. Remiantis Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką 1 priede, išskiria šiuos Lietuvos Respublikos vidaus reikalų ministerijos sektorius, subsektorius ir paslaugas (žr. 23 lent.).

23 lentelė. LR vidaus reikalų ministerija – YSI objekto sektoriai, subsektoriai ir paslaugos

Atsakinga institucija	Sektorius	Subsektorius	Paslaugos
Lietuvos Respublikos vidaus reikalų ministerija	Informacinių technologijų ir elektroninių ryšių sektorius	Skaitmeninės infrastruktūros subsektorius	Elektroninės atpažinties paslauga
	Civilinės saugos sektorius	Ekstremaliųjų situacijų valdymo subsektorius	Bendrojo pagalbos centro paslauga; Perspėjimo apie ekstremaliuosius įvykius ir situacijas, jų likvidavimo, padarinių šalinimo, gyventojų ir turto gelbėjimo organizavimo ir koordinavimo paslauga.

Šaltinis: parengta autorės pagal Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką, 1 priedas, 2018

Analizuojant Lietuvos Respublikos vidaus reikalų ministerijos nuostatus buvo pastebėta, kad ministerija vykdo neformalųjį tarpinstitucinį bendradarbiavimą tai yra formuoja valstybės politiką vietos savivaldos srityje, organizuoti, koordinuoti ir kontroliuoti jos įgyvendinimą. Taip pat kontroliuoja pavaldžių institucijų ir įstaigų veiklą, atlieka jų valdymo priežiūrą, koordinuoja Vyriausybei atskaitingų institucijų funkcijų peržiūros procesą ir koordinuoja valstybės ir savivaldybių institucijų veiklą bendruomeninių organizacijų klausimais. Tačiau apie kibernetinio saugumo užtikrinimą tarpinstitucinį bendradarbiavimą ir formalųjį tarpinstitucinį bendradarbiavimą nėra minima.

Lietuvos Respublikos žemės ūkio ministerija remiantis ministerijos nuostatais formuoja efektyvius Europos Sąjungos valstybių patirtį atitinkančius rizikos ir krizių valdymo modelius ir priemones žemės ūkyje. Organizuoja jų įgyvendinimą ir ekstremaliųjų situacijų atvejais nustato specialiąsias apsaugos, padarinių šalinimo priemones. Tai pat yra Nekilnojamo turto kadastro duomenų saugos nuostatuose žemės ūkio ministerijai kaip Kadastro valdytojai yra taikomi ir naudojami kibernetinio saugumo dokumentai. Kibernetinio saugumo dokumentai tai yra saugos dokumentai į kuriuos įeina:

- ✓ kadastro duomenų saugos nuostatai;
- ✓ kadastro saugaus elektroninės informacijos tvarkymo taisyklės;
- ✓ kadastro veiklos tęstinumo valdymo planas;

- ✓ kadastro naudotojų administravimo taisyklė.

Už kibernetinio saugumo dokumentų santraukos parengimą atsakingas kibernetinio saugumo vadovas. Kibernetinio saugumo dokumentų santrauka rengiama remiantis būtinumo žinoti principu. Taigi pagal Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką 1 priede, išskiria šiuos Lietuvos Respublikos žemės ūkio ministerijos sektorius, subsektorius ir paslaugas (žr. 24 lent.).

24 lentelė. LR žemės ūkio ministerija – YSI objekto sektoriai, subsektoriai ir paslaugos

Atsakinga institucija	Sektorius	Subsektorius	Paslaugos
Letuvos Respublikos žemės ūkio ministerija	Maisto produktų sektorius	Maisto produktų tiekimo ir paskirstymo subsektorius	Žemės ūkio ir maisto produktų gamybos paslauga; Aprūpinimo maistu (valstybės atsargų saugojimo) paslauga; Maisto kokybės ir saugos užtikrinimo paslauga.

Šaltinis: parengta autorės pagal Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką, 1 priedas, 2018

Kaip matome 24 lentelėje remiantis Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką žemės ūkio ministerija esanti Kadastro valdytoja teikianti paslaugą nėra įtraukta. O ***analizuojant Lietuvos Respublikos žemės ūkio ministerijos nuostatus*** buvo pastebėta, kad veiklos tiksluose ir funkcijose yra minima ministerijos koordinavimas, kontroliavimas, organizavimas, dalyvavimas maisto produktų sektoriuje. Taigi galima daryti prielaida, žemės ūkio ministerija vykdo neformalųjį tarpinstitucinį bendradarbiavimą, tačiau formaliuoju būdu bendradarbiavimas su kitomis valstybės institucijomis nėra reglamentuotas. Taip pat yra nuostatuose yra sakoma, kad žemės ūkio ministerija atlieka valstybės registrų ir kadastrų:

- ✓ Ūkininkų ūkių registro;
- ✓ Lietuvos Respublikos fitosanitarinio registro;
- ✓ Lietuvos Respublikos žemės ūkio ir kaimo verslo registro;
- ✓ Lietuvos Respublikos patvirtintų pašarų ūkio subjektų registro;
- ✓ Ūkinių gyvūnų registro, Lietuvos Respublikos traktorių;
- ✓ Savaeigių ir žemės ūkio mašinų ir jų priekabų registro;
- ✓ Gyvūnų augintinių registro;
- ✓ Georeferencinio pagrindo kadastro;
- ✓ Nekilnojamojo turto kadastro valdytojo funkcijas.

Tačiau apie tarpinstitucinį bendradarbiavimą užtikrinant valdomų valstybės registrų kibernetinį saugumą nuostatuose nei formaliuoju nei neformaliuoju būdu nėra minima.

Lietuvos Respublikos Vyriausybė remiantis Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką 1 priede, išskiria šiuos Lietuvos Respublikos Vyriausybės sektorius, subsektorius ir paslaugas (žr. 25 lent.).

25 lentelė. LR Vyriausybė – YSI objekto sektoriai, subsektoriai ir paslaugos

Atsakinga institucija	Sektorius	Subsektorius	Paslaugos
Lietuvos Respublikos Vyriausybė	Valstybės valdymo sektorius	Valstybės valdžios funkcijų vykdymo subsektorius	Valstybės valdžios funkcijų vykdymo paslauga

Šaltinis: parengta autorės pagal Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką, 1 priedas, 2018

Analizuojant Lietuvos Respublikos Vyriausybės programoje buvo pastebėta, kad Vyriausybė pasižada sustiprinti šalies kibernetinio saugumo infrastruktūrą, gerinti tarpinstitucinį bendradarbiavimą kibernetinio saugumo srityje, užtikrinant kritinės informacinių ir ryšių technologijų infrastruktūros bei elektroninės informacijos saugumą ir visuomenės supratimą apie saugaus naudojimosi elektronine erdve svarbą. Taip pat stiprinti strategini komunikaciją, įdiegti kibernetinio saugumo informacinį tinklą ir automatizuoti prevencinių priemonių taikymą. Reguliariai organizuoti nacionalines kibernetinio saugumo pratybas. Tačiau analizuojant Lietuvos Respublikos Vyriausybės kanceliarijos nuostatus buvo pastebėta, kad veiklos tiksluose ir funkcijose apie valstybės valdžios funkcijų vykdymą bendradarbiaujant su kitomis valstybės institucijomis užtikrinant kibernetinį saugumą nėra minima.

Lietuvos Respublikos teisingumo ministerija. Remiantis Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką 1 priede, išskiria šiuos Lietuvos Respublikos teisingumo ministerijos sektorius, subsektorius ir paslaugas (žr. 26 lent.).

26 lentelė. LR teisingumo ministerija – YSI objekto sektoriai, subsektoriai ir paslaugos

Atsakinga institucija	Sektorius	Subsektorius	Paslaugos
Lietuvos Respublikos teisingumo ministerija	Viešojo saugumo ir teisinės tvarkos sektorius	Viešojo saugumo ir teisinės tvarkos užtikrinimo subsektorius	Teisminės ir baudžiamosios sistemos veikimo paslauga

Šaltinis: parengta autorės pagal Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką, 1 priedas, 2018

Analizuojant Lietuvos Respublikos teisingumo ministerijos nuostatus buvo pastebėta, kad ministerija daugiausiai bendradarbiauja su kitomis valstybės institucijomis rengiant teisės aktus, atstovaujant institucijų ir valstybės interesus teismuose. Taip pat kartu su valstybės institucijomis rengia

mokslines konferencijas teisės teorijos ir praktikos klausimais, kaupia, analizuoja ir apibendrina teorinę ir praktinę teisinę medžiagą. Nepaisant tai, kad teisingumo ministerija yra atsakinga YSII už teisminės ir baudžiamosios sistemos veikimo paslauga, nuostatuose apie tarpinstitucinį bendradarbiavimą užtikrinant kibernetinį saugumą nėra minima.

Lietuvos Respublikos krašto apsaugos ministerija. Remiantis Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką 1 priede, išskiria šiuos Lietuvos Respublikos krašto apsaugos ministerijos sektorius, subsektorius ir paslaugas (žr. 27 lent.).

27 lentelė. LR krašto apsaugos ministerija – YSI objekto sektoriai, subsektoriai ir paslaugos

Atsakinga institucija	Sektorius	Subsektorius	Paslaugos
Lietuvos Respublikos krašto apsaugos ministerija	Krašto apsaugos sektorius	Valstybės gynybos subsektorius	Valstybės ginkluotos gynybos paslauga

Šaltinis: parengta autorės pagal Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką, 1 priedas, 2018

Analizuojant Lietuvos Respublikos krašto apsaugos ministerijos nuostatus buvo pastebėta, kad Ministerija vykdo formalųjį tarpinstitucinį bendradarbiavimą organizuojant kariuomenės bendradarbiavimą su civilinėmis institucijomis, kurios tiesiogiai prisideda prie krašto apsaugos sistemos stiprinimo ir visuomenės parengimo Lietuvos gynybai. Taip pat bendradarbiauja su kitomis valstybės institucijomis rengiant piliečius ginkluotai krašto apsaugai, civilinei saugai ir ugdant pilietiškumą. Remiantis nuostatais, karšto apsaugos ministerija vykdo ir neformalųjį tarpinstitucinį bendradarbiavimą rengiant seminarus, konferencijas, simpoziumus, tarptautinius pasitarimus gynybos ir bendradarbiavimo klausimais, koordinuoti ministerijų, kitų Vyriausybės įstaigų, vietos savivaldos vykdomųjų institucijų veiklą Lietuvos gynybos ir civilinės saugos srityje.

Apibendrinant valstybės institucijų tarpinstitucinio bendradarbiavimo formavimo procesų analizė, remiantis LR teisės aktais galima daryti išvada, kad tarpinstitucinis bendradarbiavimas kibernetinio saugumo srityje Lietuvoje yra neišplėtotas. Valstybės institucijų nuostatuose nepakankamai išvystyta bendradarbiavimo kultūra centrinės valdžios ir institucijų lygmeniu. Institucijos įvairių valstybės sektorių nebendradarbiauja neformaliuoju būdu. Nepaisant tai, kad visos nagrinėjamos valstybės institucijos yra įtrauktos į ypatingos svarbos infrastruktūros sąrašą, tarpinstitucinis bendradrbiavimas užtikrinant kibernetinį saugumą, jų nuostatuose nėra reglamentuotas. Tai pat valstybės institucijų nuostatuose matyti, kad jos maksimaliai neišnaudoja viena kitos stipriąsias puses.

Galimai tai įtakoja nuostatuose kibernetinio saugumo užtikrinimo tikslu nebuvimas, o tai savo ruožtu atspindi jų veiklos tikslai ir funkcijos.

3.3. Tarpinstitucinio bendradarbiavimo Lietuvoje kibernetinio saugumo srityje ypatumai

2020 m. kovo mėn. Vilniuje buvo atlikta ekspertų apklausa, kurios tikslas – ištirti ir apibrėžti Lietuvos tarpinstitucinio bendradarbiavimo kibernetinio saugumo srityje ypatumus. Uždavinys minėtam tikslui pasiekti buvo nustatyti kokiu būdu vyksta valstybės institucijų atsakingu už ypatingos svarbos infrastruktūros objektus (toliau YSI objekati) ir ypatingos svarbos informacines infrastruktūras (toliau YSII) bendradarbiavimas su Nacionaliniu kibernetinio saugumo centru (toliau NKSC) ir atvirkščiai: formaliuoju (reglamentuotu teisės aktuose), neformaliuoju (nereglamentuotu teisės aktuose: neformalūs susitikimai, pokalbiai telefonu, seminarai, mokymai, konferencijos, susirašinėjimai el. paštu, koordinavimas ir kita) ar mišriuoju būdu (formaliuoju ir neformaliuoju).

Tyrime dalyvavo 13 valstybės institucijų. Kiekviena instituciją atstovavo vienas ekspertas turintis profesinės patirties, kompetencijos ir patikimą bei pakankamai išsamią informaciją apie tiriamą problemą. Kiekvienam respondentui buvo paaiškintas tyrimo tikslas bei kur ir kaip bus panaudota iš jų gauta informacija. Ekspertų apklausai pasirinktas apklausos anketavimo būdas, kuri sudarė anketa iš atvirų ir uždarų 7 – 10 klausimų. Apklausa vyko raštu sudarant anketavimą. Ekspertui elektroniniu paštu buvo siunčiamas klausimynas anketa ir prašoma ją užpildyti.

Nacionalinio kibernetinio saugumo centro apklausos rezultatai

Siekiant nustatyti tarpinstitucinį bendradarbiavimą NKSC su kitomis valstybės institucijomis buvo panaudotas ekspertų vertinimo metodas. Ekspertų metodas padėjo nustatyti kokiu būdu Nacionalinis kibernetinio saugumo centras formaliuoju ar neformaliuoju NKSC vykdo tarpinstitucinį bendradarbiavimą su valstybės institucijomis.

Reflektuojant eksperto apklausos rezultatus buvo nustatyta, kad NKSC vykdo tarpinstitucinį bendradarbiavimą su valstybės institucijomis atsakingomis už YSII (***1.*** *Ar vykdote tarpinstitucinį bendradarbiavimą su valstybės institucijomis atsakingomis už YSI objektus ir YSII? Atasakimas:* ***- NKSC vykdo tarpinstitucinį bendradarbiavimą su valstybės institucijomis atsakingomis už YSII***). Toliau buvo nustatyta, kad NKSC tarpinstitucinį bendradarbiavimą su valstybės institucijomis atsakingomis už YSII vykdo teisės aktuose numatytais atvejais, taip pat iškilus poreikiui YSII valdytojams ar NKSC siekiant užtikrinti kibernetinį saugumą jų valdomoje infrastruktūroje (***2.*** *Kokiais atvejais vykdote tarpinstitucinį bendradarbiavimą su valstybės institucijomis atsakingomis už YSI objektus ir YSII? Atsakimas:* ***- NKSC tarpinstitucinį bendradarbiavimą su valstybės institucijomis atsakingomis už YSII vykdo teisės aktuose numatytais atvejais, taip pat iškilus poreikiui YSII valdytojams ar NKSC siekiant užtikrinti kibernetinį saugumą jų valdomoje infrastruktūroje).*** Nustatytas vyraujantis tarpinstitucinis

bendradarbiavimo būdas tarp NKSC ir valstybės institucijomis atsakingomis už YSII kuris vykdomas mišriuoju būdu *(**3.** Kokiais būdais vykdote tarpinstitucinį bendradarbiavimą: formaliuoju (reglamentuoja teisės aktai), neformaliuoju (pagal poreikį, nereglamentuojamas) ar mišriuoju? Atsakimas: - **NKSC tarpinstitucinį bendradarbiavimą vykdo mišriuoju būdu).*** NKSC vykdo tarpinstitucini bendradrbiavimą su valstybės institucijomis atsakingomis už YSII visą parą kiekvieną dieną *(**4.** Kaip dažnai vykdote tarpinstitucinį bendradarbiavimą su valstybės institucijomis atsakingomis už YSI objektus ir YSII? Atsakimas: - **24/7).*** Nustatyta, kad vyraujančios priemonės kurių pagalba NKSC bendradarbiauja formaliuoju ir neformaliuoju būdu su valstybės institucijomis atsakingomis už YSII yra susitikimai, susirašinėjimas el. paštu, pokalbiai telefonu, konferencijos, mokymai, vaizdo pokalbiai *(**5.** Kokiomis priemonėmis vykdote tarpinstitucinį bendradarbiavimą: jeigu vykdote formaliuoju būdu (susitikimai, el. paštas, telefonu, konferencijos, mokymai, vaizdo pokalbiai ar kita-nurodyti) jeigu vykdote neformaliuoju būdu (susitikimai, el. paštas, telefonu, konferencijos, mokymai, vaizdo pokalbiai ar kita- nurodyti)? Atsakimas: - **Visomis išvardintomis).*** Taip pat nustatyta, NKSC vykdo neformaliuojų būdu tarpinstitucinį bendradarbiavimą su valstybės institucijomis atsakingomis už YSII *(**6.** Jeigu nevykdote neformaliuoju būdu tarpinstitucinio bendradarbiavimo tai Jūsų nuomonė toks bendradarbiavimo būdas yra naudingas LR užtikrinant kibernetinį saugumą? Pagrįskite savo atsakymą. Atsakimas: - **Vykdome).*** Pagal NKSC poreikis reglamentuoti neformalųjį tarpinstitucinio bendradarbiavimo būdą LR teisės aktuose nustatyta, kad nėra, nes tai tik biurokratizuotų bendradarbiavimą *(**7.** Jūsų nuomonė ar yra poreikis reglamentuoti neformalųjį būdą tarpinstitucinio bendradarbiavimo LR teisės aktuose? Atsakimas: - **Poreikio reglamentuoti neformalųjį tarpinstitucinio bendradarbiavimo būdą LR teisės aktuose nėra, tai tik biurokratizuotų bendradarbiavimą).***

Apibendrinant Nacionalinio kibernetinio saugumo centro apklausos rezultatus galima daryti išvadą, kad NKSC vykdoma 24/7 tarpinstitucinį bendradarbiavimą mišriuoju būdu gerina sąveiką tarp valstybės institucijų atsakingu už YSII remiantis ne tik teisinių reglamentavimų, bet ir neformaliuoju tarpinstituciniu bendradarbiavimu kuriame vyrauja labai svarbus gebėjimas greitai priimti ir perduoti informaciją. Nepaisant tai, kad NKSC tarpinstitucinis bendradarbiavimas formuojasi ne tik remiantis teisės aktais, bet ir *neformaliuoju būdu (susitikimai, el. paštas, telefonu, konferencijos, mokymai, vaizdo pokalbiai* parodo, kad NKSC įžvelgia poreikį stiprinti informacinės visuomenės saugumą, suteikiant valstybės tarnyboms ir savivaldos darbuotojams žinių kibernetinio saugumo srityje, kad jie gebėtų įvertinti kibernetinio saugumo rizikas ir taikyti efektyvias kibernetinio saugumo priemones savo informacinių sistemų apsaugai ir tokiu būdu prisidėti prie saugios informacinės visuomenės kūrimo proceso Lietuvos valstybiniame sektoriuje.

Valstybės institucijų eksperto apklausos anketa

Siekiant nustatyti tarpinstitucinį bendradarbiavimą valstybės institucijų atsakingu už YSII su Nacionaliniu kibernetinio saugumo centru buvo panaudotas ekspertų vertinimo metodas kuris padėjo nustatyti kokiu būdu valstybės institucijos formaliuoju ar neformaliuoju vykdo tarpinstitucinį bendradarbiavimą su Nacionaliniu kibernetinio saugumo centru. Tyrime dalyvavo 12 valstybės institucijų iš kuriu LR Vyriausybė nedalyvavo. Buvo nustatyta, kad visos 11 valstybės institucijų atsakingu už YSII vykdo tarpinstitucinį bendradarbiavimą su NKSC (žr. 28 lent.).

28 lentelė. Ar vykdote tarpinstitucinį bendradrbiabimą su NKSC?

1. Klausimas / Atsakymas	LR vidaus reikalų ministerija	LR aplinkos ministerija	LR ūkio ministerija	LR susisiekimo ministerija	LR sveikatos apsaugos m.	LR finansų ministerija	LR krašto apsaugos m.	LR žemės ūkio ministerija	LR užsienio reikalų m.	LR energetikos ministerija	LR teisingumo ministerija	LR Vyriausuybė
a) *taip* ***b)*** *ne*	**a)**	**a)**	**a)**	**a)**	**a)**	**a)**	**a)**	**a)**	**a)**	**a)**	**a)**	**X**

Šaltinis: parengta autorės

Valstybės institucijos, išskyrus LR sveikatos apsaugos ministerija, vykdo tarpinstitucinį bendradarbiavimą su NKSC mišriu būdu. LR sveikatos apsaugos ministerija vykdo tarpinstitucinį bendradarbiavimą formaliuoju būdu (žr. 29 lent.).

29 lentelė. Kaip vykdote tarpinstitucinį bendradrbiabimą su NKSC?

2. Klausimas / Atsakymas	LR vidaus reikalų ministerija	LR aplinkos ministerija	LR ūkio ministerija	LR susisiekimo ministerija	LR sveikatos apsaugos m.	LR finansų ministerija	LR krašto apsaugos m.	LR žemės ūkio ministerija	LR užsienio reikalų m.	LR energetikos ministerija	LR teisingumo ministerija	LR Vyriausuybė
a) *formaliuoju būdu* ***b)*** *neformaliuoju būdu* ***c)*** *mišriu (derinant formalųjį ir neformalųjį bendradrbiavimo būdą)*	**c)**	**c)**	**c)**	**c)**	**a)**	**c)**	**c)**	**c**	**c)**	**c)**	**c)**	**X**

Šaltinis: parengta autorės

Visos valstybės institucijos formaliuoju būdu bendradarbiauja incidentų atvejais, kaip reglamentuota teisės aktuose. Prevenciškai du trečdaliai valstybės institucijų vykdo tarpinstitucinį bendradarbiavimą. Taip pat toks kiekis valstybės institucijų bendradarbiaujant dalyvauja ir mokymuose (žr. 30 lent.).

30 lentelė. Kokiais atvejais vykdomas tarpinstitucinis bendradarbiavimas su NKSC formaliuoju būdu?

3. Klausimas / Atsakymas	LR vidaus reikalų m.	LR aplinkos ministerija	LR ūkio ministerija	LR susisiekimo ministerija	LR sveikatos apsaugos m.	LR finansų ministerija	LR krašto apsaugos m.	LR žemės ūkio ministerija	LR užsienio reikalų m.	LR energetikos ministerija	LR teisingumo ministerija	LR Vyriausybė
a) *incidentų atvejais* ***b)*** *prevenciškai* ***c)*** *mokymai* ***d)*** *kiti (nurodyti konkrečius atvejus)*	**a)** **b)**	**a)** **b)** **c)**	**a)** **b)**	**a)** **b)** **c)**	**a)**	**a)** **b)** **c)**	**a)** **b)** **c)**	**a)**	**a)** **b)** **c)**	**a)** **c)**	**a)** **c)**	**X**

Šaltinis: parengta autorės

Nagrinėjant priemonės paaiškėjo, kad kai kurios valstybės institucijos vykdant tarpinstitucinį bendradarbiavimą naudojasi *Kibernetinio saugumo informaciniu tinklu* (toliau **d)-KSIT**) (žr. 31 lent.).

31 lentelė. Kokiomis priemonėmis vykdote tarpinstitucinį bendradarbiavimą formaliuoju būdu su NKSC?

4. Klausimas / Atsakymas	LR vidaus reikalų m.	LR aplinkos ministerija	LR ūkio ministerija	LR susisiekimo ministerija	LR sveikatos apsaugos m.	LR finansų ministerija	LR krašto apsaugos m.	LR žemės ūkio ministerija	LR užsienio reikalų m.	LR energetikos ministerija	LR teisingumo ministerija	LR Vyriausybė
a) *susitikimai* ***b)*** *telefono pokalbiai* ***c)*** *el. paštu* ***d)*** *kitos priemonės (nurodyti konkrečias priemonės)*	**a)** **b)** **c)** **d)**	**a)** **b)** **c)**	**a)** **b)** **c)**	**a)** **b)** **c)**	**b)** **c)**	**a)** **b)** **c)** **d)**	**a)** **b)** **c)** **d)**	**b)** **c)**	**a)** **b)** **c)** **d)**	**a)** **b)** **c)** **d)**	**b)** **c)** **d)**	**X**

Šaltinis: parengta autorės

Valstybės institucijos atsakingos už YSII vykdo tarpinstitucinį bendradarbiavimą formaliuoju būdu su NKSC nuo 1 iki 3 mėnesio laikotarpyje, tačiau LR vidaus reikalų ministerijos ekspertas pareiškė, kad bendradarbiauja su NKSC *kas metus (t.y. karta per metus) arba pagal poreikį* (žr. 32 lent.).

32 lentelė. Kaip dažnai vykdomas tarpinstitucinis bendradarbiavimas formaliuoju būdu su NKSC?

5. Klausimas / **Atsakymas**	LR vidaus reikalų m.	LR aplinkos ministerija	LR ūkio ministerija	LR susisiekimo ministerija	LR sveikatos apsaugos m.	LR finansų ministerija	LR krašto apsaugos m.	LR žemės ūkio ministerija	LR užsienio reikalų m.	LR energetikos ministerija	LR teisingumo ministerija	LR Vyriausybė
a) *1-3 mėn.* ***b)*** *3-6 mėn.* ***c)*** *6-12 mėn.* ***d)*** *12 mėn. ir daugiau*	Kas metus arba pagal poreikį	**a)**	**a)**	**a)**	**a)**	**a)**	**a)**	**a)**	**a)**	**a)**	**a)**	**X**

Šaltinis: parengta autorės

Dauguma valstybės institucijų neformaliuoju būdu vykdo tarpinstitucinį bendradarbiavimą su NKSC incidentų atvejais ir prevenciškai. LR vidaus reikalų ministerija išskyrus minėtu atveju bendradarbiauja su NKSC *aiškinantis kibernetinio saugumo reikalavimų turinį ir įgyvendinimo būdus* ***(d)***, o LR sveikatos apsaugos ministerija nepateikė atsakymo (žr. 33 lent.).

33 lentelė. Kokiais atvejais vykdomas tarpinstitucinis bendradrbiavimas su NKSC neformaliuoju būdu?

6. Klausimas / **Atsakymas**	LR vidaus reikalų m.	LR aplinkos ministerija	LR ūkio ministerija	LR susisiekimo ministerija	LR sveikatos apsaugos m.	LR finansų ministerija	LR krašto apsaugos m.	LR žemės ūkio ministerija	LR užsienio reikalų m.	LR energetikos ministerija	LR teisingumo ministerija	LR Vyriausybė
a) *incidentų atvejais* ***b)*** *prevenciškai* ***c)*** *mokymai* ***d)*** *kiti (nurodyti konkrečius atvejus)*	**a)** **b)** **d)**	**b)**	**b)**	**a)** **b)**	**X**	**b)**	**a)** **b)**	**a)** **b)**	**a)** **b)**	**a)** **b)**	**a)** **b)**	**X**

Šaltinis: parengta autorės

Šešios valstybės institucijos vykdant tarpinstitucinį bendradarbiavimą neformaliuoju būdu naudojasi *Kibernetinio saugumo informaciniu tinklu* (toliau **d)-KSIT**), o du iš ju naudoja kaip priemonė neformalūs susitikimai. Bendrai visos valstybės institucijos atsakingos už YSII neformaliajame bendradarbiavime naudojasi el. paštu ir telefono pokalbiais (žr. 34 lent.).

34 lentelė. Kokiomis priemonėmis vykdote tarpinstitucinį bendradarbiavimą neformaliuoju būdu su NKSC?

7. Klausimas / **Atsakymas**	LR vidaus reikalų ministerija	LR aplinkos ministerija	LR ūkio ministerija	LR susisiekimo ministerija	LR sveikatos apsaugos m.	LR finansų ministerija	LR krašto apsaugos m.	LR žemės ūkio ministerija	LR užsienio reikalų m.	LR energetikos ministerija	LR teisingumo ministerija	LR Vyriausuybė
a) *susitikimai* ***b)*** *telefono pokalbiai* ***c)*** *el. paštas* ***d)*** *kitos priemonės (nurodyti konkrečias)*	**a)** **b)** **c)** **d)**	**b)** **c)**	**b)** **c)**	**b)** **c)**	**X**	**b)** **c)** **d)**	**a)** **b)** **c)** **d)**	**b)** **c)**	**b)** **c)** **d)**	**b)** **c)** **d)**	**b)** **c)** **d)**	**X**

Šaltinis: parengta autorės

LR vidaus reiklų ministerija vykdo neformalųjį tarpinstitucinį bendradarbiavimą pagal poreikį, labai nereguliariai. Visos kitos institucijos taip pat kaip naudojant formalųjį bendradarbiavimo būdą nuo 1 iki 3 mėnesio laikotarpyje. LR sveikatos apsaugos ministerija nepateikė atsakymo ir tai byloja apie neformaliojo būdo nebuvimą bendradarbiaujant su NKSC (žr. 35 lent.).

35 lentelė. Kaip dažnai vykdomas tarpinstitucinis bendradarbiavimas neformaliuoju būdu su NKSC?

8. Klausimas / **Atsakymas**	LR vidaus reikalų m.	LR aplinkos ministerija	LR ūkio ministerija	LR susisiekimo ministerija	LR sveikatos apsaugos m.	LR finansų ministerija	LR krašto apsaugos m.	LR žemės ūkio ministerija	LR užsienio reikalų m.	LR energetikos ministerija	LR teisingumo ministerija	LR Vyriausuybė
a) *1-3 mėn.* ***b)*** *3-6 mėn.* ***c)*** *6-12 mėn.* ***d)*** *12 mėn. ir daugiau*	**d)** pagal poreikį, labai nereguliariai	**a)**	**a)**	**a)**	**X**	**a)**	**a)**	**a)**	**a)**	**a)**	**a)**	**X**

Šaltinis: parengta autorės

Visos valstybės institucijos yra patenkintos tarpinstituciniu bendradarbiavimu su NKSC, išskyrus LR vidaus reikalų ministerijos, kuria iš dalies NKSC tenkina bendradarbiavimo poreikius (žr. 36 lent.).

36 lentelė. Jūsų nuomonė ar tarpinstitucinio bendradarbiavimo kokybė su NKSC tenkina Jūsų poreikius?

9. Klausimas / Atsakymas	LR vidaus reikalų ministerija	LR aplinkos ministerija	LR ūkio ministerija	LR susisiekimo ministerija	LR sveikatos apsaugos m.	LR finansų ministerija	LR krašto apsaugos m.	LR žemės ūkio ministerija	LR užsienio reikalų m.	LR energetikos ministerija	LR teisingumo ministerija	LR Vyriausuybė
a) *tenkina* ***b)*** *netenkina* ***c)*** *iš dalies tenkina*	**c)**	**a)**	**a)**	**a)**	**a)**	**a)**	**a)**	**a)**	**a)**	**a)**	**a)**	**X**

Šaltinis: parengta autorės

Visos valstybės institucijos atsakingos už YSII pateikė atsakymą, kad neformaliojo būdo reglamentavimo poreikio tarpistituciniame bendradarbiavime *nėra* (žr. 37 lent.).

37 lentelė. Neformaliojo būdo reglamentavimo poreikis tarpistituciniame bendradrbiavime

10. Klausimas / Atsakymas	LR vidaus reikalų ministerija	LR aplinkos ministerija	LR ūkio ministerija	LR susisiekimo ministerija	LR sveikatos apsaugos m.	LR finansų ministerija	LR krašto apsaugos m.	LR žemės ūkio ministerija	LR užsienio reikalų m.	LR energetikos ministerija	LR teisingumo ministerija	LR Vyriausuybė
Jūsų nuomonė ar yra poreikis reglamentuoti neformalią būdą tarpinstitucinio bendradarbiavimo LR teisės aktuose užtikrinant kibernetinį saugumą?	Esminio poreikio nėra	Nėra. Tarpinstitucinį bendradarbiavimas taps formaliuoju.	Poreikio nėra	Poreikio nėra	Poreikio nemato	Poreikio nėra	Poreikio nėra	Poreikio nėra	Poreikio nėra	Poreikio nėra	Poreikio nėra	**X**

Šaltinis: parengta autorės

Apibendrinant ekspertų (valstybės institucijos atsakingos už YSII) apklausos anketą buvo nustatyta, kad visos valstybės institucijos atsakingos už YSII vykdo tarpinstitucinį bendradarbiavimą su NKSC mišriu būdu, išskyrus LR sveikatos apsaugos ministerija. Institucijos formaliuoju būdu bendradarbiauja incidentų atvejais, kaip reglamentuota teisės aktuose. Du trečdaliai (apie 33%) valstybės institucijų prevenciškai vykdo tarpinstitucinį bendradarbiavimą. Taip pat 33% valstybės institucijų bendradarbiaujant dalyvauja ir mokymuose. Tam apie 60% valstybės institucijų naudojasi Kibernetinio saugumo informaciniu tinklu. Kitos vyraujančios bendradarbiavimo priemonės el. paštas, telefono pokalbiai ir susitikimai. Tarpinstitucinis bendradarbiavimas formaliuoju būdu su NKSC vyksta nuo 1 iki 3 mėnesio laikotarpyje, tačiau LR vidaus reikalų ministerijos ekspertas pareiškė, kad bendradarbiauja su NKSC kas metus (t.y. karta per metus) arba pagal poreikį.

Dauguma valstybės institucijų neformaliuoju būdu vykdo tarpinstitucinį bendradarbiavimą su NKSC incidentų atvejais ir prevenciškai. LR vidaus reikalų ministerija išskyrus minėtu atveju bendradarbiauja su NKSC aiškinantis kibernetinio saugumo reikalavimų turinį ir įgyvendinimo būdus. Apie 60% valstybės institucijų vykdo tarpinstitucinį bendradrbiavimą neformaliuoju būdu naudojantis Kibernetinio saugumo informaciniu tinklu. Bendrai visos valstybės institucijos atsakingos už YSII neformaliajame bendradarbiavime naudojasi el. paštu ir telefono pokalbiais. o apie 20% iš ju naudoja kaip priemonė neformalūs susitikimai.

LR vidaus reiklaų ministerija vykdo neformalųjį tarpisntitucinį bendradarbiavimą pagal poreikį, labai ne reguliariai, o visos kitos institucijos bendradarbiauja nuo 1 iki 3 mėnesio laikotarpyje. LR sveikatos apsaugos ministerija nepateikė atsakymo ir tai byloja apie neformaliuojo būdo nebuvimą bendradarbiaujant su NKSC.

Tyrimas parodė, kad isntitucijos yra patenkintos tarpinstituciniu bendradarbiavimu su Nacionaliniu kibernetinio saugumo centru, išskyrus LR vidaus reikalų ministerijos, kurios NKSC poreikius tenkina iš dalies, tačiau pastebėtina, kad valstybės institucijos vangiai dalyvauja mokymuose. Poreikį reglamentuoti LR teisės aktuose neformalųjį tarpistitucinio bendradarbiavimo būdą valstybės institucijos atsakingos už YSII nemato.

IŠVADOS IR *PASIŪLYMAI*

1. Kibernetinis saugumas yra naujai ir plačiai vartojamas terminas, kurio apibrėžimai yra labai skirtingi, dažnai subjektyvus, o kartais ir neinformatyvus. Taigi galima laikytis nuomonės, kad kibernetinis saugumas yra veiksmų visumą, kur pasitelkiant į išteklius, **bendradarbiavimą**, procesus ir struktūras, palaikoma ir apsaugoma kibernetinė erdvė nuo organizuotu kibernetinių atakų ir nusikaltimų. **Formalus bendradarbiavimas** yra vienas iš pagrindinių tarpinstitucino bendradarbiavimo būdu, kurio procedūros reglamentuotos ir apibrėžtos teisės aktuose. Tačiau **stiprinantis tarpinstitucinį bendradarbiavimą kibernetinio saugumo srityje yra neformalus bendradarbiavimo būdas**, kuris paskatina glaudesnį tarpinstitucinį bendradarbiavimą ir neformalia tinklaveiką. Pagrindinis ir **esminis ypatumas** tarpinstituciniame bendradarbiavime kibernetinio saugumo srityje yra **visavertė partnerystė grindžiamą informacijos keitimosi**. **Informavimo principas** bendradarbiaujant sukuria galimybė susipažinti su kitų institucjų veikla, jos specifika bei kita aktualia informacija ir dalintis svarbia informacija. Lietuvoje tarpinstituciniame bendradarbiavime kibernetinio suagumo srityje vyrauja **mišrus: hierarchinis/tinklų modelis**. Koordinavimo priemonė yra teisės aktai, o valdymas grindžiamas suinteresuotųjų grupių tinkle pagal veiklos planą. Tarpinstitucinio bendradarbiavimo valdant ir tiriant kibernetinius incidentus tvarka nustatoma Nacionaliniame kibernetinių incidentų valdymo priemonėse.

2. Tarpinstitucinio bendradarbiavimo Lietuvoje kibernetinio saugumo srityje empirinis tyrimas, susideda iš trijų etapu. ***Pirmame etape*** analizuojami NKSC tarpinstitucinio bendradarbiavimo ypatumai ir skatinančios priemonės pasitelkiant į teisini reglamentavimą ir veiklos ataskaitos. ***Antrame etape*** analizuojamos dvylika valstybės institucijų kurios atsakingos už ypatingos svarbos infrastruktūros objektus ir ypatingos svarbos informacinė infrastruktūra tarpinstitucinio bendradarbiavimo ypatumai ir skatinančios priemonės pasitelkiant į institucijų veiklos planus ir bendra teisinį reglamentavimą. ***Trečiame etape*** siekiant nustatyti tarpinstitucinį bendradarbiavimą NKSC su kitomis valstybės institucijomis ir siekiant nustatyti tarpinstitucinį bendradarbiavimą valstybės institucijų atsakingu už YSI objektus ir YSII su NKSC panaudotas ekspertų vertinimo metodas – ***apklausos anketavimo būdas***. Ekspertų metodas pasirinktas, siekiant pateikti kokiu būdu formaliuoju ar neformaliuoju NKSC ir valstybės institucijos vykdo tarpinstitucinį bendradarbiavimą. Anketa suformuota iš uždaru ir atviru 7 – 10 klausimų. Buvo išlaikytas respondentų anonimiškumas.

3. Valstybės institucijų tarpinstitucinio bendradarbiavimo formavimo procesų analizė, remiantis LR teisės aktais parodė, kad tarpinstitucinis **bendradarbiavimas formaliuoju būdu kibernetinio saugumo srityje Lietuvoje yra neišplėtotas**. **Kibernetinio saugumo sritis reglamentuota fragmentiškai ir nenuosekliai.** Valstybės institucijų nuostatuose nepakankamai išplėtota bendradarbiavimo kultūra centrinės valdžios ir institucijų lygmeniu ir tai įtakoja valstybės institucijų įvairių sektorių bendradarbiavimo nebuvimą. Nepaisant tai, kad visos nagrinėjimos valstyvės institucijos

yra įtrauktos į ypatingos svarbos infrastruktūros sąrašą, **tarpinstitucinis bendradarbiavimas užtikrinant kibernetinį saugumą, jų nuostatuose nėra reglamentuotas**. Tai pat valstybės institucijų nuostatuose matyti, kad jos maksimaliai neišnaudoja viena kitos stipriąsias puses. Galimai tai įtakoja nuostatuose tarpinstitucinio bendradarbiavimo kibernetinio saugumo užtikrinimo tikslu nebuvimas, o tai savo ruožtu atspindi valstybės institucijų veiklos tiksluose ir funkcijuose.

a) NKSC tarpinstitucinio bendardarbiavimo formavimo procesų analizė parodė, kad tarpinstitucinis bendradarbiavimas formuojasi ne tik remiantis teisės aktais kuriuose reglamentuotas bendradarbiavimas įvykus incidentams. NKSC įžvelgia neformaliojo bendradarbiavimo būdo poreikį, kuris padės stiprinti informacinės visuomenės saugumą, efektyviai taikyti kibernetinio saugumo priemones informacinių sistemų apsaugai. ***NKSC*** dalyvauja valstybės institucijų mokymų organizavime (*„Kibernetinis skydas 2019“, „Kompleksiniai kibernetinės saugos mokymai valstybės ir savivaldybių institucijų ir įstaigų darbuotojams*“) ***vykdant neformalųjį tarpinstitucinį bendradarbiavimą*** taip prisidedant prie saugios informacinės visuomenės kūrimo proceso Lietuvos valstybiniame sektoriuje.

b) Valstybės institucijų bendradarbiavimo formavimo procesų analizė parodė, kad tarpinstitucinis bendradarbiavimas kibernetinio saugumo srityje Lietuvoje yra neišplėtotas. Tai parodė valstybės institucijų nuostatų analizė, kuriuose nepakankamai išvystyta bendradarbiavimo kultūra centrinės valdžios ir institucijų lygmeniu. Institucijos įvairių valstybės sektorių nebendradarbiauja neformaliuoju būdu. Nepaisant tai, kad visos nagrinėjamos valstybės institucijos yra įtrauktos į ypatingos svarbos infrastruktūros sąrašą, tarpinstitucinis bendradarbiavimas užtikrinant kibernetinį saugumą, jų nuostatuose nėra reglamentuotas. Tai pat valstybės institucijų nuostatuose matyti, kad jos maksimaliai neišnaudoja viena kitos stipriąsias puses. Galimai tai įtakoja nuostatuose kibernetinio saugumo užtikrinimo tikslu nebuvimas, o tai savo ruožtu atspindi jų veiklos tikslai ir funkcijos.

c) Tarpinstitucinio bendradarbiavimo Lietuvoje kibernetinio saugumo srityje ypatumų analizė parodė, kad tarpinstitucinis bendradarbiavimas vyksta mišriuoju būdu, remiantis ne tik teisinių reglamentavimų, bet ir neformaliuoju tarpinstituciniu bendradarbiavimu. Tyrimo metu buvo nustatyta, kad visos valstybės institucijos ir NKSC formaliuoju būdu bendradarbiauja incidentų atvejais, kaip reglamentuota teisės aktuose. Neformaliuoju būdu apie 33% valstybės institucijų prevenciškai vykdo tarpinstitucinį bendradarbiavimą aiškinantis kibernetinio saugumo reikalavimų turinį ir įgyvendinimo būdus, o kiti 33 % valstybės istitucijų bendradarbiaujant dalyvauja ir mokymuose. Vienas iš vyraujančio tarpinstitucinio bendradarbiavimo (formaliuoju ir neformaliuoju būdu) priemonių ypatumo yra tai, kad apie 60% valstybės institucijų naudojasi Kibernetinio saugumo informaciniu tinklu, likusieji pasirinko bendradarbiavimo priemonės el. paštą, telefono pokalbius ir susitikimus. Tarpinstitucinis bendradarbiavimas formaliuoju būdu ir neformaliuoju būdu vyksta nuo 1 iki 3 mėnesio laikotarpyje. Tyrimas parodė, kad institucijos bendrai yra patenkintos tarpinstituciniu bendradarbiavimu, tačiau

pastebėtina, kad valstybės institucijos vangiai dalyvauja mokymuose. Poreikį reglamentuoti LR teisės aktuose neformalųjį tarpinstitucinio bendradarbiavimo būdą valstybės institucijos nemato.

4. Tyrimo hipotezė nepasitvirtino, kuri teigė, kad yra poreikis reglamentuoti Lietuvos Respublikos teisės aktuose neformalųjį tarpinstitucinį bendardarbiavimą kibernetinio saugumo srityje. Gauti rezultatai parodė, kad visos valstybės institucijos nemato poreikio reglamentuoti neformalųjį tarpistitucinio bendradarbiavimo būdą. Toks požiūris gali byloti apie nepakankamai išvystyta bendradarbiavimo kultūra centrinės valdžios ir institucijų lygmenyje.

5. Nors tyrimo rezultatai parodė, kad tarpinstitucinis bendradarbiavimas Lietuvoje kibernetinio saugumo srityje egzistuoja formaliuoju būdu ir pagal institucijų poreikį, neformaliuoju būdu, tačiau galutiniai rezultatai nesiekia siektinų. Siekiant padidinti tarpinstitucinio bendradarbiavimo produktyvumą, reikia sukurti bendradarbiavimo mokymosi mechanizmus. Tarpinstitucinio bendardarbiavimo tikslai užtikrinant kibernetinį saugumą turi būti organizuoti tiksliai, sistemingai ir nuolatiniai, tinkamai suderinti veiksmai ir aiški veikimo schema.

6. Reglamentuoti Lietuvos Respublikos teisės aktuose mokymu būtinumą. Mokymu procesas grindžiamas analizė ir dialogu, kuriame visi dalyviai bendradarbiauja taip ugdydami tarpinstitucinio bendradarbiavimo kultūrą. Tai padės efektyviai identifikuoti tarpistitucinio bendradarbiavimo užtikrinant kibernetinį saugumą problemas, išryškins institucijų bendradarbiavimo galimybės ir padės surasti optimalų tarpinstitucinio bendardarbiavimo užtikrinant kibernetinį saugumą sprendimo variantus.

LITERATŪRA

1. LR Vyriausybės nutarimas „Dėl vystomojo bendradarbiavimo tarpinstitucinio veiklos plano patvirtinimo“. 2016 m. rugsėjo 21 d. Nr. 937, Vilnius Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/728ed9a083e611e6a0f68fd135e6f40c?jfwid=-wd7z7yc3k

2. Tarpinstitucinio bendradarbiavimo analizės atlikimo, analogiškos patirties ES šalyse ir esamos teisinės bazės Lietuvoje įvertinimo galutinė ataskaita. Vilnius, 2012. Prieiga per internetą: http://www.esparama.lt/es_parama_pletra/failai/ESFproduktai/2012_tarpinstitucinio_bendradarbiavimo_analize.pdf

3. Jurkonienė, I. ir Karčiauskienė, R. (2017). Tarpinstitucinio bendradarbiavimo stiprinimo koncepcija. Prieiga per internetą: http://kurklt.lt/wp-content/uploads/2016/10/tarpinstitucinio-bendradarbiavimo-stiprinimo-koncepcija-final.pdf

4. Smith, D. & Katz, J. S. (2000). Collaborative Approaches to Research. Prieiga per internetą: http://users.sussex.ac.uk/~sylvank/pubs/collc.pdf

5. Vishik, C., Matsubara, M. & Plonk, A. (2016). Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms. CHAPTER 11, 221- 242. Prieiga per internetą: https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_Ch11.pdf

6. Guy Peters, B. (1998). Managing horizontal government // *The polititics of coordination*. Prieiga per internetą: http://publications.gc.ca/collections/Collection/SC94-61-21-1998E.pdf

7. Puškorius, S. (2007). Bendradarbiavimo efektyvumas. Prieiga per internetą: https://www.mruni.eu/upload/iblock/513/2_s.puskorius.pdf

8. Raišienė, A. G. (2015). Bendradarbiavimo kaip viešojo sektoriaus veiklos organizavimo alternatyvos teoriniai aspektai. 319. Prieiga per internetą: https://www.researchgate.net/publication/268288295_Bendradarbiavimo_kaip_viesojo_sektoriaus_veiklos_organizavimo_alternatyvos_teoriniai_aspektai

9. Amoroso, E. (2006). Cyber Security, New Jersey.

10. Department of Homeland Security, 2009. National Initiative Cybersecurity careers and studies // *Adapted from: CNSSI 4009, NIST SP 800-53 Rev 4, NIPP, DHS National Preparedness Goal; White House Cyberspace Policy Review, May 2009.* Prieiga per internetą: https://niccs.us-cert.gov/about-niccs/glossary#letter_c

11. Lewis, J. A. (2006). Cybersecurity and Critical Infrastructure Protection // *Center for Strategic and International Studies.* Prieiga per internetą: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/0601_cscip_preliminary.pdf

12. Committee on National Security Systems, (CNSS). 2010. National Information Assurance Glossary //*National Risk Management Policy and Framework for National Security Systems* // CNSS Instruction No. 4009 Prieiga per internetą: https://www.hsdl.org/?abstract&did=7447

13. International Telecommunication Union ITU. (2009). Overview of Cybersecurity // *Recommendation ITU-T X.1205. Geneva*. Prieiga per internetą: https://www.itu.int/rec/T-REC-X.1205-200804-I/en

14. Kemmerer, R. A. (2003). Cybersecurity. // *Proceedings of the 25th IEEE International Conference on Software Engineering* // 705-715. Prieiga per internetą: https://ieeexplore.ieee.org/document/1201257

15. Government of Canada, (2018). Emergency management vocabulary // *Public Works and Government Services. Canada. 2012//* 24. Prieiga per internetą: http://publications.gc.ca/site/eng/417764/publication.html

16. Canongia, C., & Mandarino, R. (2014). Cybersecurity: The New Challenge of the Information Society // *In Crisis Management: Concepts, Methodologies, Tools and Applications: 60-80. Hershey, PA: IGI Global*. Prieiga per internetą: https://www.igi-global.com/gateway/chapter/90712#pnlRecommendationForm

17. Oxford dictionaries, (2018). Prieiga per internetą: https://en.oxforddictionaries.com/definition/Cybersecurity

18. Viešosios politikos ir vadybos institutas, (2012). Tarpinstitucinio bendradarbiavimo analizės atlikimo, analogiškos patirties ES šalyse ir esamos teisinės bazės Lietuvoje įvertinimo. Galutinė ataskaita. //23-25, Vilnius. Prieiga per internetą: file:// tarpinstitucinio_bendradarbiavimo_analize.pdf

19. Miginis, N. ir Ulozas, M. (2014). Praktinis vadovas. Tarpžinibynio bendradarbiavimo stiprinimas.// 36-37. Prieiga per internetą: https://jrd.lt/informacija-dirbantiems-su-jaunimu/metodiniai-leidiniai/el-biblioteka/leidinystaisytas_2014.10.07.pdf

20. Lietuvos Respublikos kibernetinio saugumo įstatymas (2018). Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/15e540727ac211e89188e16a6495e98c

21. Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinis veiklos planas (2019). Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/faeb5eb4a6c811e9aab6d8dd69c6da66?jfwid=dg8d31595

22. Nacionalinė kibernetinio saugumo strategija (2018). Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f?jfwid=dg8d31595

23. Kardelis, K. (2002). Mokslinių tyrimų metodologija ir metodai. 2-asis pataisytas ir papildytas leidimas. Kaunas.// p. 86// Prieiga per internetą: https://verslas09.files.wordpress.com/2010/01/mtp.pdf

24. Bailey, K. (1987). Methods of Social Research. N.Y. Prieiga per internetą: https://books.google.lt/books?hl=lt&lr=&id=NT8eiiYhIpoC&oi=fnd&pg=PR15&dq=BAILEY,+K.+

Methods+of+Social+Research.+N.Y.,+1987.&ots=6-dHLS87TC&sig=b_KsyMIsF2ZEsqVFGUQfZFX7hKw&redir_esc=y#v=onepage&q=BAILEY%2C%20K.%20Methods%20of%20Social%20Research.%20N.Y.%2C%201987.&f=false

25. Tidikis, R. (2003). Socialinių mokslų tyrimų metodologija. Vilnius. *628 p.* Prieiga per internetą: https://www.scribd.com/doc/36462514/Tidikis-Socialiniu-Moksliniu-Tyrimu-Metodologija

26. Butkevičienė, E. (2011). Apklausų duomenų analizė. Seminaro medžiaga. Kaunas.// *Projektas „Lietuvos HSM duomenų archyvo LiDA plėtra“ SFMIS Nr. VP1-3.1-ŠMM-02-V-02-001*. Prieiga per internetą;https://www.lidata.eu/files/mokymai/seminaras_20110129/Apklausu_duomenu_analize_20111111.pdf

27. Kardelis, K. (2002). Mokslinių tyrimų metodologija ir metodai. 2-asis pataisytas ir papildytas leidimas. Kaunas. Prieiga per internetą: https://www.scribd.com/doc/37948910/K-Kardelis-Mokslini%C5%B3-tyrim%C5%B3-metodologija-ir-metodai

28. Cohen, L. Manion, L. Ir Morrison, K. (2007). Research methods in education. London and New York. //*Sixth edition, p. 47//* Prieiga per internetą: https://www.academia.edu/37378137/research_methods_in_education_book_by_Cohen_and_Manion.pdf

29. Kardelis, K. (2002). Mokslinių tyrimų metodologija ir metodai. 2-asis leidimas, Šiauliai. // *p. 93* // Prieiga per internetą: https://www.scribd.com/doc/37948910/K-Kardelis-Mokslini%C5%B3-tyrim%C5%B3-metodologija-ir-metodai

30. Nacionalinis kibernetinio saugumo centras. *//Oficiali svetainė//* Prieiga per interneta: https://www.nksc.lt/veikla.html

31. Kompleksiniai kibernetinės saugos mokymai valstybės ir savivaldybių institucijų ir įstaigų dirbantiesiems. //*Vykdomas projektas*// Prieiga per internetą: https://www.nksc.lt/veikla.html

32. Pratybų „Kibernetinis skydas 2019“ ataskaita visuomenei (2019). Prieiga per internetą: https://www.nksc.lt/doc/KS2019_pratybu_ataskaita.pdf

33. Nacionalinio kibernetinio saugumo centro prie krašto apsaugos ministerijos nuostatai. Įsakymas dėl Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos nuostatų ir struktūros patvirtinimo (2017). Prieiga per internetą: https://e-tar.lt/acc/legalAct.html?documentId=fa16ffd08e3d11e7a3c4a5eb10f04386&lang=lt

34. Komisijos komunikatas Europos parlamentui, tarybai, europos ekonomikos ir socialinių reiklalų komitetui bei regionų komitetui (2009). // *Dėl ypatingos svarbos informacinės infrastruktūros apsaugos //Europos apsauga nuo didelio masto kibernetinių antpuolių ir veiklos sutrukdymo – geresnė parengtis, didesnis saugumas ir atsparumas //SEC(2009) 399// SEC(2009) 400//* Briuselis. Prieiga per internetą: https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=COM%3A2009%3A0149%3AFIN

35. Lietuvos Respublikos aplinkos ministerijos nuostatai, 2019. Prieiga per internetą: https://www.e-tar.lt/portal/lt/legalAct/TAR.A3B226BB10B2/asr

36. Lietuvos Respublikos finansų ministerijos nuostatai, 2019. Prieiga per internetą; https://www.e-tar.lt/portal/lt/legalAct/TAR.FAD9F07C5A37/nuOsbkUXiL

37. Komisijos rekomendacija (ES) 2019/553 dėl energetikos sektoriaus kibernetinio saugumo (pranešta dokumentu Nr. C (2019) 2400), 2019. Prieiga per internetą: https://op.europa.eu/en/publication-detail/-/publication/370b898e-576f-11e9-a8ed-01aa75ed71a1/language-lt

38. Lietuvos Respublikos energetikos ministerijos nuostatai, 2019. Prieiga per internetą: https://www.e-tar.lt/portal/lt/legalAct/TAR.CDD674E49C6C/asr

39. Lietuvos Respublikos susisiekimo ministerijos nuostatai, 2010. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.383855?jfwid=rivwzvpvg

40. Lietuvos respublikos sveikatos apsaugos ministerijos nuostatai, 2019. Prieiga per internetą: https://www.e-tar.lt/portal/lt/legalAct/TAR.C9F500A0ED72/asr

41. Lietuvos Respublikos sveikatos apsaugos ministerijos valdomų ir valstybės įmonės registrų centro tvarkomų elektroninės sveikatos sistemos informacinių sistemų duomenų saugos nuostatai, 2019. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/01adad619e3711e9aab6d8dd69c6da66?jfwid=nl6mq61vl

42. Lietuvos Respublikos ekonomikos ir inovacijų ministerijos nuostatai, 2018. Prieiga per internetą: https://www.e-tar.lt/portal/lt/legalAct/TAR.3CE5C3AA17FB/HdXJlAOtYp

43. Nutarimas Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo, 2018.//*Nacionalinė kibernetinio saugumo strategija// Ypatingos svarbos informacinės infrastruktūros identifikavimo metodika// Lietuvos Respublikos Vyriausybė//* Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/KnPJZYNCpd

44. Lietuvos respublikos užsienio reikalų ministerijos nuostatai, 2020. Prieiga per internetą: https://www.e-tar.lt/portal/lt/legalAct/TAR.BD6F04D9850F/XXlUDxqbEC

45. Lietuvos Respublikos užsienio reukalų ministerijos 2019 m. ataskaita, 2019. Prieiga per internetą: https://www.urm.lt/default/lt/veikla/veiklos-ataskaita

46. Uwe, P. (2003). Informal Circles of Ministers: A Way Outof the EU's Institutional Dilemmas?// *European Law Journal, Vol. 9, No. 1, February 2003, pp. 109 – 124//* Oxford OX4 2DQ, UK. Prieiga per internetą: https://onlinelibrary.wiley.com/doi/epdf/10.1111/1468-0386.00172

47. Lietuvos Respublikos žemės ūkio ministerijos nuostatai, 2019. Prieiga per internetą: https://www.e-tar.lt/portal/lt/legalAct/TAR.64CF02BD2377/asr

48. Nekilnojamo turto kadastro duomenų saugos nuostatai, 2018. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/2c524bc2ccc311e8a82fc67610e51066?jfwid=q8i88m9wc

49. Septynioliktosios Lietuvos Respublikos Vyriausybės programa, 2016. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/886c7282c12811e682539852a4b72dd4?positionInSearchResults=0&searchModelUUID=1363e857-8fa3-478c-b09d-8b4f23b7af2d

50. Lietuvos Respublikos Vyriausybės kanceliarijos nuostatai, 2013. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.445402

51. Lietuvos Respublikos teisingumo ministerijos nuostatai, 2010. Prieiga per internetą: https://www.e-tar.lt/portal/lt/legalAct/TAR.E50DDEBA5927/hOsjmFVBIC

52. Lietuvos krašto apsaugos ministerijos nuostatai, 1998. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.60411?jfwid=-vkzfygrpz

53. Jesse, M. (2015). 7 Things You Should Know About Cross-Institutional Collaboration. //EDUCAUSE Learning Initiative (ELI)// Prieiga per internetą: https://library.educause.edu/-/media/files/library/2015/7/eli7122-pdf.pdf

54. Venables, A., Tan, G. ir Pradhan, S. (2014). A collaborative framework for a cross-institutional assessment to shape future IT professionals. Issues in Informing Science and Information Technology, 11, 215-223. Prieiga per internetą: http://iisit.org/Vol11/IISITv11p215-223Venables0451.pdf

Priedas 1. Nacionalinio kibernetinio saugumo centro eksperto apklausos anketa

Ekspertų apklausos anketa Gerb. Eksperte, Mykolo Romerio universiteto Ekonomikos ir verslo fakulteto magistrantė Žana Januško atlieka tyrimą "Tarpinstitucinio bendradarbiavimo Lietuvoje kibernetinio saugumo srityje vertinimas "**,** kurio tikslas – ištirti ir apibrėžti Lietuvos tarpinstitucinio bendradarbiavimo kibernetinio saugumo srityje ypatumus.

Vienas iš uždavinių minėtam tikslui pasiekti yra nustatyti kokiu būdu vyksta Nacionalinio kibernetinio saugumo centro (toliau NKSC) bendradarbiavimas su valstybės institucijomis atsakingomis už ypatingos svarbos infrastruktūros objektus (toliau YSI objektai) ir ypatingos svarbos informacines infrastruktūras (toliau YSII): formaliuoju (reglamentuotu teisės aktuose), neformaliuoju (nereglamentuotu teisės aktuose: neformalūs susitikimai, pokalbiai telefonu, seminarai, mokymai, konferencijos, susirašinėjimai el. paštu, koordinavimas ir kita.) ar mišriuoju būdu (formaliuoju ir neformaliuoju).

Jūsų atsakymai į klausimus padės atlikti išsamų tyrimą. Būčiau dėkinga už Jūsų išreikštą nuomonę. Apibendrintus apklausos rezultatus ir magistro tyrimą atsiųsiu užbaigusi darbą.

1. Ar vykdote tarpinstitucinį bendradarbiavimą su valstybės institucijomis atsakingomis už YSI objektus ir YSII?
2. Kokiais atvejais vykdote tarpinstitucinį bendradarbiavimą su valstybės institucijomis atsakingomis už YSI objektus ir YSII?
3. Kokiais būdais vykdote tarpinstitucinį bendradarbiavimą: formaliuoju (reglamentuoja teisės aktai), neformaliuoju (pagal poreikį, nereglamentuojamas) ar mišriuoju?
4. Kaip dažnai vykdote tarpinstitucinį bendradarbiavimą su valstybės institucijomis atsakingomis už YSI objektus ir YSII?
5. Kokiomis priemonėmis vykdote tarpinstitucinį bendradarbiavimą: jeigu vykdote formaliuoju būdu (susitikimai, el. paštas, telefonu, konferencijos, mokymai, vaizdo pokalbiai ar kita-nurodyti) jeigu vykdote neformaliuoju būdu (susitikimai, el. paštas, telefonu, konferencijos, mokymai, vaizdo pokalbiai ar kita-nurodyti)?
6. Jeigu nevykdote neformaliuoju būdu tarpinstitucinio bendradarbiavimo tai Jūsų nuomonė toks bendradarbiavimo būdas yra naudingas LR užtikrinant kibernetinį saugumą? Pagrįskite savo atsakymą. ****Klausimyno tęsinys kitame puslapyje***

7. Jūsų nuomonė ar yra poreikis reglamentuoti neformalųjį būdą tarpinstitucinio bendradarbiavimo LR teisės aktuose?

Ačiū už Jūsų laiką!

Priedas 2. Valstybės institucijų eksperto apklausos anketa

Ekspertų apklausos anketa Gerb. Eksperte, Mykolo Romerio universiteto Ekonomikos ir verslo fakulteto magistrantė Žana Januško atlieka tyrimą "Tarpinstitucinio bendradarbiavimo Lietuvoje kibernetinio saugumo srityje vertinimas "**,** kurio tikslas – ištirti ir apibrėžti Lietuvos tarpinstitucinio bendradarbiavimo kibernetinio saugumo srityje ypatumus.

Vienas uždavinių minėtam tikslui pasiekti – nustatyti kokiu būdu vyksta valstybės institucijų atsakingu už ypatingos svarbos infrastruktūros objektus (toliau YSI objekati) ir ypatingos svarbos informacines infrastruktūras (toliau YSII) bendradarbiavimas su Nacionaliniu kibernetinio saugumo centru (toliau NKSC): formaliuoju (reglamentuotu teisės aktuose), neformaliuoju (nereglamentuotu teisės aktuose: neformalūs susitikimai, pokalbiai telefonu, seminarai, mokymai, konferencijos, susirašinėjimai el. paštu, koordinavimas ir kita) ar mišriuoju būdu (formaliuoju ir neformaliuoju).

Jūsų atsakymai į klausimus padės atlikti išsamų tyrimą. Būčiau dėkinga už Jūsų išreikštą nuomonę. Apibendrintus apklausos rezultatus ir magistro tyrimą atsiųsiu užbaigusi darbą.

1. Ar vykdote tarpinstitucinį bendradarbiavimą su NKSC? *a) taip* *b) ne*
2.Kaip vykdote tarpinstitucinį bendradarbiavimą su NKSC? *a) formaliuoju būdu* *b) neformaliuoju būdu* *c) mišriu (derinant formalųjį ir neformalųjį bendradarbiavimo būdą)*
3.Kokiais atvejais vykdomas tarpinstitucinis bendradarbiavimas su NKSC formaliuoju būdu? *a) incidentų atvejais* *b) prevenciškai* *c) mokymai* *d) kiti (nurodyti konkrečius atvejus)*
4.Kokiomis priemonėmis vykdote tarpinstitucinį bendradarbiavimą formaliuoju būdu su NKSC? *a) susitikimai* *b) telefono pokalbiai* *c) el. paštu* *d) kitos priemonės (nurodyti konkrečias priemonės)* ***Klausimyno tęsinys kitame puslapyje***

5.Kaip dažnai vykdomas tarpinstitucinis bendradarbiavimas formaliuoju būdu su NKSC?

a) 1-3 mėn
b) 3-6 mėn
c) 6-12 mėn
d) 12 mėn. ir daugiau

6.Kokiais atvejais vykdomas tarpinstitucinis bendradarbiavimas su NKSC neformaliuoju būdu?

a) incidentų atvejais
b) prevenciškai
c) mokymai
d) kiti (nurodyti konkrečius atvejus)

7. Kokiomis priemonėmis vykdote tarpinstitucinį bendradarbiavimą neformaliuoju būdu su NKSC?

a) susitikimai
b) telefono pokalbiai
c) el. paštas
d) kitos priemonės (nurodyti konkrečias priemonės)

8.Kaip dažnai vykdomas tarpinstitucinis bendradarbiavimas neformaliuoju būdu su NKSC?

a) 1-3 mėn
b) 3-6 mėn
c) 6-12 mėn
d) 12 mėn. ir daugiau

9.Jūsų nuomonė ar tarpinstitucinio bendradarbiavimo kokybė su NKSC tenkina Jūsų poreikius?

a) tenkina
b) netenkina
c) iš dalies tenkina

10.Jūsų nuomonė ar yra poreikis reglamentuoti neformalią būdą tarpinstitucinio bendradarbiavimo LR teisės aktuose užtikrinant kibernetinį saugumą?

Ačiū už Jūsų laiką!

Januško Ž. (2020). *Tarpinstitucinio bendradarbiavimo Lietuvoje kibernetinio saugumo srityje vertinimas* (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas.

ANOTACIJA

Magistro baigiamajame darbe išanalizuotas ir įvertintas tarpinstitucinis bendradarbiavimas Lietuvoje kibernetinio saugumo srityje ir remiantis ekspertiniu vertinimu tikrinamas empiriškai. Pirmame skyriuje nagrinėjama kibernetinio saugumo koncepcija, tarpinstitucinio bendradarbiavimo samprata ir tarpinstitucinio bendradarbiavimo ypatumai kibernetinio saugumo srityje. Antrame darbo skyriuje yra surengtas tarpinstitucinio bendradarbiavimo kibernetinio saugumo srityje tyrimo modelis, atliktas tyrimo metodikos pagrindimas bei iškelta pagrindinė tyrimo hipotezė. Trečiame skyriuje remiantis teisės aktais bei veiklos ataskaitomis pateikiami Nacionalinio kibernetinio saugumo centro ir Lietuvos valstybės institucijų tarpinstitucinio bendradarbiavimo formavimo procesai. Susisteminami ekspertinio tyrimo metu gauti duomenys, patvirtinamos ar atmetamos hipotezės ir daromos išvados. Ketvirtame skyriuje yra pateikiamos išvados bei siūlymai, dėl poreikio reglamentuoti neformalųjį tarpinstitucinį bendradarbiavimą Lietuvos Respublikos teisės aktuose užtikrinant kibernetinį saugumą bei iškeliamos empirinio tyrimo metu išryškėjusios problemos.

Pagrindiniai žodžiai: kibernetinis saugumas, tarpinstitucinis bendradarbiavimas, formalus bendradarbiavimo būdas, neformalus bendradarbiavimo būdas.

Janusko Z. (2020). *Assessment of the cross - institutional cooperation in cyber security in Lithuania* (master thesis). Vilnius: Mykolas Romeris University.

ANNOTATION

The Master's thesis analyzes and assess cross-institutional cooperation in the field of cyber security in Lithuania and based on the assessment of the expert judgment verified empirically. The first chapter deals with the concept of cyber security, the concept of cross-institutional cooperation and cross-institutional cooperation in the field of cyber security features. The second chapter is organized cross-institutional cooperation in the field of cyber security research model, research methodology and justification of brought the main hypothesis. The third chapter in accordance with the legislation and activity reports are the National Cyber Security Center and the Lithuanian state institutions cross - institutional cooperation forming processes. Summed up the expert study findings are confirmed or rejected hypotheses and draw conclusions. The fourth section presents the conclusions and recommendations on the need to regulate the informal cross-institutional cooperation between the Republic of Lithuania legislation ensuring cyber security and brought empirical study emerged problems.

Key words: cyber security, cross-institutional cooperation, formal cooperation, informal cooperation.

Januško Ž. (2020). *Tarpinstitucinio bendradarbiavimo Lietuvoje kibernetinio saugumo srityje vertinimas* (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas.

SANTRAUKA

Tarpinstitucinis bendradarbiavimas kibernetinio saugumo srityje magistro baigiamojo darbo tema aktuali Lietuvos Respublikos valstybės institucijoms. Šiomis dienomis valstybės institucijose tarpinstitucinio bendradarbiavimo principas užtikrinant kibernetinį saugumą vis dar yra neįtraukiamas į jų nuostatus ir teisinį reglamentavimą. Remiantis tarpinstitucinio bendradarbiavimo naujoviškumu, ypač kibernetinio saugumo srityje kur valstybės institucijos atsakingos už ypatingos svarbos objektus ir kuriu neveikimas ar veiklos sutrikdymas gali padaryti didelę žalą nacionaliniam saugumui, šalies ūkiui, valstybės ar visuomenės interesams, reikalauja visapusiškai plėtoti bendradarbiavimo kultūrą centrinės valdžios ir institucijų lygmeniu. Tyrimo objektas – tarpinstitucinis bendradarbiavimas Lietuvoje kibernetinio saugumo srityje. Šio tyrimo tikslas yra išnagrinėjus mokslinius požiūrius, praktinius aspektus į tarpinstitucinį bendradarbiavimą kibernetinio saugumo srityje ir parengus tyrimo metodologiją ištirti ir apibrėžti Lietuvos tarpinstitucinio bendradarbiavimo kibernetinio saugumo srityje ypatumus. Taip pat buvo iškelti ir tyrimo uždaviniai: pateikti tarpinstitucinio bendradarbiavimo kibernetinio saugumo srityje teorinius aspektus, parengti teikti tarpinstitucinio bendradarbiavimo kibernetinio saugumo srityje tyrimo metodologija ir išanalizuoti tarpinstitucinį bendradarbiavimą Lietuvoje kibernetinio saugumo srityje bei atsižvelgiant į atliktą tyrimą prireikus pateikti pasiūlymus dėl tarpinstitucinio bendradarbiavimo Lietuvoje kibernetinio saugumo srityje tobulinimo. Tyrimo metodika: sisteminė, apibendrinimo, lyginamoji ir aprašomoji mokslinės literatūros analizė bei teisės dokumentų turinio analizė, lyginimo metodas, ekspertinis vertinimas ir jo analizė. Empirinio tyrimo metu buvo iškelta pagrindinė hipotezė: tikėtina, kad yra poreikis reglamentuoti Lietuvos Respublikos teisės aktuose neformalųjį tarpinstitucinį bendradarbiavimą kibernetinio saugumo srityje. Atlikus ekspertinį vertinimą tyrimo hipotezė nepasitvirtino. Gauti rezultatai parodė, kad visos valstybės institucijos nemato poreikio reglamentuoti neformalųjį tarpinstitucinio bendradarbiavimo būdą. Toks požiūris gali byloti apie nepakankamai išvystyta bendradarbiavimo kultūra centrinės valdžios ir institucijų lygmeniu. Ekspertinio tyrimo metu taip pat buvo gauta, kad istitucijos bendrai yra patenkintos tarpinstituciniu bendradarbiavimu, tačiau pastebėtina, kad valstybės institucijos vangiai dalyvauja mokymuose. Pagrindiniai veiksniai, turintys labai didelę įtaką tarpinstituciniam bendradarbiavimui Lietuvoje užtikrinant kibernetinį saugumą yra mokymai, sistemingai ir nuolatiniai organizuoti tiksliai, tinkamai suderinti veiksmai ir aiški veikimo schema. Atlikto tyrimo rezultatai gali būti naudojami nagrinėjant tarpinstitucinio bendradarbiavimo užtikrinant kibernetinį saugumą formavimą, vertinant tarpinstitucinio

bendradarbiavimo formavimo procesų naudą bei sudarant sąlygojančius veiksnius veiksmingoms tarpinstitucinio bendradarbiavimo užtikrinant kibernetinį saugumą formavimo procesams skatinimui.

Magistro baigiamojo darbo pabaigoje pateikiamos išvados bei siūlymai dėl tarpinstitucinio bendradarbiavimo kibernetinio saugumo srityje.

Janusko Z. (2020). *Assessment of the cross - institutional cooperation in cyber security in Lithuania* (master thesis). Vilnius: Mykolas Romeris University.

SUMMARY

Cross-institutional cooperation in the field of cyber security master's thesis topic relevant state institutions of the Republic of Lithuania. These days, state institutions cross-institutional cooperation principle of ensuring cyber security is still not included in their regulations and legal regulation. On the basis of cross-institutional cooperation in innovation, especially in the field of cyber security where a state institutions responsible for special objects to provide key input and whose failure or disruption can cause serious damage to national security, the economy, the state or the public interest require the full cooperation develop culture of the central government and institutional level. The object of research - Lithuania cross-institutional cooperation in cyber security. The purpose of the investigation is the examination of scientific approaches to the practical aspects of cross-institutional cooperation in the field of cyber security and after developing the research methodology to investigate and define the Lithuanian cross-institutional cooperation in the field of cyber security peculiarities. Research objectives were also presented: to present theoretical aspects of cross-institutional cooperation in cyber security, to develop methodology for researching cross-institutional cooperation in cyber security and to analyze cross-institutional cooperation in cyber security in Lithuania and depending on analysis to make proposals for improving cross-institutional cooperation. Methods of the investigation: systematic, generalization, comparative and descriptive analysis of scientific literature and document content analysis, comparison method, expert evaluation**.** During the empirical research, the main hypothesis was raised: it is probable that there is a need to regulate informal ccross-institutional cooperation in the field of cyber security in the legal acts of the Republic of Lithuania. After the expert evaluation, the research hypothesis was not confirmed. The results obtained showed that not all state institutions see the need to regulate the informal way of cross-institutional cooperation. Such an approach may indicate an underdeveloped culture of cooperation at the level of central government and institutions. The expert study also showed that institutions are generally satisfied with cross-institutional cooperation, but it should be noted that state institutions are slow to participate in training. The main factors that have a very significant impact on cross-institutional cooperation in ensuring cyber security in Lithuania are training, systematic and continuous organization of precise, properly coordinated actions and a clear scheme of operation. The results of the research can be used to examine the formation of cross-institutional cooperation in ensuring cyber security, to assess the benefits of cross-institutional cooperation formation processes and to create

the determining factors for effective promotion of cross-institutional cooperation in cyber security formation processes.

At the end of the master's thesis, conclusions and suggestions for cross-institutional cooperation in the field of cyber security are presented.

.

Forma patvirtinta Mykolo Romerio universiteto
Senato 2016 m. gegužės 9 d. nutarimu Nr.1SN-44

PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ

2020 m. 04 mėn. 06 d.
Vilnius

Aš, Mykolo Romerio universiteto, Ekonomikos ir verslo fakulteto, Kibernetinio saugumo valdymo programos studentė Žana Januško patvirtinu, kad šis magistro baigiamasis darbas „Tarpinstitucinio bendradarbiavimo Lietuvoje kibernetinio saugumo srityje vertinimas“:

1. Yra atliktas savarankiškai ir sąžiningai;
2. Nebuvo pristatytas ir gintas kitoje mokslo įstaigoje Lietuvoje ar užsienyje;
3. Yra parašytas remiantis akademinio rašymo principais ir susipažinus su rašto darbų metodiniais nurodymais.

Man žinoma, kad už sąžiningos konkurencijos principo pažeidimą – plagijavimą studentas gali būti šalinamas iš Universiteto kaip už šiurkštų akademinės etikos pažeidimą.

Žana Januško