MYKOLO ROMERIO UNIVERSITETAS
VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

AISTĖ POCIENĖ

KIBERNETINIO SAUGUMO KULTŪROS FORMAVIMO PROBLEMOS LIETUVOS VIEŠAJAME SEKTORIUJE

Magistro baigiamasis darbas

Vadovas
doc. dr. M. Laurinaitis

VILNIUS, 2021

MYKOLO ROMERIO UNIVERSITETAS
VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

KIBERNETINIO SAUGUMO KULTŪROS FORMAVIMO PROBLEMOS LIETUVOS VIEŠAJAME SEKTORIUJE

Kibernetinio saugumo valdymo magistro baigiamasis darbas
Studijų programa 6211LX066

Vadovas
doc. dr. M. Laurinaitis
2021 05

Recenzentas

Atliko
KSVvmis19-1 gr. stud.
Aistė Pocienė
2021 05 03

VILNIUS, 2021

TURINYS

LENTELĖS 4
PAVEIKSLAI 5
ĮVADAS 6
1. TEORINĖ KIBERNETINIO SAUGUMO KULTŪROS SAMPRATOS ANALIZĖ 9
1.1. Kibernetinio saugumo kultūros sąvoka ir raidos analizė 9
1. 2. Kibernetinio saugumo kultūros formavimo organizacijoje samprata 12
1.1.1. Strategijos kūrimas ir politikos formavimas 12
1.1.2. Vadovavimas ir valdymas 14
1.1.3. Kibernetinio saugumo švietimas 16
1.1.4. Kibernetinio saugumo higiena 20
1.1.5. Bendradarbiavimas kibernetinio saugumo klausimais 22
1.3 Kibernetinio saugumo kultūros formavimo ypatumai viešajame sektoriuje 25
2. KIBERNETINIO SAUGUMO KULTŪROS FORMAVIMO VIEŠAJAME SEKTORIUJE TYRIMO METODOLOGIJA 31
2.1 Empirinio tyrimo metodologija 31
2.2. Empirinio tyrimo organizavimas ir loginė eiga 33
3. KIBERNETINIO SAUGUMO KULTŪROS FORMAVIMO LIETUVOS VIEŠAJAME SEKTORIUJE EMPIRINIS TYRIMAS 40
3.1. Teisinis reglamentavimas 40
3.2. NKSC vaidmuo Lietuvos kibernetinio saugumo kultūros formavime 48
3.3. LR ministerijų kibernetinio saugumo kultūros formavimo tiriamieji aspektai 52
3.4. Tyrimo gautų rezultatų interpretacija 61
3.4.1. Lietuvos Respublikos ministerijų ekspertinio vertinimo rezultatai 62
3.4.2. Nacionalinio kibernetinio saugumo centro ekspertinio vertinimo rezultatai 68
IŠVADOS 75
LITERATŪROS SĄRAŠAS 788
ANOTACIJA 85
ANNOTATION 86
SANTRAUKA 87
SUMMARY 89
PRIEDAI 90
PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ 96

LENTELĖS

1 lentelė. Privataus ir viešojo sektoriaus bendradarbiavimą skatinantys faktoriai 23
2 lentelė. Ekspertinio vertinimo apklausos klausimų sudarymo instrumentarijus 34
3 lentelė. Ekspertinio interviu klausimų sudarymo instrumentarijus 37
4 lentelė. Lietuvos viešojo sektoriaus institucijų pareigos Lietuvos kibernetinio saugumo įstatyminiame kontekste 42
5 lentelė. LR ministerijų uždaviniai kibernetinio saugumo kultūros formavime nacionaliniu lygmeniu 52
6 lentelė. 1 klausimas: Jūsų atstovaujama institucija: 62
7 lentelė. 2 klausimas: Jūsų nuomone, ar atstovaujamoje institucijoje yra tinkamai palaikoma kibernetinio saugumo higiena? 63
8 lentelė. 3 klausimas: Ar jūsų institucijoje yra organizuojami kibernetinio saugumo mokymai darbuotojams? 63
9 lentelė. 4 klausimas: Kaip manote, kas paskatintų darbuotojo, kurio tiesioginės funkcijos nėra susijusios su kibernetiniu saugumu, įsitraukimą į organizacijos kibernetinio saugumo kultūros formavimą? 64
10 lentelė. 5 klausimas: Ar jūsų institucijoje yra sudarytos sąlygos kelti personalo, kurio funkcijos tiesiogiai susijusios su kibernetiniu saugumu, kvalifikaciją? 64
11 lentelė. 6 klausimas: Kaip dažnai jūsų institucija dalyvauja NKSC ar kitų institucijų organizuojamose kibernetinio saugumo pratybose? 65
12 lentelė. 7 klausimas: Jūsų nuomone, kokios priežastys lemia žemą valstybinių institucijų dalyvavimo NKSC ar kitų institucijų organizuojamose statistinį rodiklį? 65
13 lentelė. 8 klausimas: Kokias jūsų atstovaujamos institucijos bendradarbiavimo formas kibernetinio saugumo klausimais su kitomis institucijomis galite įvardinti? 66
14 lentelė. 9 klausimas: Jūsų nuomone, ar visų lygmenų vadovai yra įsitraukę į kibernetinio saugumo kultūros formavimą jūsų atstovaujamoje institucijoje? Jei taip, kokiais būdais? 67

PAVEIKSLAI

1 pav. Kibernetinio saugumo subjektų ir NKSC techninėmis kibernetinio saugumo stebėsenos priemonėmis surinkta informacija apie kenkimo PĮ pagal ypatingos svarbos paslaugų sektorius 26
2 pav. Kibernetinio saugumo įgyvendinimo kliūtys viešajame sektoriuje..... 27
3 pav. IT saugos specialisto darbo užmokestis privačiame ir viešajame sektoriuje..... 28
4 pav. Kibernetinio saugumo kultūros formavimo viešajame sektoriuje teorinis modelis 30
5 pav. Ekspertų skaičiaus įtaka vertinimo patikimumui..... 33
6 pav. Viešojo sektoriaus institucijų interneto svetainių pažeidžiamumas 57
7 pav. LR ministerijų dalyvavimo statistika nacionalinesė kibernetinio saugumo pratybose „Kibernetinis skydas“ 2019 m. ir 2020 m. 59

ĮVADAS

Darbo aktualumas. Šiandieniniame pasaulyje kibernetinė erdvė pakeitė žmonių tarpusavio sąveiką, informacijos ieškojimo, pasikeitimo mechanizmus ir tapo ne tik pasaulinio vystymosi dalimi, bet ir politinės bei karinės kovos arena. Ryšių ir informacinių sistemų technologijos tapo įrankiu manipuliuoti informacija, daryti įtaka visuomenės požiūrio formavimui ir skleisti dezinformaciją įvairius visuomenės informavimo šaltinius, kas galiausiai sukelia didžiulį disbalansą tarptautiniuose santykiuose ir kenkia visuomenės sanglaudai. Didelio mąsto kibernetinės atakos ar kiti elektroninės erdvės pažeidimai dažnai prasidedantys nuo menkiausio neapdairumo, kibernetinio išprusimo stokos ar silpniausios valstybės valdomos ir saugomos infrastruktūros spragų, gali eskaluoti ir paveikti valstybių nacionalinį saugumą. Pasaulinio ekonomikos forumo globalių rizikų ataskaitoje (2021) yra nurodoma, jog valstybės kritinės svarbos informacinės infrastruktūros sutrikdymas ar išvis netekimas dėl sistemų priklausomybės nuo kibernetinių tinklų ir technologijų yra vis dar išliekanti ir ypač opi technologinė rizika globaliu mastu. Todėl vis daugiau valstybių įvardija, kad kibernetinis saugumas yra viena iš priemonių užtikrinti nacionalinį saugumą, o valstybės informacinių išteklių, ypatingos svarbos infrastruktūros objektų (toliau – YSI objektų)[1] ir jų valdomos ypatingos svarbos informacinės infrastruktūros (toliau – YSII)[2] kibernetinis saugumas yra valstybės strateginiai prioritetai.

Kad valstybiniai kritinės svarbos sektoriai galėtų teikti kokybiškas paslaugas, jie tampa vis labiau priklausomi nuo informacinių technologijų, kurioms atitinkamai kyla naujos, elektroninėje erdvėje progresuojančios grėsmės. Kibernetinio saugumo rizikų didėjimą informacinėse infrastruktūrose ir ryšių ir informacinių sistemų (toliau – RIS) tinkluose lemia daugybė veiksnių, pradedant nuo nepakankamos technologinės plėtros informacinių sistemų viduje iki didėjančio sudėtingesnių atakų vektorių skaičiaus. Tačiau žvelgiant iš viešojo sektoriaus prizmės, kibernetinio saugumo rizikas lemia ne tik techniniai, bet ir organizaciniai veiksniai. Pavyzdžiui, nuolatiniai biudžeto suvaržymai, kvalifikuoto personalo trūkumas, nekonkurencingas darbo užmokestis yra tik dalis faktorių, lemiančių viešojo sektoriaus kibernetinio saugumo palaikymo problematiką. Ir nors šios problemos didžiąja dalimi visuomenėje yra gerai žinomos, tai institucijų neatitraukia nuo esminio, strateginio lygmens tikslo – kuo saugesnės ir atsparesnės kibernetinės aplinkos sukūrimo valstybės informacinėje infrastruktūroje.

Visgi, nors Lietuvos valstybinėms institucijoms, kaip kibernetinio saugumo subjektams, kibernetinio saugumo įgyvendinimą reglamentuoja teisės aktai, tai neatspindi bendros kibernetinio saugumo kultūros viešajame sektoriuje, jos formavimo tendencijų. Kol kibernetinis saugumas nekoreliuoja su veiklos procesais, tol iššūkis išlaikyti informacinės infrastruktūros kibernetinį saugumą

[1] **Ypatingos svarbos infrastruktūros objektas** – institucija, įstaiga, įmonė ar jos struktūrinis padalinys, projektuojamas, statomas ar esamas įrenginys, turtas ar jo dalis, kurių valdytojas yra viešasis arba privatus juridinis asmuo.
[2] **Ypatingos svarbos informacinė infrastruktūra** – ryšių ir informacinė sistema ar jos dalis, ryšių ir informacinių sistemų grupė, apdorojanti neįslaptintą informaciją.

viešajame sektoriuje bus IT departamento kompetencijoje. Kad to išvengti, yra svarbu skatinti sisteminį valstybinių institucijų požiūrį į kibernetinį saugumą, taip formuojant kibernetinio saugumo kultūrą, kurios procesai priverstų į kibernetinį saugumą pažvelgti visai iš kitos plotmės. Todėl norint suprasti esminius iššūkius valdyti viešojo sektoriaus institucijų kibernetinę erdvę, reikalingas išsamus situacijos vertinimas per norminį pagrindą, nustatantį techninių priemonių kibernetinėms rizikoms valdyti, kibernetinei saugai ir higienai užtikrinti pritaikomumą institucijų poreikiams, ir organizacinį, socialinį bei vadybinį, įvertinant viešojo sektoriaus institucijų bendradarbiavimo kibernetinio saugumo klausimais ypatumus, vadovų indėlį darbuotojų požiūrio į kibernetinį saugumą formavime, kibernetinio saugumo švietimą bei RIS saugos personalo ir administratorių kvalifikacijos kėlimo galimybes. Visų šių faktorių praktinis įgyvendinimas valstybinėse institucijose kuria efektyvią kibernetinio saugumo kultūrą ir nacionaliniu lygmeniu. Dėl to šiai dienai yra aktualu nagrinėti Lietuvos viešojo sektoriaus institucijų kibernetinio saugumo kultūros įgyvendinimo ypatumus ir jų efektyvumą sąlygojančias problemas, tarpusavio sąveiką ir priklausomybę.

Mokslinis naujumas / teorinis reikšmingumas. Kibernetinio saugumo kultūros formavimo organizacijoje aspektai moksliniame kontekste yra pradėti nagrinėti visai neseniai. Užsienio mokslininkų ir tarptautinių institucijų (Ashenden, 2008; Hedstrom, Kolkowska, Karlsson ir Allen, 2011; Ashenden ir Sasse, 2013; Kolkowska ir Dhillon, 2013; Solms ir Niekerk, 2013; Flores, Antonsen ir Ekstedt, 2014; Karlsson ir Hedstrom, 2014; Kearney ir Kruger, 2016; ENISA, 2017) publikuojamose studijose išskiriamos įvairios sąlygos kibernetinio saugumo kultūros efektyviam įgyvendinimui. Dalis institucijų yra pasidalinusios netgi gerosios praktikos pavyzdžiais, kaip kryptingai formuoti darbuotojų požiūrį į kibernetinės erdvės saugumo užtikrinimo būtinumą. Pastebėtina ir tai, kad dalis mokslinės literatūros yra orientuota bendrine prasme į organizaciją, neišskiriant, ar tai turėtų būti privatus, ar viešasis sektorius. Politikos, kaštų, reikšmės valstybės nacionalinio saugumui ir organizacinių bei procedūrinių priemonių skirtumai tarp privataus ir viešojo sektorių reikalauja atskirti šių sektorių organizacijų kibernetinio saugumo kultūros formavimo praktikas ir netaikyti vienodų mechanizmų. Taip pat nagrinėtoje literatūroje pasigendama kibernetinio saugumo kultūros kaip reiškinio nagrinėjimo ne tik per tam tikrus kriterijus, bet ir per jų tarpusavio sąveiką ir priklausomybę vienas nuo kito. Tai leidžia konstruoti ***mokslinę problemą***, kurią galima formuluoti klausimu „Kaip kibernetinio saugumo kultūros priemonių įgyvendinimas Lietuvos viešojo sektoriaus institucijose koreliuoja su nacionalinio kibernetinio saugumo stiprinimu?“. Taigi, šiame darbe bus išryškinti esminiai kibernetinio saugumo kultūros įgyvendinimo ypatumai ir problemos, su kuriomis susiduria Lietuvos viešojo sektoriaus institucijos jų įgyvendinimo procese bei pateikti siūlymai / rekomendacijos dėl kibernetinio saugumo kultūros gerinimo nacionaliniu lygmeniu.

Tyrimo hipotezė. Kibernetinio saugumo kultūros formavimo neefektyvumą Lietuvos viešajame sektoriuje lemia vadybos stoka.

Praktinis taikomumas. Darbe atskleistos pagrindinės kibernetinio saugumo kultūros formavimo problemos ir joms spręsti pateikti siūlymai galėtų būti pritaikyti ir kitiems Lietuvos kibernetinio saugumo subjektams.

Darbo objektas. Kibernetinio saugumo kultūra Lietuvos viešajame sektoriuje.

Darbo tikslas – ištirti kibernetinio saugumo kultūros formavimo ypatumus ir problemas Lietuvos viešajame sektoriuje.

Darbo uždaviniai:

1. Konceptualizuoti kibernetinio saugumo kultūros sampratą.
2. Atskleisti kibernetinio saugumo kultūros įgyvendinimo Lietuvos viešajame sektoriuje pagrindinius teisinio reglamentavimo aspektus.
3. Išanalizuoti kibernetinio saugumo kultūros įgyvendinimo procesus ir problemas Lietuvos valstybinėse institucijose.
4. Pateikti siūlymus ir rekomendacijas identifikuotoms kibernetinio saugumo kultūros formavimo problemoms spręsti.

Tyrimo metodika. Analizuojant kibernetinio saugumo kultūros formavimo problemas Lietuvos viešajame sektoriuje, tyrime naudojama sisteminė, apibendrinimo, lyginamoji ir aprašomoji mokslinės literatūros analizė bei teisės aktų turinio analizė, atliekamas ekspertinis vertinimas empiriškai patvirtinti autoriaus gautus analizės rezultatus.

1. TEORINĖ KIBERNETINIO SAUGUMO KULTŪROS SAMPRATOS ANALIZĖ

1.1. Kibernetinio saugumo kultūros sąvoka ir raidos analizė

Kibernetinio saugumo kultūros sąvoka yra ganėtinai nauja, o pats reiškinys pradėtas aiškinti tik šio amžiaus pradžioje. Dažniausiai mokslinėje literatūroje galima pamatyti, kad kibernetinio saugumo kultūros sąvoka yra tapatinama su informacinio saugumo kultūros sąvoka, kuri nors ir atsirado kur kas anksčiau, tačiau turi nemažai glaudžiai tarpusavyje susijusių teorinių aspektų. Toliau darbe bus detalizuoti pastarieji panašumai bei tam tikri esminiai skirtumai su tikslu atskleisti sąvokų teorinę raidą ir suformuluoti teorinio pagrindo kriterijus.

Visų pirma, yra svarbu konceptualizuoti patį kibernetinį saugumą ir informacijos saugumą kaip du atskirus reiškinius. Informacijos saugumas yra visuma priemonių, skirtų apsaugoti duomenis nuo neteisėtos prieigos ar turinio pakeitimų, tais atvejais, kai informacija yra saugoma arba perduodama iš vienos vietos į kitą (Fruhlinger, 2020). Kitaip tariant, tai informacijos saugumas apima informacijos ir informacinių sistemų apsaugą nuo neteisėtos prieigos, naudojimo, atskleidimo, sutrikdymo, pakeitimo, peržiūros, tikrinimo, registravimo ir sunaikinimo. Bendras informacijos saugumo tikslas yra išsaugoti informacijos ir informacijos išteklių konfidencialumą, vientisumą ir prieinamumą. Visapusiški informacinio saugumo sprendimai apima įvairialypes nagrinėjamos informacijos fizines, procedūrines ir logines apsaugos formas. Informacijos saugumo samprata ir su ja susijusi praktika bei procedūros nuolat tobulėja, kad atitiktų sklandžią verslo aplinką. Tačiau vien to, kad organizacijos įgyvendina informacijos saugumo sprendimus, nepakanka. Šiuo metu visi interneto ir informacinių sistemų vartotojai turi turėti bent pagrindinį kibernetinio saugumo supratimo ir žinių lygį, kad galėtų saugiai vykdyti savo kasdienę veiklą. Todėl dabar saugumo problemoms spręsti reikia labiau suderintų ir tikslingesnių nacionalinės ir tarptautinės visuomenės, viešojo ir privataus sektoriaus pastangų. Dėl to buvo apibrėžta kita saugumo rūšis, būtent – kibernetinis saugumas. ,,Kibernetinis saugumas apima asmens, visuomenės ar tautos interesų apsaugą, įskaitant jų informaciją ir ne informacija pagrįstą turtą, kurį reikia apsaugoti nuo rizikos, susijusios su jų sąveika su elektronine erdve.“ (Solms ir Niekerk, 2013, p. 100). Informacijos saugumo srityje nuoroda į žmogiškąjį faktorių paprastai yra susijusi su žmogaus vaidmeniu (– imis) saugumo procese. Kibernetinio saugumo srityje šis veiksnys turi papildomą dimensiją – ,,žmonės yra potencialūs kibernetinių atakų taikiniai ar net nesąmoningai dalyvaujantys kibernetinėje atakoje.“ (ten pat, p. 97). Apie tai kalba ir kitas teoretikas, Schlienger (2003), pasak kurio informacinis saugumas ir jo valdymas dažniausiai nepaiso žmogiškosios dimensijos: pagrindinis dėmesys skiriamas techninėms ir procedūrinėms priemonėms, o pats žmogus vertinamas kaip saugumo priešas bet visai ne kaip saugumo subjektas. Nors visa tai atskleidžia viena pagrindinių sąvokų skirtumų – žmogiškąjį faktorių, kaip visai atskirai nuo technologinių procesų tiriamąjį ir didžiulę įtaką kibernetinio saugumo kontekste darantį subjektą.

Tuo tarpu yra teoretikų, manančių, kad nereikėtų pamiršti ar ignoruoti šių dviejų sąvokų priklausomybės viena nuo kitos. Teoretikas Ashenden (2008) laiko informacijos saugumo valdymą „žmogiškuoju iššūkiu“, nurodydamas poreikį suprasti, kad pavieniai organizacijos nariai ne tik turi su darbu susijusį socialinį identitetą, bet ir suteikia tapatybę darbo vietoje. Tai reiškia, kad bet koks bandymas pakeisti ar patobulinti kibernetinį saugumą turi apimti ir kultūrinius organizacijos aspektus. Todėl svarbu suprasti, kas kuria ir daro įtaką organizacijos kultūrai, kad būtų galima efektyviai suprasti žmogaus elgesį ir kodėl darbuotojai elgiasi taip, kaip elgiasi kibernetinio saugumo srityje. Taip pat svarbu konstruoti sisteminį požiūrį į šių dviejų sąvokų koreliaciją, kad suprasti, kaip jos integruojasi organizacijos kultūros kontekste. Taigi, informacinis saugumas yra informacijos, kuri yra turtas, apsauga nuo galimos žalos, kylančios dėl įvairių grėsmių ir pažeidžiamumų. Tačiau informacijos naudojimo ribos peržengė techninių priemonių kontekstą. Su laiku, remiantis aptartais apibrėžimais, informacinio saugumo poreikį iš esmės pakeitė kibernetinio saugumo poreikis, o kibernetinio saugumo ribos ir jo įgyvendinimui kylančios rizikos yra visgi didesnės nei informacijos saugumo. Visuomenės kontekste rizika ir grėsmė, su kuria susiduria vartotojai, yra labiau apimanti, nei tos, kurioms būdingas tipinis informacinis saugumas. Tačiau dar svarbiau yra gebėti vertinti žmogiškąjį faktorių organizaciniame kontekste, nepriklausomai nuo to, ar tai yra IT departamento vadovas, ar RIS saugos personalas, ar galinės įrangos naudotojas.

Išryškinus pagrindinius skirtumus ir panašumus tarp informacinio ir kibernetinio saugumo sąvoku, svarbu integruoti jų esminius kriterijus organizacijos kultūros sąvokos kontekste. Kibernetinio saugumo kultūra literatūroje vertinama kaip kažkas, ką galima pakeisti ir iš dalies valdyti. Dažniausiai naudojama organizacinės kultūros koncepcija išplaukia iš Scheino (1996), kuris kultūrą apibūdina kaip „pagrindinių tylių prielaidų apie tai, koks yra pasaulis ir koks turėtų būti, rinkinys, kuris yra ir turėtų būti toks, kokia yra žmonių grupė, taip pat ir toks, kuris lemia jų suvokimą, mintis, jausmus ir tam tikru mastu – jų atvirą elgesį.“ (p. 236). Remiantis Hatch (1993), organizacijos kultūra vertinama kaip pasireiškianti trimis lygiais:

- Tyliomis prielaidomis, kurios yra įsitikinimai apie tikrovę ir žmogaus prigimtį;
- Vertinamomis vertybėmis, susijusiomis su socialiniais principais, filosofija, tikslais ir standartais;
- Artefaktais, kurie yra matomi, apčiuopiami ir girdimi veiklos rezultatai, pagrįsti vertybėmis ir prielaidomis.

Šis trijų sluoksnių organizacijos kultūros konceptualizavimas buvo daugelio informacijos saugumo kultūros modelių ar rėmų pagrindas. Tačiau nagrinėjant mokslinę literatūrą, Niekerk ir Solms (2010) ir ENISA (2017), **kibernetinio saugumo kultūros kontekste** yra pridedamas papildomas, ketvirtasis sluoksnis:

- Žinios.

Pasak autorių, žinios daro įtaką prielaidoms, vertybėms ir elgsenai, dėl to visi sluoksniai yra tarpusavyje susiję ir stipriai vienas nu kito priklausomi. Visgi, norint užtikrinti tinkamų priemonių įgyvendinimą, gali reikėti suprasti kiekvieną iš jų atskirai. Pavyzdžiui, remiantis Hedstrom ir kt. (2011) atliktu tyrimu, supratimas apie žmonių veiksmus ir kokios prielaidos juos skatina taip elgtis gali padėti geriau suprasti informacijos saugumo kultūros įgyvendinimo problemas, nes pasak teoretikų neatitikimas gali kilti dėl tarpusavyje nesuderinamų ar konkuruojančių dalykų, pavyzdžiui, tarp organizacijos strategijos ir paties darbuotojo vertybių, kuriuos atspindi darbuotojų atliekamas darbas. Tačiau vertybes kaip prielaidas dažniausiai kibernetinio saugumo kontekste yra per daug sudėtinga nagrinėti, nes jos turi būti daromos iš to, ką sako ir daro organizacijos nariai. Todėl vis dažniau mokslinėje literatūroje apie kibernetinio saugumo kultūrą yra nagrinėjamas stebimų artefaktų ir elgesio sluoksnių faktorius. Kaip minėta anksčiau, kai kurie į savo kibernetinio saugumo kultūros modelius įtraukia ketvirtąjį, žinių lygmenį, užuot traktavę juos kaip trijų pradinių lygmenų sudedamąjį komponentą. Niekerk ir Solms (2010) teigia, kad „ši adaptacija yra būtina, nes informacinio saugumo kultūroje negalima manyti, kad egzistuoja reikalingos žinios.“ (p. 486). Kadangi kibernetinis saugumas, iš esmės, yra susijęs su rizika, taip pat dažnai pabrėžiama, kad kibernetinis saugumas yra nuolatinis rizikos nustatymo, įvertinimo ir reagavimo į ją procesas (ENISA, 2017). Ashenden ir Sasse (2013) teigia, kad informacinio saugumo vertinimas, kaip neatsiejama verslo vykdymo dalis, yra svarbus, siekiant išvengti prieštaringų išankstinių nusistatymų organizacijoje, kurie gali sumažinti kibernetinio saugumo vaidmenį ir priemonių efektyvumą. Visuma žinių apie kibernetinį saugumą ir nuolat vertinamos su juo susijusios rizikos padeda kibernetinio saugumo kultūrai vystytis natūraliai, t. y. nuolat atsižvelgiant organizacijoje į darbuotojų elgesį ir jų požiūrį į informaciją kaip siektiną apsaugoti turtą plačiąja prasme.

Taigi brandi kibernetinio saugumo kultūra yra susijusi su saugumo supratimo ir rizikos suvokimo puoselėjimu bei jautrumu grėsmių pokyčiams. Įsitikinimai apie žmones ir jų elgesį elektroninėje erdvėje yra labai svarbi prielaida nagrinėjant kibernetinio saugumo kultūrą. Taip pat svarbu paminėti, kad kalbant apie kibernetinio saugumo kultūrą, nereikėtų jos visiškai atskirti nuo informacinio saugumo kultūros sąvokos, nes organizaciniai faktoriai tiriant žmonių elgseną yra vienas nuo kito neatsiejami. Vis gi, nagrinėjant mokslinę literatūrą pasidaro aišku, kad vieno ir visuotino kibernetinio saugumo kultūros sąvokos apibrėžimo nėra. Tačiau išanalizavus dalį teoretikų pasisakymų ir viešų pamąstymų apie esmines kibernetinio saugumo ir organizacijos kultūros teorines prielaidas, galima teigti, kad ***kibernetinio saugumo kultūra yra žinių, įsitikinimų, darbuotojų suvokimo, bei organizacijoje taikomų normų ir vertybių apie kibernetinį saugumą visuma, kuri atsiskleidžia ir pasireiškia žmonių elgesiu elektroninėje erdvėje.***

1. 2. Kibernetinio saugumo kultūros formavimo organizacijoje samprata

Šiandieniniame pasaulyje, kuomet didžioji darbo dalis yra perkelta į elektroninę erdvę, yra labai svarbu kurti sisteminį požiūrį į galimas rizikas ir grėsmes kibernetiniam saugumui. Tam, kad tikslas būtų pasiektas, organizacijos vis sparčiau įsitraukia į kibernetinio saugumo kultūros formavimą savo viduje. Taip pat dalis jų yra priklausomos ne tik nuo vidinių taisyklių ir egzistuojančios saugumo politikos, bet ir nuo išorinių veiksnių, kurie automatiškai įpareigoja laikytis teisės aktų ir kitų reglamentuotų taisyklių kibernetiniam saugumui užtikrinti tiek nacionaliniame, tiek tarptautiniame kontekste. Praeitame skyriuje išnagrinėjus kibernetinio saugumo kultūros sąvoką, tapo akivaizdu, kad pagrindiniai pastarąją organizacijos kultūrą reikalingi įvertinti aspektai yra žmonės / darbuotojai, jų požiūris, supratimas bei žinios. Taip pat svarbios yra ir prielaidos, vertinant patį žmogiškąjį faktorių, nes jos yra susijusios ne tik su vertybėmis, bet ir su organizacijos taikoma politika geriausiai valdyti kibernetinį saugumą ir kibernetinio saugumo kultūrą (Barton ir kt., 2016). Pavyzdžiui, organizacija, kuri kibernetinį saugumą laiko neatsiejama verslo dalimi, greičiausiai siekia pusiausvyros tarp kibernetinio saugumo tikslų ir kitų verslo sričių tikslų. Toks tikslo ir vertės suderinimas mokslinėje literatūroje dažnai minimas kaip svarbus faktorius, norint sėkmingai įgyvendinti kibernetinį saugumą užtikrinančias priemones (Ashenden, 2008; Ashenden ir Sasse, 2013; Flores, Antonsen ir Ekstedt, 2014; Hedstrom ir kt., 2011; Karlsson ir Hedstrom, 2014; Kearney ir Kruger, 2016; Kolkowska ir Dhillon, 2013). Kita susijusi vertybė yra ta, ar kibernetinis saugumas vertinamas kaip visos organizacijos ar konkrečių jos dalių atsakomybė. Vis gi, visa tai yra susiję ir stipriai priklauso nuo organizacijos strategijos ir politikos, vadybos ir valdymo, įvestos ir nuolatos palaikomos kibernetinės higienos, organizacijos darbuotojų švietimo, bendradarbiavimo kibernetinio saugumo kontekste, tai pat gebėjimo įvertinti žmogiškąjį faktorių.

1.1.1. Strategijos kūrimas ir politikos formavimas

Strategija, kaip sąvoka, dažniausiai yra siejama su organizacijos visapusiško plano sudarymu ir siektinų tikslų užsibrėžimu. 1962 m. verslo istorikas Alfredas D. Chandleris, cituojama pagal Fred Nickols (2016), pasiūlė strategiją apibrėžti kaip „įmonės pagrindinių ilgalaikių tikslų ir uždavinių suformulavimu, veiksmų kurso parinkimu ir išteklių, reikalingų šiems tikslams įgyvendinti, paskirstymu.“ (p. 1). Vadinasi, strategija turi būti kuriama aukščiausiame organizacijos vadovų lygmenyje, o pati formuluotė turi būti aiški ir lengvai įsisąmoninama. Jos efektyvus realizavimas priklausys nuo žemesnių valdymo lygių įsitraukimo ir darbuotojų sąmoningumo bei nusiteikimo.

Kalbant apie organizacijos kibernetinio saugumo kultūros formavimą, viena iš būtinųjų sąlygų yra strategijos ir procedūrų parengimas, kur turi būti nustatyta aiški atsakomybė, taip pat vadovaujamasi saugumo elgsena ir nuostatomis. Be to, literatūroje galima rasti ir tokių motyvų kaip vidaus politikos nustatymas, siekiant parodyti valdymo ketinimus ir kibernetinio saugumo svarbą, taip pat pateikti

bendras rekomendacijas tam, kad laiku spręsti valdymo iššūkius ir problemas (Knapp, Morris, Marshal ir Byrd, 2009, p. 494). Remdamiesi pradiniu arba esamu saugumo būklės įvertinimu, aukščiausiasis organizacijos valdymo sluoksnis turėtų parengti kibernetinio saugumo strategiją, į kurią būtų įtraukta organizacijos politika, kuria būtų vadovaujamasi, siekiant keisti ar gerinti organizacijos saugumo kultūrą, taip pat nustatomi saugumo tikslai ir organizacijos vizija kibernetinio saugumo plotmėje. Be visa to, ,,labai svarbu yra numatyti darbuotojų vaidmenį įgyvendinant organizacijos kibernetinį saugumą ir kokio rezultato siekiama, nes nuolatiniai elgesio pokyčiai įmanomi tik tada, kada tai susiję ir prilyginama su pačių darbuotojų sėkme ir pasitenkinimu.“ (ENISA, 2017, p. 31). Vadinasi, darbuotojas organizacijos strategijoje turi įžvelgti save, kaip vieną iš dedamųjų kibernetiniam saugumui užtikrinti, o jo vaidmuo yra kertinė sąlygą pasiekti efektyvų kibernetinio saugumo kultūros įgyvendinimą. Siekiant gauti darbuotojų paramą, supratimą ir palaikymą, visi organizacijos darbuotojai turėtų būti skatinami dalyvauti rengiant kibernetinio saugumo politiką. Tai užtikrina, kad saugumo priemonės būtų pritaikytos prie funkcinių ir hierarchinių organizacijos skirtumų ir kad jos nebūtų pernelyg apsunkintos ar komplikuotos. Sėkminga strategija, pasak ENISA (2017) rekomendacijų:

,,1) turėtų sustiprinti valdymo ir vadovavimo koncepciją;

2) turėtų būti suprojektuota panašiai kaip ir kitos verslo funkcijos, kad būtų lengviau įsisavinti;

3) turėtų būti kuo labiau pritaikyta, kad galima būtų panaudoti ją kuo ilgesnį laiką;

4) jos efektyvumas turėtų būti išmatuojamas, kad galima būtų pademonstruoti sėkmę.“ (p. 31-32).

Remiantis Hedstrom ir kt. (2011), jie pažymi, kad svarbu rasti pusiausvyrą tarp vadovybės ir darbuotojų perspektyvų, kad tokia politika būtų naudinga. Žvelgiant iš darbuotojo perspektyvos, jie siūlo vadovautis kokybės kriterijais, pagrįstais išorės ir vidaus politikos suderinamumu su dabartine darbo praktika, kad joje nebūtų nustatomi jokie tikslo konfliktai, o vyrautų aiškios tikslinės grupės ir būtų paaiškinamos atsakomybės bei lūkesčiai. Dalis autorių pabrėžia, kad kibernetinio saugumo politika yra dinamiško pobūdžio, ir kad būtina suprasti kontekstinius veiksnius, kurie gali turėti įtakos jos priėmimui (Knapp ir kt., 2009). Remiantis Karlsson ir Hedstrom (2014) dėl darbuotojų perspektyvos formuojant politiką, yra teigiama, kad informacinio saugumo valdymas turi aiškiau įtraukti vartotojus į informacijos saugumo kontrolės planavimą ir įgyvendinimą. Svarbu nustatyti konfliktų sritis tarp saugumo procedūrų ir teisėtų profesinio darbo vertybių ir įtraukti specialistus į šių konfliktų derinimą. Taigi darbuotojo perspektyva yra kontekstinių veiksnių, galinčių turėti įtakos priimant politiką, dalis ir į tai turėtų būti atsižvelgiama per organizacijos politikos formavimo procesą.

Kibernetinio saugumo kultūros įgyvendinimo strategija ir politika organizacijoje turėtų būti įtraukta į bendrą organizacijos strategiją, o aukštesnysis vadovų sluoksnis turėtų remti ir signalizuoti apie paramą ir skirti reikiamus išteklius kibernetinio saugumo kultūrai formuoti bei užtikrinti. Kibernetinio saugumo kultūros strategija ir politika turi koreliuoti su rizikos valdymo priemonėmis.

Organizacijos strategija ir politika kibernetinio saugumo klausimais turėtų kelti darbuotojų sąmoningumą ir supratimą apie rizikas ir grėsmes elektroninėje erdvėje bei nustatyti jų indėlį šiame kontekste.

1.1.2. Vadovavimas ir valdymas

Kibernetinis saugumas, kaip siektinas organizacijos rezultatas, negali apsieiti be tinkamo ir kryptingo vadovavimo ir valdymo. Sukūrus organizacijos strategiją ir patvirtinus kibernetinio saugumo kultūros įgyvendinimo politiką, labai svarbu, kad egzistuotų loginė tikslo įgyvendinimo hierarchija, kuri prasidėtų vadovų lygmeniu ir baigtųsi galiniu vartotoju tam, kad apibrėžti kiekvieno darbuotojo pareigas ir indelį kibernetinio saugumo kontekste. Remiantis ENISA (2017) išleistomis rekomendacijomis dėl kibernetinio saugumo kultūros formavimo organizacijoje, galima išskirti du vadovų sluoksnius:

1) *Aukštesnysis* – valdyba ar paskirtas aukšto rango asmuo, kuris teikia paramą kibernetinio saugumo užtikrinimui organizacijoje ir užtikrina pakankamus išteklius (žmogiškuosius ir finansinius) efektyvios kibernetinio saugumo kultūros įgyvendinimui ir išlaikymui. Aukštesnysis vadovų sluoksnis yra atsakingas už kibernetinio saugumo strategijos organizacijoje parengimą ir nustatytos politikos įtraukimą į ją. Taip pat šis vadovų sluoksnis yra atsakingas už bendro ir kiek platesnio kibernetinio saugumo supratimą ir požiūrio formavimą organizacijoje bei prioritetų nustatymą, kurie atitiktų organizacinius interesus.

2) *Vidurinis* – asmenys, paskirti vadovais, vadovauti atskiroms organizacijoms grupėms, taip pat tarpininkai, tarp darbuotojų ir aukštesniojo vadovų sluoksnio. Pagrindinis šio vadovų lygmens užduotis – kelti darbuotojų savimonę ir motyvaciją, paskirstyti užduotis ir nurodyti jų svarbą bei indėlį bendrame, organizacijos siektiname kibernetinio saugumo užtikrinimo rezultate. Kitaip tariant, vidurinis vadovų sluoksnis yra kertinis organizacijos organas, kas liečia kibernetinio saugumo kultūros formavimą. Todėl labai svarbu, kad šio tipo vadovai būtų motyvuoti ir gerai suprantantis kibernetinio saugumo svarbą bei naudą, norint efektyviai įtraukti ir pavaldžius darbuotojus. Kad kibernetinis saugumas nebūtų traktuojamas kaip našta, vidurinis vadovų sluoksnis turėtų nuolat skatinti saugų elgesį elektroninėje erdvėje, motyvuojant bei teikiant grįžtamąjį ryšį apie jų tinkamos veiklos rezultatą bendrame organizacijos kibernetinio saugumo kontekste.

Kalbant bendrai apie vadovų indėlį kibernetinio saugumo kultūros formavimo procese, labai svarbu surasti tinkamas paramos formas. Tokia parama gali būti teikiama įvairiais būdais: pradedant noru finansiškai investuoti į iniciatyvas ir palaikant kibernetinį saugumą, baigiant kibernetinio saugumo funkcijų paskirstymu bei organizavimu ir tolesniais su kibernetinio saugumu susijusiais darbais. Vadybos palaikymas yra nepaprastai svarbus kuriant ir išlaikant dėmesį kibernetiniam saugumui ir daro didelę įtaką kitų kibernetinio saugumo praktikų vykdymui. Vadybos palaikymo svarbą taip pat aiškina Niekerk ir Solms (2010), kurie teigia, kad saugumo kultūros kontekste elgesį organizacijoje lemia

darbuotojai, kurie bando patenkinti vadovybės reikalavimus, ir turimos žinios, leidžiančios tai padaryti. Todėl pirmiausia žinios suteikia darbuotojams priemones pakeisti jų elgesį. Vadinasi, vadovybė ne tik nustato organizacijos kryptį ir reikalavimus kibernetinio saugumo kontekste, tačiau jie taip pat turi suteikti darbuotojams galimybę įvykdyti tuos reikalavimus. Barton, Tejay, Lane ir Terrel (2016) pateikia įdomių rezultatų, kurie rodo, kad aukštesniųjų vadovų pastebėjimai ir suvokimas apie kibernetinio saugumo įgyvendinimą kitose organizacijose, daro įtaką ir darbuotojų įsitikinimams dėl kibernetinio saugumo. Panašiai teigia Flores ir kt. (2014) pabrėždami, kad būtent dalijimasis žiniomis apie saugumą gali padėti sumažinti rizikas. Jie nustatė, kad oficialios saugumo struktūros ir valdymo komitetai prisideda prie dalijimosi žiniomis, tačiau norint sukurti dalijimosi žiniomis mechanizmus, svarbiausi yra koordinavimo procesai, susiję su rizikos valdymu ir veiklos stebėjimu. Tokio dalijimosi žiniomis svarbą organizacijoje dar labiau pabrėžia Kearney ir Kruger 2016) teigdami, kad „suvokimo suderinimas tarp visų organizacijos darbuotojų grupių yra būtina saugios kibernetinės aplinkos sąlyga.“ (p. 50). Todėl įtraukimas ir dalyvavimas turėtų vykti visais organizacijos lygiais, tiek vertikaliai, tiek horizontaliai, siekiant palengvinti kibernetinio saugumo kultūros formavimą ir suteikti organizacijos nariams galimybę teigiamai prisidėti prie organizacijos saugumo. Kaip ir paminėta anksčiau, kitas labai svarbus vadovybės indėlis kibernetinio saugumo kultūros formavime yra motyvavimas. Pasak Ruighaver ir Maynard (2006), yra labai svarbu motyvuoti organizacijos narius, nes tai skatina nuolat mąstyti apie savo elgesį, suprasti, kaip tai gali turėti įtakos saugumui, ir ką jie patys gali padaryti, norėdami pagerinti bendrą organizacijos kibernetinį saugumą. Lin ir Wittmer (2017) tyrimas parodė, kad darbuotojai turi potencialo teigiamai prisidėti prie kibernetinio saugumo, jei jų dalyvavimas skatinamas, o tai, savo ruožtu, skatina iniciatyvumą, nes „pagal savo darbo patirtį darbuotojai gali nustatyti kibernetiniam saugumui iškilusias problemas kūrybiškai. Todėl svarbu iš jų reikalauti pastebėjimų, kurie remiasi į jų darbo patirtį ir specifines žinias.“ (p. 5). Visa tai parodo, kokią didžiulę įtaką požiūrio į kibernetinį saugumą formavime daro komunikacija ir derybos tarp vadovų ir darbuotojų, skatinimas įsitraukti. Be to, Ruighaver ir Maynard (2006) pabrėžia ir tai, kad svarbu, jog darbuotojai būtų atsakingi už tam tikras saugumo sritis, turėtų atsakomybės jausmą, kuris būtų traktuojamas kaip siektina darbuotojo savybė ir nuolat pabrėžiama paskatinimu. Sprendimų aptarimas ir grįžtamojo ryšio teikimas yra ne mažiau svarbūs formuojant ne tik atsakomybės jausmą, bet ir atskaitomybę.

Skyriuje aptartas vadovybės indėlis kibernetinio saugumo kultūros formavimo kontekste atskleidė, kad vadovų lygmuo, o jei konkrečiai vidurinis jų sluoksnis, kuris nuolatos kontaktuoja su kiekvienu iš pavaldžių darbuotojų, daro didžiausią įtaką požiūrio į saugumą formavime. Nuoseklus, struktūrizuotas ir motyvuojantis kibernetinio saugumo įgyvendinimo planas yra neatsiejama dalis efektyvios kibernetinio saugumo kultūros, kaip siekiamo rezultato, procese. Todėl labai svarbu, kad griežtą ir kritinį požiūrį bei suvokimą apie kibernetinį saugumą, visų pirma, turėtų patys organizacijos vadovai.

1.1.3. Kibernetinio saugumo švietimas

Kibernetinio saugumo kultūra yra dažnai suprantama kaip aibė techninių ir organizacinių sprendimų, kurie turėtų užkardyti rizikas elektroninėje erdvėje ir apsaugoti organizaciją nuo kibernetinių incidentų. Tačiau dažnai išsamiai ir apgalvotai parengta kibernetinio saugumo įgyvendinimo strategija ir ją lydinti organizacijos politika ne visada praktikoje yra taip paprastai įgyvendinama. Žinant tai, kad visi organizaciniai ir techniniai sprendimai yra sukurti ir įgyvendinami žmonių, derėtų kritiškai įvertinti ir galimas tų sprendimų klaidas, rizikas ar netinkamą panaudojimą. Todėl kibernetinio saugumo kultūra gali būti veiksminga tik tada, kada darbuotojai turi tam reikalingas priemones, žinias, įgūdžius ir supratimą apie savo vaidmenį bendrame jos įgyvendinimo kontekste. Tam, kad pastaroji sąlyga būtų įgyvendinta, reikalingas darbuotojų švietimas kibernetinio saugumo klausimais bei nuolatinis kvalifikacijos atnaujinimas, žinių vertinimas. Įvairūs mokymai, pratybos, diskusijos, paskaitos, simuliacijos ar kitos interaktyvios veiklos formuoja darbuotojų požiūrį į kibernetinį saugumą, ugdo kritinį mąstymą ir priverčia vertinti rizikas. Todėl toliau skyriuje bus detaliau aptartos kibernetinio švietimo formos ir bendrinė gebėjimo nuolatos įvertinti žmogiškąjį faktorių nauda, norint suformuoti efektyvią organizacijos kibernetinio saugumo kultūrą.

Dažnai eiliniam darbuotojui kyla abejonių dėl to, ar kibernetinės grėsmės iš tikrųjų yra realios ir ar jos yra svarbios organizacijai, kurioje jis dirba. Tai akcentuoja ir Cone, Irvine, Thompson ir Nguyen (2007) teigdami, kad ,,vartotojai gali būti apatiški kibernetinio saugumo grėsmių atžvilgiu ir dažnai laikosi ,,stručio požiūrio“ į naudojamų informacinių sistemų saugumą, manydami, kad mažai ką gali padaryti, kad sušvelnintų pastarųjų pažeidžiamumą.“ (p. 63). Remiantis vienos didžiausių pasaulyje telekomunikacijų įmonės ,,Verizon” atliktu tyrimu (2020), net 67 % visų kibernetinių incidentų sudarė prisijungimo duomenų vagystės, socialiniai išpuoliai (sukčiavimas, socialinė inžinerija, kenksmingo kodo pristatymas el. laišku ir pan.) bei konfigūracijos klaidų išnaudojimas. Nors tai ir atskleidžia, kad daugiau nei pusė kibernetinių incidentų įvyko dėl žmogiškosios klaidos, kita vertus, nederėtų žmogaus laikyti kaip grėsmės kibernetiniam saugumui, o atvirkščiai – įvertinti, kaip jis gali prisidėti prie pastarųjų grėsmių mažinimo. Apie tai rašė ir teoretikas Schlienger (2003) teigdamas, kad informacinis saugumas ir jo valdymas dažniausiai nepaiso žmogiškosios dimensijos: pagrindinis dėmesys skiriamas techninėms ir procedūrinėms priemonėms, o pats žmogus vertinamas kaip saugumo priešas bet visai ne kaip saugumo subjektas. Taigi, žmonių vaidmuo kibernetinio saugumo rizikų vertinime yra aiškus. Tačiau žinių perdavimas, sąmoningumo didinimas ir įtakos darymas darbuotojų elgesiui elektroninėje erdvėje yra kur kas didesnio dėmesio reikalaujantys iššūkiai, kuriuos ignoruojant, kibernetinio saugumo kultūra negali būti efektyviai įgyvendinta. Dėl šios priežasties labai svarbu yra įvertinti organizacijos darbuotojų žinias, kvalifikaciją, motyvaciją bei įsitikinimus apie kibernetinį saugumą ir jo svarbą. Remiantis ENISA (2017) norint veiksmingai paveikti organizacijos supratimą apie saugumą, mokymo programos turėtų būti rengiamos atsižvelgiant į du dalykus: ,,(1) supratimą apie atsakomybes, susijusias su skirtingomis

darbuotojų funkcijomis; (2) minimalaus informuotumo lygio visos įmonės mastu pasiekimą.“ (p. 39). Pfleeger ir Caputo (2012) sutinka ir teigia, kad „dauguma darbuotojų neturi bendro supratimo apie saugumą ir nežino, kaip saugumas gali paveikti visas jų darbo funkcijas ir kitas veiklas.“ (p. 602). Taip pat nemaža dalis kibernetinio saugumo specialistų savo tyrimuose (Kearney, 2010; Thomson ir Niekerk, 2011) įvardija žmogaus supratimo didinimą kibernetinio saugumo srityje kaip vieną pagrindinių priemonių, siekiant sumažinti organizacijos RIS pažeidžiamumą. Tačiau tam, kad darbuotojus būtų galima įtraukti į kibernetinių incidentų rizikų mažinimo procesą, organizacijoje turėtų būti aiškiai įvardinta būtina apsaugoti infrastruktūra ir informacija, jų svarba organizacijai ir pastarųjų kontrolės praradimo pasekmės. Be to, Thsohou, Karyada ir Kokolakis (2015) teigia, kad žmonės aiškina ir interpretuoja su rizika susijusią informaciją per pažintinio ir kultūrinio šališkumo objektyvus. „Nepripažindamos ir neatsižvelgdamos į jų poveikį žmogaus informacijos apdorojimui ir sprendimų priėmimui, saugumo supratimo programos nesugeba patenkinti individualių darbuotojų mokymosi poreikių.“ (p. 139). Todėl svarbu pasirūpinti, kad mokymo turinys ir tipas atitiktų tikslinę (– es) grupę (– es) pagal darbuotojų atliekamas funkcijas, žinias ir pagal tai, kiek stipriai jų veikla gali daryti įtakos visos organizacijos kibernetiniam saugumui. Siekdama geriau informuoti apie kibernetinį saugumą, organizacija turi užtikrinti, kad mokymai būtų pritaikyti tikslinei populiacijai, nes „negalima manyti, kad vidutinis darbuotojas turi reikiamų žinių, kad galėtų saugiai atlikti savo darbą“ (Niekerk ir Solms, 2010, p. 478). Todėl akivaizdu, kad patys mokymai turėtų suteikti bent bazinį lygį, o darbuotojai mokymų metu turėtų įgyti žinių apie rizikas, gauti įgūdžių ir išmokti savikontrolės, konkrečiai susijusios su jų tiesiogine veikla ir vaidmeniu organizacijoje. Pavyzdžiui, Choi ir Nazareth (2015) atliktas tyrimas nustatė, kad organizacijos vadybininkų mokymas atlikti lyderystės pokyčius, teigiamai paveikė kibernetinio saugumo įgyvendinimo efektyvumą. Vadinasi, tokio pobūdžio vadų mokymai gali teigiamai paveikti ir bendrą organizacijos sąmoningumą: vadovai gebės paaiškinti ir įtikinti darbuotojus visuose organizacijos lygmenyse apie tai, kas yra kibernetinis saugumas, kokios yra galimos rizikos ir kaip jos gali paveikti jų atsakomybės sritis bei darbo funkcijas. Tačiau egzistuoja dar dvi, atskiro dėmesio vertinant žmogiškąjį faktorių reikalaujančios darbuotojų grupės – RIS saugos personalas ir galinių įrenginių naudotojai.

Remiantis ENISA (2017) rekomendacijomis dėl kibernetinio saugumo kultūros įgyvendinimo organizacijoje, RIS saugos personalo / komandos vaidmuo organizacijoje yra daugialypis. Komanda turėtų užtikrinti, kad būtų priimtos naujausios techninės priemonės, kurios yra veiksmingos, paprastos, naudingos ir palaiko saugų elgesį, nes nėra pernelyg apsunkintos. Norėdami veiksmingai pasiekti šiuos tikslus pritaikydami sprendimus, techninę infrastruktūrą prižiūrintys asmenys turi suprasti ne tik savo organizacijos verslo struktūrą ir jos veiklą, bet ir turėti specifinių žinių ir reikiamą kvalifikaciją. Dėl šios priežasties organizacijos išūkiu tampa ir nuolatinis IT personalo kvalifikacijos kėlimas bei žinių atnaujinimas, norint, jog su kibernetinio saugumo techniniais sprendimais dirbanti komanda turėtų

pakankamai kompetencijos, galėtų bendradarbiauti su išorės paslaugų teikėjais, galėtų valdyti bei sumažinti riziką klaidų organizacijos RIS konfigūracijoje, gebėtų pasidalinti savo įžvalgomis ir teikti siūlymus organizacijos vadovybei. Tai taip pat gali paskatinti saugumo švietimo plėtrą ir prevencinių technologijų pritaikymą visoje organizacijoje. RIS saugos personalo suvokimo, gebėjimų, žinių ir motyvacijos vertinimas, remiantis įvairių kibernetinio saugumo praktikų **(**Trevors, 2019; Stitt, 2020; Brook, 2020**)** įžvalgomis, turėtų būti įvykdytas dar darbo pokalbio metu. Ankstyvas organizacijos RIS saugos personalo vertinimas, neleidžia atsirasti su organizacijos strategija ir kibernetinio saugumo politika nekoreliuojantiems veiksmams, žmogiškosioms klaidoms, taip pat kilti nesusipratimams.

Kita ne mažiau svarbi darbuotojų grupė, daranti įtaką organizacijos kibernetinei saugumo kultūrai yra galinių įrenginių naudotojai. Ši žmonių grupė dažniausiai nepasižymi žiniomis apie kibernetinį saugumą, nes jų pareigos organizacijoje nėra su tuo tiesiogiai susijusios. ,,Todėl kiekviena organizacija turi skatinti kultūrą, kurioje visi darbuotojai, šiuo atveju ir RIS naudotojai, yra atsakingi, gindami įmonę nuo kibernetinių atakų.“ (Kearney, 2010, p. 36). Kad politika būtų veiksmingai įgyvendinta, ji pirmiausia turi būti suprantama visiems darbuotojams. Nesuprantat, ko iš jų tikimasi, organizacijos RIS naudotojams yra sunku jos laikytis ir dažnai tai gali atrodyti kaip primesta prievolė, stabdanti verslo procesus ir jų produktyvumą siekiant darbo rezultato. Esminiu išūkiu tampa įmonės verslo misijos ir siektino rezultato suderinamumas su kibernetinio saugumo įgyvendinimo klausimais. Todėl ir RIS naudotojams turėtų būti aišku, koks yra tikslus jų vaidmuo ir atsakomybė kibernetinio saugumo užtikrinimo kontekste. Kitas svarbus aspektas yra tai, kad žmonės gali padėti užkirsti kelią saugumo pažeidimams tik tada, kai žino apie pavojus ir yra mokomi saugaus elgesio elektroninėje erdvėje neatsiejamai nuo jų įprasto darbo. Bendra kliūtis kurti aplinką, kurioje vadovybė ir darbuotojai dirba siekdami tų pačių informacijos saugumo tikslų, yra darbuotojų apatija (Thomson ir Niekerk, 2011). Ji atsiranda dėl žinių ir kvalifikacijos stokos. Yra teigiama, kad ,,darbuotojai aktyviai stengsis apeiti saugumo politiką, jei ji neleis jiems atlikti nustatytų verslo funkcijų; bus primesta, kas, jų manymu, yra nepateisinama našta; ir (arba) įves sumaišties, kam turėtų būti teikiama pirmenybė organizacijoje. Paprastai tai kyla ne iš pykčio ar dviprasmybės, o iš noro sėkmingai atlikti savo darbą.“ (ENISA, 2017, p. 30). Vadinasi, neužtenka paruošti kvalifikuoto IT personalo ir galvoti, kad organizacijos kibernetinis saugumas bus užtikrintas. Didžiulį dėmesį į kibernetinio saugumo grėsmių supratimo formavimą ar kėlimą reikia skirti ir su kibernetiniu saugumu tiesiogiai nesusijusiems organizacijos darbuotojams. Kibernetinė higiena ir elgesio elektroninėje erdvėje taisyklės neturėtų būti suprastos kaip IT personalo atsakomybė. Tai turėtų būti diegiama kaip bendras, visų organizacijos darbuotojų siektinas rezultatas.

Informavimo apie kibernetinį saugumą mokymuose turėtų būti atsižvelgiama į tai, kad skirtingi darbuotojų vaidmenys gali turėti skirtingus žinių ir mokymo metodų poreikius. Kalbant apie mokymų formas ir metodus, iš esmės, nėra nustatyta reikalavimų ar nuostatų, jei pasiektas rezultatas koreliuos su išsikeltais tikslais. Taip pat svarbu, kad kibernetinio saugumo mokymai būtų įdomūs ir įtraukiantys.

Vadinasi, metodai perteikti darbuotojams žinias apie kibernetinio saugumo svarbą yra pačios organizacijos vidinis dalykas, priklausantis nuo politikos, biudžeto, ar net norų. Tačiau nereikėtų traktuoti, kad kiekvienai auditorijai yra tinkami visi mokymosi metodai. Nors ENISA (2017) savo rekomendacijose siūlo mokymų formas nuo elementarių filmų ar žaidimų iki individualizuotų seminarų, krizių valdymo pratybų, Cone ir kt. (2007) pažymi, kad „daugelis mokymo formų žlunga, nes yra neprotingos ir nereikalauja, kad vartotojai galvotų apie saugumo koncepcijas ir jas taikytų.“ (p. 63). Jis taip pat pabrėžia, kad svarbu yra, jog mokymasis, be to, kad sudomintų besimokančiuosius, galėtų suteikti galimybę besimokantiesiems išreikšti ir gilinti žinias, naudojant scenarijaus pagrindu pritaikomus įgūdžius ir technologijas, gerinančias jų supratimą. Kitas svarbus dalykas, į kurį reikia atkreipti dėmesį organizuojant mokymą yra tai, kad jis turėtų būti neatsiejamas nuo organizacijos darbotvarkės ir būti nuolatinio tobulinimosi kampanijos dalimi. Pfleeger ir Captuo (2012) aiškina, kad elgesio pokyčiams reikia laiko, todėl pokyčių inicijavimo planai turėtų būti numatyti pakankamai racionaliame laiko periode juos įgyvendinti ir leisti, kad tai taptų kultūros ar bendrosios praktikos dalimi. Tuo tarpu Eminagaoglu, Ucar ir Eren (2009) pabrėžia, kad reikia nuolatinių informuotumo apie kibernetinį saugumą didinimo kampanijų ir pagalbinės medžiagos, siekiant užtikrinti, kad darbuotojai nepamirš to, ko išmoko pradinio mokymo metu, ir atkreipia dėmesį, kad kampanijos laikui bėgant turi keistis. Taigi, sudarius tinkamą sąmoningumo ugdymo programą atsispindės kiekvieno darbuotojo psichologija, pažintiniai gebėjimai, socialinis požiūris ir šiuolaikinė darbo aplinka. Programos turėtų suteikti darbuotojams autonomiją, įsitraukimą ir atsakomybę, o saugumo tikslai turėtų būti suderinti su įmonės motyvacija ir organizacine struktūra. Galiausiai vadovybė turėtų parodyti organizacijos pavyzdį, skirdama pakankamai išteklių ir siūlydama nuolatines gaires ir palaikymą: svarbūs konkretūs, realistiški ir išmatuojami tikslai, taip pat tinkamas bendravimas su darbuotojais, norint sėkmingai įgyvendinti bet kokią sąmoningumo ugdymo programą. Geros supratimo apie saugumą programos sėkmės veiksniai gali būti susisteminti taip, kad būtų kaskart atsižvelgiama tiek į aktualias, naujo tipo grėsmes, tiek į darbuotojų ir organizacijos pokyčius. Turėtų būti įtrauktos visos reikalingos žinios įvairiems darbuotojams, taip pat vadovybės vizija apie vaidmenis ir atsakomybę. Programa turėtų teigiamai paveikti dalyvių žinias, požiūrį ir elgesį. Atvira komunikacija ir sąmoningumas visoje organizacijoje leidžia užtikrinti vidinį nuoseklumą ir grįžtamąjį ryšį apie tobulintinus dalykus.

Žinios, požiūris, vertybės ir suvokimas gali nulemti žmonių elgesį. Be to, reikalingas ir pačios organizacijos gebėjimas valdyti žmogiškojo faktoriaus riziką, kartu suteikiant organizacijai galimybę priimti ir naudoti naujas informacines technologijas. Tai svarbu, nes saugumo supratimo programos, švietimas ir mokymas gali būti panaudoti taip, kad paveiktų darbuotojų žinias, kurios kartu su organizacijos kultūros pokyčiais gali sukurti ir ilgalaikę kibernetinio saugumo kultūrą. Švietimas yra nepamainoma priemonė norint pakeisti darbuotojų supratimą į kibernetinį saugumą bei išaiškinimą, ką, kaip ir kodėl daryti kitaip. RIS saugos personalas turėtų gebėti savo turima kvalifikacija rinkti duomenys

apie kibernetinę riziką ir išpuolius prieš organizacijos RIS tinklus tam, kad būtų išsamiai suprastas galimų rizikų profilis ir įvertintas įgyvendintos kibernetinio saugumo kultūros programos poveikis. Tuo tarpu su kibernetiniu saugumu ir jo užtikrinimu tiesiogiai nesusiję darbuotojai turėtų suprasti, kad jų elgesys stipriai prisideda prie organizacijos kibernetinio saugumo profilio kūrimo elektroninėje erdvėje. Todėl galima teigti, kad grėsmių tinkamas pateikimas ir priemonių suteikimas, priimtino ir nepriimtino elgesio apibrėžimas, taikytinos sankcijos ir atsakomosios priemonės, taip pat naujausių kibernetinio saugumo užtikrinimo praktikų pateikimas – skatina žmonių atsakomybę ir jos laikymąsi. Šis supratimas gali būti pasiektas per atvirą, savalaikį bendravimą ir tinkamą bei gerai suplanuotą kibernetinio saugumo švietimo kultūrą.

1.1.4. Kibernetinio saugumo higiena

Kibernetinio saugumo higiena mokslinėje literatūroje yra apibrėžiama, kaip kibernetinio saugumo įgyvendinimo praktika, kurią turėtų palaikyti interneto vartotojai su tikslu užtikrinti savo asmens duomenų, patalpintų prie interneto prijungtuose įrenginiuose, saugumą ir vientisumą kibernetinių pavojų kontekste (Vishwanathm ir kt., 2020). Kitaip tariant, kibernetinė higiena atskleidžia geriausią praktiką ir kitą veiklą, kurią kompiuterių sistemos administratoriai ir naudotojai, dalyvaudami bendroje internetinėje veikloje, gali įsipareigoti vykdyti su tikslu pagerinti tiek savo, tiek organizacijos, kurioje dirba kibernetinį saugumą. Pavyzdžiui, naršydami internete, siųsdami el. laiškus, talpindami organizacijos ar asmens duomenis į debesį. Analizuojant kibernetinio saugumo kultūros sąvoką mokslinėje literatūroje dažnai kibernetinio saugumo higiena nėra traktuojama kaip kibernetinio saugumo kultūros dalis. Tačiau vis daugiau šiuolaikinių praktikų ir IT ekspertų, susiduriančių su kasdieniais iššūkiais formuojant organizacijos kibernetinio saugumo kultūrą, pabrėžia kibernetinio saugumo higienos svarbą ir įvardija, jog tai didžiąja dalimi turi būti integruota į kibernetinio saugumo kultūros strategijos kūrimo ir politikos formavimo procesus. Todėl toliau skyriuje bus nagrinėjama, kaip kibernetinio saugumo higiena turėtų būti integruota į kibernetinio saugumo kultūros formavimą organizacijoje.

Praeituose skyriuose išnagrinėjus kibernetinio saugumo švietimo ir gebėjimo vertinti žmogiškąjį faktorių indėlį, formuojant organizacijos kibernetinio saugumo kultūrą, akivaizdu, kad organizacijos strategija ir politika kartu su darbuotojų gebėjimais kritiškai vertinti kibernetinį saugumą, nepriklausomai nuo to, kokią rolę jie žaidžia viso to kontekste, turi sukurti ir praktinę priemonių kibernetiniam saugumui užtikrinti bazę. ENISA (2016) savo atliktame tyrime apie kibernetinės higienos praktikas Europos valstybėse, išskyrė 5 pagrindinius praktinius kibernetinės higienos įvedimo ir palaikymo tikslus:

,,1) Apsaugoti perimetrą;

2) Apsaugoti tinklą;

3) Apsaugoti asmeninius įrenginius;

4) Gebėti saugiau naudotis debesijos paslaugomis;

5) Apsaugoti tiekimo grandinę (angl. Supply Chain).“ (p. 15).

Visi šie tikslai turėtų atsispindėti organizacijos kibernetinio saugumo strategijoje ir formuojamoje politikoje. Tačiau tam, kad tikslai neliktų tik teorine siekiamybe, organizacijai reikėtų įvardinti ir šiems tikslams pasiekti ketinamus naudoti metodus. Patys metodai, remiantis ENISA tyrimu (ten pat, p. 24) ir ekspertų (Trevors, 2019; Stitt, 2020; Brook, 2020) įžvalgomis, yra daugiau mažiau panašūs ir IT bendruomenėje suprantami vienodai:

1) Nusistatyti svarbiausias organizacijos paslaugas, produktus, suteikti jiems prioritetus;

2) Dokumentuoti visą turimą techninę įrangą su tikslu turėti valdomo ir turimo apsaugoti RIS turto paveikslą;

3) Dokumentuoti visos programinės įrangos sąrašą, jog vykdyti savalaikį jos palaikymą, atnaujinimą, pažeidžiamumų stebėjimą;

4) Sudaryti organizacijos reagavimo į kibernetinius incidentus planą;

5) Valdyti sistemų prieigą remiantis mažiausių teisių suteikimo principu ir prižiūrėti vartotojų paskyras;

6) Valdyti technologinius pokyčius ir naudoti RIS įrangos standartizuotas saugias konfigūracijas;

7) Įvesti slaptažodžių kūrimo ir keitimo sistemą;

8) Valdyti kibernetinę riziką, susijusią su tiekėjais ir išorinėmis techninėmis priklausomybėmis (debesijos paslaugos);

9) Filtruoti elektroninius laiškus;

10) Sudaryti vartotojams galimybę pranešti IT saugos personalui apie galimas kenkėjiškas veiklas;

11) Reguliariai kurti atsargines duomenų kopijas ir atlikti savalaikį bandomąjį sistemos atkūrimą;

12) Užtikrinti panašų saugumo lygį visoje tiekimo grandinėje.

Organizacija pati gali nuspręsti kiek ir kokių metodų ji naudos kibernetinio saugumo higienai savo informacinėse sistemose / tinkluose įvesti, priklausomai nuo turimų tiek finansinių, tiek žmogiškųjų išteklių. Įprastos kibernetinės higienos procedūrų ir metodų taikymas organizacijos kompiuteriams ir programinei įrangai yra naudingas dėl dviejų priežasčių – atsiranda savalaikė sistemų priežiūra ir užtikrinamas saugumas. Priežiūra būtina, kad kompiuteriai ir programinė įranga veiktų maksimaliai efektyviai, nes failai su laiku gali tapti fragmentuotais, o programinė įranga technologiškai pasenti. Dėl šios priežasties padidėja organizacijos informacinių sistemų ir tinklų pažeidžiamumo rizika. Todėl įprastinė sistemų techninė priežiūra, tikėtina, leis organizacijai greičiau pastebėti daugelio valdomų

sistemų ir tinklo spragų bei jas operatyviai spręsti, neleidžiant iškilti rizikoms, tokioms kaip duomenų praradimas, ar kritinių paslaugų sutrikdymas.

Taigi, aukščiau paminėti kibernetinės higienos įvedimo metodai kuria pridėtinę vertę formuojant bendrąjį organizacijos kibernetinio saugumo paveikslą. Be visa to, yra svarbu suprasti, kad darbuotojai ir kiti organizacijos nariai yra pirmoji gynybos linija nuo kibernetinių atakų. Tai, kaip jie elgiasi kibernetinėje erdvėje būdami darbe ir naudodamiesi organizacijos teikiama infrastruktūra daro įtaką organizacijos pažeidžiamumui. Dažnai viskas, ko reikia, yra vienas silpnas slaptažodis, netinkamas prisijungimas prie viešojo tinklo arba spustelėjimas ant nepatvirtintos nuorodos, kad iškiltų pavojus organizacijos kibernetiniam saugumui. Organizacinė kibernetinio saugumo kultūra, kurioje nepakankamai akcentuojama kibernetinio saugumo higiena, sukels daugiau galimybių nusikaltėliams rasti sistemos pažeidžiamumus. Tad norint sukurti tvirtą kibernetinio saugumo kultūrą, turi būti į jos formavimą įtraukti visi suinteresuotieji subjektai, o jiems vadovautis sukurtos griežtos kibernetinio saugumo higienos taisyklės.

1.1.5. Bendradarbiavimas kibernetinio saugumo klausimais

Kibernetinio saugumo kultūra dažniausiai nėra formaliai apibrėžta ar įvardinta su kibernetiniu saugumu susijusiuose teisės aktuose. Pats žodis kultūra iš esmės yra suprantamas kaip kintantis ir nuo daugybės išorinių rodiklių priklausantis veiksnys. Kiekvienoje aplinkoje, konkrečiu atveju organizacijoje, kultūra gali būti skirtinga, o tai reiškia, kad yra apstu ir skirtingų patirčių, geruųjų ir blogųjų praktikų. Visa tai gali būti pritaikoma ir kibernetinio saugumo kultūrai. Poreikis skirtingoms organizacijoms bendradarbiauti, dalintis patirtimi, praktikoje veikiančiais ar nepasiteisinusiais saugumo sprendimais yra kibernetinio saugumo, kaip reiškinio, tiek nacionaliniu, tiek globaliu mastu užtikrinimo dalis. Todėl toliau darbe bus analizuojamas tarpinstitucinio ir viešojo-privataus sektorių bendradarbiavimo faktorius kibernetinio saugumo kultūros įgyvendinimo kontekste.

Susisteminus literatūroje dažniausiai aptinkamas tarpinstitucinio bendradarbiavimo sąvokas, tarpinstitucinį bendradarbiavimą būtų galima apibrėžti, kaip priemonių visumą, kurių pagalba vyksta formali arba neformali sąveika tarp bet kokio tipo institucijų, išplečiant jų žinias ir pajėgumus, informacijos keitimosi rūpimais klausimais konkrečiose srityse metodais. Išanalizavus mokslinėje literatūroje tarpinstitucinio bendradarbiavimo būdus, galima išskirti šiuos du pagrindinius:

1) *Formalus* – teisės aktuose reglamentuota partnerystė;

2) *Neformalus* – bendradarbiavimas, kurio formos ir procedūros nėra reglamentuotos teisės aktuose. Šią bendradarbiavimo formą taikančios institucijos dažnu atveju savo iniciatyva pasirenka metodus informacijos apsikeitimui.

Jurkonienės ir Karčiauskienės (2017) atliktame tyrime akcentuojama neformaliojo tarpinstuticinio bendradarbiavimo svarba ir įtaka siektiniems rezultatams. Jos siūlo išskirti sekančias neformalaus tarpinstitucinio bendradarbiavimo formas:

„1) Kanclerių klubas – susitikimai, kuriuose gvildenamos kiekvienos institucijos problemos, dalijamasi gerosiomis patirtimis, keliamos kompetencijos, stiprinami ryšiai ir bendradarbiavimas, formuojama konsensuso kultūra, informuojama apie kitų institucijų įsipareigojimus ir siekius.

2) Strategų tinklas – orientuotas į strategų vaidmens stiprinimą, kurie turėtų įtvirtinti bendrus tarpinstitucinių klausimų sprendimo standartus ir praktikas, savo ruožtu, užkirstų kelią rutininiams, pokyčių nedarantiems sprendiniams ir neleistų kurti perteklinių dokumentų.

3) Pažangos gildija – savo srities ekspertų, praktikų ir akademikų sutelkimas su tikslu analizuoti realių problemų sprendimą, analizuojant egzistuojančius iššūkius ir įsitraukiant į sprendimų paieškas.“ (p. 15-17).

Šie tarpinstitucinio bendradarbiavimo metodai / formos gali būti pritaikomi įvairiose srityse, tarp jų ir organizacijos kibernetinio saugumo kultūros formavime. Veiksmingas kibernetinio saugumo kultūros diegimas organizacijoje reikalauja įvairios tiek nacionalinės, tiek tarptautinės bendradarbiavimo veiklos, kurią apsibrėžti galima tik suprantat tarpinstitucinio bendradarbiavimo esmę ir teorijos siūlomus metodus. Kad kibernetinis saugumas būtų pažįstamas per skirtingų organizacijų saugumo prizmes, ši veikla turi būti vykdoma ne tik tarp to paties tipo organizacijų, bet ir įvairiais lygmenimis, pavyzdžiui, tarp viešojo ir tarp privačiojo sektoriaus suinteresuotų subjektų. Todėl toliau skyriuje bus apibrėžiamos viešojo-privataus sektorių bendradarbiavimo formų praktikos.

Kalbant apie viešojo-privataus sektorių bendradarbiavimą, labai svarbu išskirti tokio bendradarbiavimo ypatumus bei svarbą ir naudą organizacijoms. Remiantis ENISA (2017, p. 13) atliktu tyrimu apie viešojo ir privataus sektoriaus bendradarbiavimą, pagrindiniai faktoriai, skatinantys organizacijas jungtis į šią iniciatyvą ir sąveikauti kibernetinio saugumo klausimų kontekste yra sekantys:

1 lentelė. Privataus ir viešojo sektoriaus bendradarbiavimą skatinantys faktoriai

Privataus sektoriaus	Viešojo sektoriaus
Galimybė pasinaudoti valstybės lėšomis	Geresnis supratimas apie YSI objektų ir pramonės apsaugą
Galimybė daryti įtaką įstatymams ir valstybės reglamentuotiems standartams	Galimybė sukurti įvairių privataus sektoriaus iniciatyvų sinergiją
Galimybė prieiti prie konfidencialios viešojo sektoriaus informacijos (ES teisės aktai, kovų su elektroniniais nusikaltimais atvejai ir pan.)	Galimybė naudotis privataus sektoriaus ištekliais (ekspertais) su tikslu lengviau

	nusistatyti tinkamus standartus ir įvesti gerąsias praktikas
Užsitikrinimas, kad produktai, teikiami šios bendradarbiavimo iniciatyvos kontekste, yra geros kokybės, kurią garantuoja pati valstybė	
Dalinimasis žiniomis, patirtimi ir gerosiomis praktikomis	
Atsparumo didinimas kibernetinėje ekosistemoje	
Pasitikėjimo didinimas tarp privataus ir viešojo sektorių: tokio tipo bendradarbiavimas leidžia sutikti skirtingus žmones su tikslu pažinti skirtingas patirtis, gauti kokybišką informaciją ir įgyti reikiamą požiūrį krizės atveju	
Užmegzti tiesioginius ir patikimus ryšius su kitomis organizacijomis	

Šaltinis: ENISA, 2017.

Organizacijų bendradarbiavimas kibernetinio saugumo klausimais neša ne tik aukščiau įvardintą naudą (žr. 1 lent.), bet ir generuoja ilgalaikių tikslų įgyvendinimą ir efektyvių rezultatų pasiekimą. Tai taip pat kuria pridėtinę vertę kibernetinio saugumo kultūros įgyvendinimo procese, nes formuoja įvairiapusį ir sisteminį požiūrį į saugumą bendrine prasme, padeda formuojant organizacijos kibernetinio saugumo politiką ir taikant kibernetinio saugumo higienos priemones.

Taigi, tarpinstitucinio bei viešojo-privataus sektorių bendradarbiavimo poreikis apima ne tik dalijimąsi informacija apie kibernetines grėsmes, rizikas, sistemų ir programinės įrangos pažeidžiamumą ir geriausią praktiką didinant atsparumą pastariems faktoriams nacionaliniu lygmeniu. Tai taip pat tai turėtų apimti ir formalių bei neformalių darbo santykių plėtojimą su pagrindiniais suinteresuotaisiais subjektais kitose šalyse, su tikslu įvertinti savo pastangas ir metodus lyginat su kitų šalių organizacijų pastangomis ir metodais įgyvendinant efektyvią kibernetinio saugumo kultūrą.

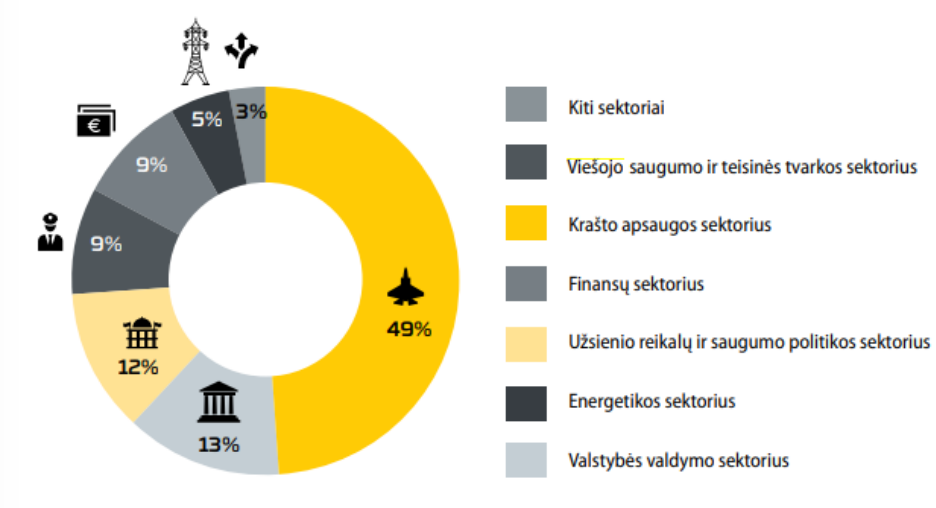
Apibendrinant, kibernetinio saugumo kultūros formavimo organizacijoje samprata, remiantis kibernetinio saugumo teoretikų, ekspertų ir įvairių tarptautinių institucijų praktinėmis įžvalgomis, yra bendrinė. Tai yra, kad visos organizacijos, įgyvendindamos kibernetinio saugumo kultūrą turi turėti kibernetinio saugumo strategiją / politiką, gebėti valdyti kibernetinį saugumą ir užtikrinti vadovavimo mechanizmus, motyvuojant darbuotojus ir formuojant jų požiūrį apie saugumą, palaikant kibernetinio saugumo higieną, skatinant skaitmeninį brandą ir keliant žinių lygį bei užtikrinant nuolatinį bendradarbiavimą kibernetinio saugumo klausimais su kitomis organizacijomis. Visgi, kad teorija galėtų būti praktiškai pritaikoma, svarbu identifikuoti šių pagrindinių aspektų įgyvendinimo būdus ir aplinkybes, lemiančias organizacijų efektyvios kibernetinio saugumo kultūros formavimą.

1.3 Kibernetinio saugumo kultūros formavimo ypatumai viešajame sektoriuje

Kibernetinio saugumo kultūros formavimas organizacijoje susideda iš aibės vadybinių, organizacinių, techninių bei žmogiškųjų elementų nepriklausomai nuo organizacijos struktūros ar veiklos specifikos. Kibernetinis saugumas ir jo įgyvendinimo svarba yra svarbi visose, elektronine erdve besinaudojančiose organizacijose, nes hakerių tikslai ir kibernetinių atakų vektoriai yra didžiąja dalimi vienodi, nepriklausomai nuo to, ar organizacija yra viešojo, ar privataus sektoriaus. Tačiau kibernetinio saugumo kultūros formavimo pagrindinių aspektų įgyvendinimo metodai ir procedūros dažnu atveju gali skirtis dėl organizacijas lydinčių vidinių ir išorinių aplinkybių, pavyzdžiui, politikos, kaštų, reikšmės valstybės nacionalinio saugumui, teisinio reglamentavimo, tarptautinių įsipareigojimų ar taikomų organizacinių ir techninių priemonių. Dėl šios priežasties, vertinant kibernetinio saugumo kultūrą valstybinėse institucijose, yra svarbu suprasti, kokios tendencijos, iššūkiai ir problemos lydi viešojo sektoriaus institucijas, skirtingai nei privataus sektoriaus. Todėl toliau skyriuje bus identifikuojami pagrindiniai kibernetinio saugumo kultūros įgyvendinimo ir palaikymo aspektai viešajame sektoriuje, remiantis pasauline patirtimi.

Visų pirma, kalbant apie privataus ir viešojo sektoriaus kibernetinio saugumo kultūros formavimo aplinkybes lemiančius skirtumus, pagrindinis aspektas yra infrastruktūros reikšmė nacionaliniam saugumui. Viešojo sektoriaus institucijos yra pagrindinės valstybinių informacinių išteklių ir viešųjų paslaugų valdytojos. Tai reiškia, kad didžioji dalis visuomenei jautrios informacijos yra tvarkomos būtent pastarosiose ryšių ir informacinėse sistemose. Todėl viešasis sektorius tampa pažeidžiamas ne tik todėl, kad tai yra politiškai ir finansiškai naudingas taikinys, bet ir todėl, kad jo valdomi ir tvarkomi duomenys yra jautrūs. Viešojo sektoriaus institucijos tvarko viešos tvarkos, priežiūros, pažeidžiamumo ir nusikaltimų įrašų duomenų bazes; jos saugo intelektinę nuosavybę, susijusią su pažangiausiais tyrimais; jos atstovauja valstybę ir vykdomas operacijas, tad sėkminga kibernetinė ataka prieš tai yra ir sėkminga ataka prieš visą valstybę. Visgi, viešojo sektoriaus organizacijos susiduria su unikaliu kibernetinio saugumo grėsmių deriniu, nes būdamos valstybiniais organais, jos yra patrauklūs taikiniai haktivistams ir valstybės remiamiems hakeriams iš užsienio, o turėdamos neskelbtinus duomenis, jos tampa pelningais taikiniais ir įprastų elektroninių nusikaltimų kontekste. Lietuvos Nacionalinis kibernetinio saugumo centras (toliau – NKSC) Kibernetinės saugumo būklės vertinimo ataskaitoje teigia, kad „įvertinęs kenkimo PĮ kibernetinių incidentų skaičių ypatingos svarbos paslaugas teikiančių kibernetinio saugumo subjektų RIS, NKSC nustatė iš viso 413 tokių kibernetinių incidentų (2018 m. buvo užfiksuota 470).” (2019, p. 26). Remiantis pastarąja ataskaita galima matyti, kad didžiausia kibernetinių grėsmių įtaka atsispindi Krašto apsaugos sektoriuje, valdančiame valstybės gynybos subsektorių (žr. pav. 1).

1 pav. Kibernetinio saugumo subjektų ir NKSC techninėmis kibernetinio saugumo stebėsenos priemonėmis surinkta informacija apie kenkimo PĮ pagal ypatingos svarbos paslaugų sektorius



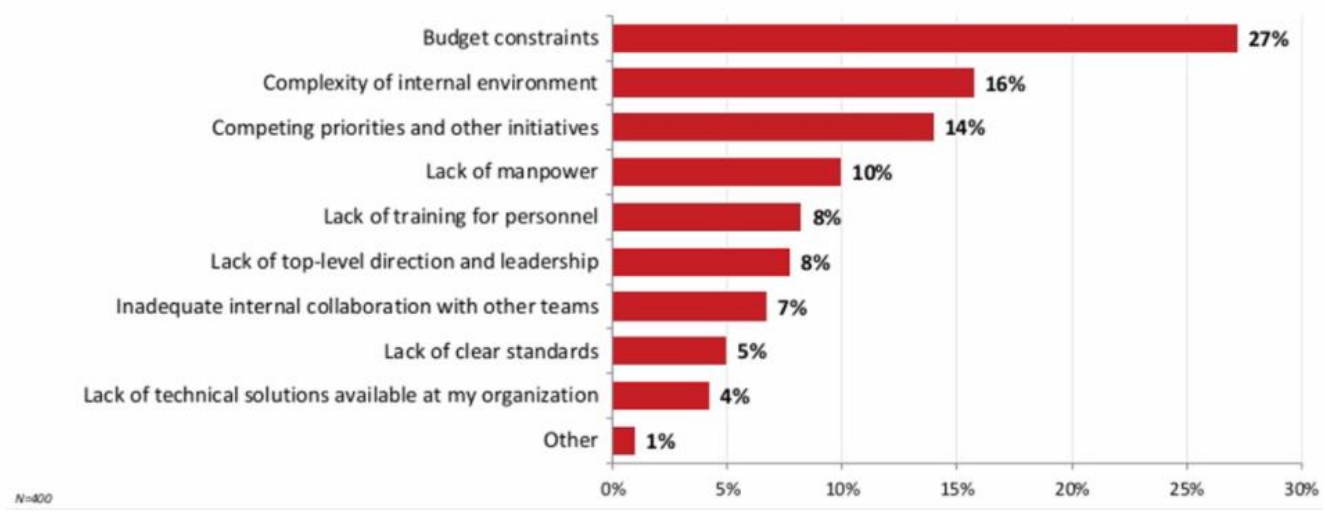
Šaltinis: Nacionalinio kibernetinio saugumo būklės ataskaita, 2019.

Atsižvelgiant į pateiktus duomenis galima teigti, kad kritinės informacinės infrastruktūros apsauga yra svarbi nacionalinio saugumo dalis ir reikalauja, kad politikos formuotojai ir jų patariamieji organai jos apsaugą spręstų nacionaliniu mastu. Pasak Harkins ir English (2018), kai vyriausybės kuria ir įgyvendina strategijas, skirtas apsaugoti savo IT turtą ir duomenis nuo kibernetinio saugumo grėsmių ir kitų nelaimių, jos taip pat turi sutelkti dėmesį į tai, kad šios paslaugos būtų atsparios. Atsparumas gali padėti užtikrinti ne tik valstybinių informacinių išteklių saugumą, bet ir sudaryti galimybę kurti išsamią ilgalaikę strategiją, kuri padėtų institucijoms eiti skaitmeninės transformacijos keliu. Be to, tai gali skatinti inovacijų kultūrą, sukurti naujų galimybių investuoti ir prisidėti prie gyvybingos ir ekonomiškai konkurencingos valstybės paveikslo. Gerai žinoma praktika, kurią taiko dauguma Vakarų Europos šalių – sukurtos visapusiškos YSII apsaugojimo organizacijos ir sistemos, įtraukiančios valstybines institucijas iš įvairių ministerijų generuoti į dabartį ir į ateitį orientuotas kibernetinio saugumo kultūros formavimo iniciatyvas. Pastarosios sistemos padeda sukurti tvirtos, veiksmingos nacionalinės kibernetinio saugumo politikos pagrindą ir atvaizduoja aukšto lygio strateginį kibernetinio saugumo rizikos gyvavimo ciklo paveikslą, kas skatina institucijas geriau suprasti savas kibernetinio saugumo rizikas ir suteikia joms galimybę taikyti rizikos valdymo principus bei geriausią praktiką, pagerinti YSI ir paslaugų saugumą bei atsparumą (ten pat).

Visų antra, biudžeto suvaržymai yra dažnas fenomenas viešojo sektoriaus institucijose. Dažnu atveju galima teigti, kad IT vadovams tenka kibernetinio saugumo įgyvendinimo užduotis atlikti su nepakankamais resursais. Tad dėl lėšų trūkumo norint apsaugoti kritinę informacinę infrastruktūrą ar ryšių ir informacines sistemas, apdorojančias įslaptintą informaciją, pagrindinės duomenų saugumo priemonės yra neintegruojamos. Ryškiausias to pavyzdys yra „WannaCry“ ataka, kuri suluošino

Jungtinės Karalystės „Nacionalinės sveikatos tarnybos“ informacines sistemas ir sugebėjo išplisti dėl ne gebėjimo ištaisyti jau žinomo pažeidžiamumo (Palmer, 2018). Taip pat svarbu paminėti, kad daugelis organizacijų kibernetinį saugumą laiko nereikalingomis išlaidomis, o investicijų grąžą traktuoja kaip minimalią ir nenešančią pridėtinės vertės kasdienės veiklos organizavime. Tai yra dažnas ir klaidingas požiūris, ypač viešojo sektoriaus institucijose, siekiančiose sumažinti išlaidas ir jas dedikuoti prioritetiniams tikslams, tiesiogiai susijusiems su institucijos funkcinėmis sritimis, tarp kurių dažniausiai kibernetinio saugumo nėra. Yra teigiama, kad „kai institucijos yra priverstos įrodyti investicijų grąžą, kad būtų užtikrintas finansavimas, jų vadovai pradeda ieškoti pelningų įmonių, o ne prevencinių technologijų ir mokymo.“ (Sanders, 2019). Remiantis „SolarWinds“ atliktu tyrimu („What is plaguing public sector cyber readiness?“, 2020), kuriame dalyvavo 400 IT operacijų ir saugumo sprendimus priimančių asmenų, įskaitant 200 federalinių, 100 valstijų ir vietos bei 100 švietimo respondentų, pagrindinė kliūtis viešojo sektoriaus institucijoms įgyvendinant kibernetinį saugumą yra nepakankamas biudžetas (žr. pav. 2).

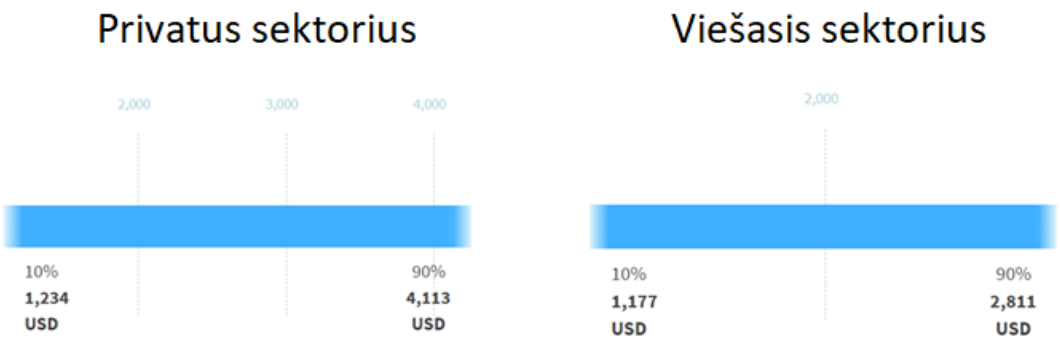
2 pav. Kibernetinio saugumo įgyvendinimo kliūtys viešajame sektoriuje



Šaltinis: Help Net Security, 2020.

Kitas labai svarbus aspektas, kurį lemia biudžeto suvaržymai yra IT saugos personalo nekonkurencingas darbo užmokestis valstybiniame sektoriuje lyginant su privačiu sektoriumi. Remiantis statistiniais duomenimis, viešajame sektoriuje IT saugos specialisto darbo užmokesčio rėžiai ir per pus mažesni nei privačiajame sektoriuje, t. y. vidutinis darbo užmokestis viešajame sektoriuje siekia 1 500 $ per mėnesį, tuo tarpu privačiame – 3 000 $ (žr. pav. 3). Todėl galima teigti, kad darbo užmokesčio skirtumai ne tik signalizuoja apie nežymų karjeros kylimo procesą valstybės tarnautojo pozicijoje, bet ir iš anksto gali padaryti įtaką jo motyvacijai bei savanoriškam tobulėjimui.

3 pav. IT saugos specialisto darbo užmokestis privačiame ir viešajame sektoriuje



Šaltinis: sudaryta autorės, remiantis www.paylab.com duomenimis.

Šis žymus darbo užmokesčio skirtumo faktorius lemia ne tik personalo trūkumą kibernetinių atakų atgrasymo kontekste, bet ir jau esamo personalo žinių bei kvalifikacijos trūkumą. Harkins ir English (2018) teigia, kad tik aštuoniolika valstybių šiandien reikalauja kibernetinio saugumo mokymų visiems savo darbuotojams. Pasak jų, norint mažinti kibernetinio saugumo rizikas viešajame sektoriuje, būtina plėtoti nusimanančią, kibernetinį raštingumą turinčią darbo jėgą. Vyriausybės ir viešojo sektoriaus organizacijos supranta, kad užpuolimas prieš vieną valdžios sektorių natūraliai paveiks ir kitą valdymo sritį. Ministerijos, kurios turi pavaldžias savo sektoriaus institucijas, turi palankų bendradarbiavimo mechanizmą skleisti kolektyvines kibernetinio saugumo žinias (Yeager, 2020). Pavyzdžiui, Energetikos ministerijos siunčiamas pranešimas apie kibernetinio saugumo situacijos vertinimą valdomame sektoriuje į elektros tiekimo agentūrą. Todėl galima teigti, kad norint sukurti kibernetinio saugumo kultūrą ir sumažinti kibernetinių atakų keliamą riziką, valstybė turėtų įgyvendinti efektyvią institucijų bendradarbiavimo metodologiją ir patikimą kibernetinio saugumo mokymo programą visoms valstybinius informacinius išteklius ir YSI infrastruktūrą valdančioms institucijoms, skiriant biudžetą proporcingą valdomų ar tvarkomų valstybės informacinių išteklių kibernetinėms rizikoms nacionalinio saugumo kontekste. Taip pat yra svarbu ir kolektyvinės žinios.

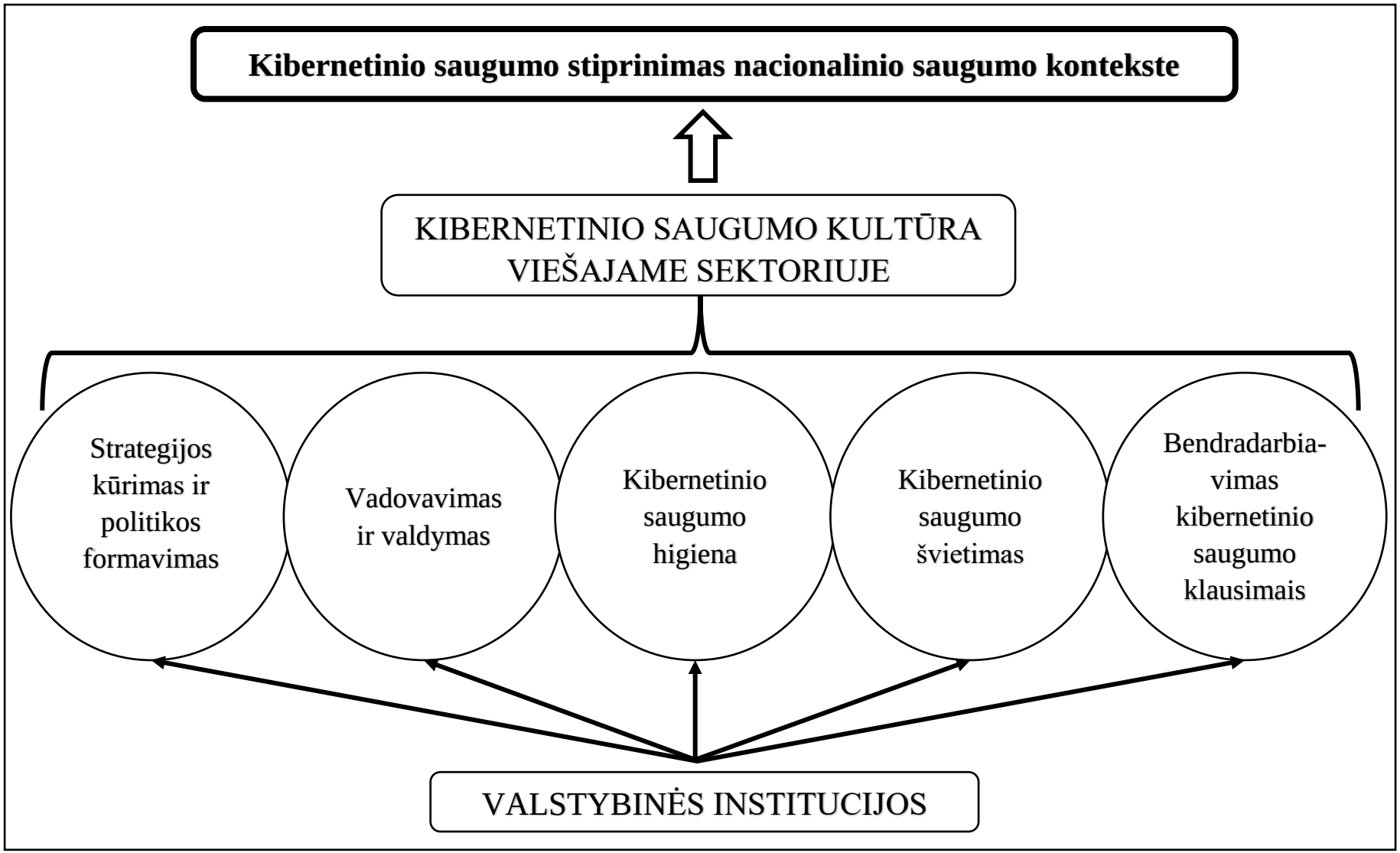
Galiausiai, kitas labai svarbus faktorius, lemiantis viešojo sektoriaus kibernetinio saugumo kultūros formavimo praktiką, yra valstybinių institucijų požiūris į naujas technologijas. Natūralu, kad politikos formuotojai nori rasti būdų, kaip apsaugoti YSII ir kitas valstybines sistemas bei išvengti naujų kibernetinių atakų vektorių. Tačiau vienu iš pagrindinių iššūkių tampa kritinių paslaugų teikimas ir perėjimas į naujus technologinius sprendimus. Visuomenėje vykstant skaitmeninei transformacijai, kuomet kaupiama ženkliai daugiau duomenų, daugiau aplikacijų veikia iš debesies ir vis daugiau darbuotojų savo darbą nori atlikti virtualiai, viešojo sektoriaus tinklai turi progresuoti technologiškai bent 15–25% per metus (Sanders, 2019). Tuo tarpu techninė įranga to technologinio progreso nėra pajėgi patempti. Galiausiai, tai tampa problema, nes viešasis sektorius istoriškai nėra pasirengęs arba ne visada

pasikliauja naujomis technologijomis, ypač programine įranga, turinčia išėjimą į atvirą internetą, ir yra linkę savo visus administruojamus duomenis užrakinti, taip apribodami tinklo plėtrą ir patikrintų saugumo sprendimų diegimą. Galima teigti, kad siekdama įveikti šiuos technologinius iššūkius, valstybinės institucijos turi mąstyti visapusiškai ir priimti išsamias, rizika pagrįstas kibernetinio saugumo strategijas, kaskart jas atnaujinant pagal visuomenėje diegiamą geriausią patirtį su tikslu prisitaikyti prie kintančių kibernetinių grėsmių profilių.

Viešojo sektoriaus kibernetinio saugumo kultūros formavimas yra neatsiejama priemonė norint užtikrinti kibernetinį saugumą nacionaliniame kontekste. Todėl vienu iš pagrindinių tikslų valstybei tampa valstybinių išteklių, YSI objektų ir YSII apsaugojimas bei kibernetinio atsparumo didinimas. Žvelgiant į kibernetinių grėsmių tendencijas, viešasis sektorius tampa vis dažnesniu kibernetinių atakų taikiniu. Pagrindinės to priežastys yra žinojimas fakto, jog valstybinės institucijos ir jų valdomos informacinės sistemos talpina labiausiai visuomenės pažeidžiamus duomenis; yra nuolatos varžomos biudžeto, kas lydi prastų kibernetinio saugumo sprendimų diegimą; stygsta profesionalaus IT saugos personalo dėl nekonkurencingų atlyginimų ir ribotų galimybių kelti kvalifikaciją.

Apibendrinant skyrių galima teigti, kad kibernetinio saugumo kultūra yra žinių, įsitikinimų, darbuotojų suvokimo, bei organizacijoje taikomų normų ir vertybių apie kibernetinį saugumą visuma, kuri atsiskleidžia ir pasireiškia žmonių elgesiu elektroninėje erdvėje. Kibernetinio saugumo kultūros formavimo tendencijas organizacijoje atspindi šie pagrindiniai teoriniai aspektai: strategijos kūrimas ir politikos formavimas, vadovavimas ir valdymas, kibernetinio saugumo higiena, kibernetinio saugumo švietimas, bendradarbiavimas kibernetinio saugumo klausimais (žr. pav. 3). Nors kibernetinis saugumas ir jo įgyvendinimas, remiantis pasauline patirtimi, yra vienodas visose organizacijose, tačiau vertinant kibernetinio saugumo kultūrą skirtingų valstybės sektorių organizacijose, būtina įvertinti jos formavimo ypatumus lemiančius priežastinius ryšius ir aplinkybes. Šiuo atveju viešajame sektoriuje – reikšmės valstybės nacionaliniam saugumui, politinės įtakos, kaštų, teisinio reglamentavimo bei taikomų organizacinių ir techninių priemonių reikalavimų.

4 pav. Kibernetinio saugumo kultūros formavimo viešajame sektoriuje teorinis modelis



Šaltinis: sudaryta autorės.

2. KIBERNETINIO SAUGUMO KULTŪROS FORMAVIMO VIEŠAJAME SEKTORIUJE TYRIMO METODOLOGIJA

2.1 Empirinio tyrimo metodologija

Vertinant nagrinėjamos mokslinės problemos specifiką ir naujumą, problemai analizuoti buvo pasirinktas kokybinio tipo tyrimas. Kokybinis tyrimas – tai toks tyrimas, kuris sociologijos, filosofijos, logikos ir individualaus stebėjimo priemonių pagalba padeda suprasti tam tikrą žmonių elgesį ir tokio elgesio priežastis (Tidikis, 2003). Tiriant darbe iškeltą mokslinę problemą, tyrimo metu rezultatų reprezentatyvumui yra labai svarbu surinkti ne kuo didesnę skirtingų nuomonių kiekybinę aibę, bet pateikti gilesnę ir platesnę informaciją, remiantis kokybišku ekspertiniu vertinimu. ,,Kokybinė surinktos informacijos analizė grindžiama teorijų sklaida, individualia patirtimi, gebėjimu įsigilinti į gausius surinktos informacijos srautus, tirti esminius momentus bei tinkamai visą medžiagą interpretuoti.“ (Valackienė ir Mikėnė, 2008, p. 34).

Tyrimo tikslas – empiriškai įvertinti Lietuvos viešojo sektoriaus kibernetinio saugumo kultūros formavimo ypatumus.

Tyrimo hipotezė – kibernetinio saugumo kultūros formavimo neefektyvumą Lietuvos viešajame sektoriuje lemia vadybos stoka.

Tyrimo uždaviniai:

1. Atlikti kibernetinį saugumą ir jo kultūros formavimą Lietuvos viešajame sektoriuje reglamentuojančių dokumentų turinio (angl. Content) analizę;
2. Atskleisti kibernetinio saugumo kultūros įgyvendinimo procesus ir problemas Lietuvos valstybinėse institucijose;
3. Identifikuoti esminius iššūkius formuojant kibernetinio saugumo kultūrą Lietuvos viešajame sektoriuje, remiantis ekspertiniu interviu.
4. Atlikti gautų tyrimo rezultatų interpretaciją, pateikiant siūlymus ir rekomendacijas identifikuotoms problemoms spręsti.

Tyrime naudojami duomenų rinkimo metodai:

1. Mokslinės literatūros ir dokumentų turinio (angl. Content) analizė;
2. Ekspertinė apklausa;
3. Neformalus struktūrizuotas interviu.

Tyrimo atranka. Kokybinio tyrimo imties sudarymui pasirinkta tikslinė kriterinė atranka. Tai yra strategija, pagal kurią tam tikros aplinkos, asmenys ar įvykiai atrenkami apgalvotai, pagal iš anksto nustatytus kriterijus, norint gauti svarbią informaciją, kuri negali būti prieinama kitokiu būdu. Būdas

veiksmingas, nes padeda surinkti kokybiškų duomenų. Tyrimui atrenkami visi, žemiau paminėtus tris kriterijus atitinkantys atvejai.

Atrankos kriterijai:

1. Vietos – atstovaujama institucija yra valstybinė, formuojanti valstybės politiką pavestose valdymo srityse;
2. Lauko – atstovaują instituciją, kuri valdo ir tvarko valstybės informacinius išteklius ar YSII;
3. Atvejo viduje – užimamos pareigos tiesiogiai susijusios su kibernetiniu saugumu.

Tyrimo reprezentatyvumas. Atrankos reprezentatyvumas reiškia, kad joje proporcingai atstovaujama stebėjimo vienetų grupėms, kurių ypatybės gali daryti įtaką tiriamiesiems požymiams. Tyrimui atliki ekspertai buvo parinkti remiantis ekspertų darbo vieta, kasdiene veikla ir funkcine sritimi, nes pasak Rupšienės (2007), kokybiniame tyrime neverta siekti tikimybinės, atsitiktinai sudarytos imties, bet priešingai – reikia pasirinkti tokius atvejus, kurie informatyvūs tiriamuoju požiūriu. Pagal tyrime nustatytus kriterijus, ekspertinio vertinimo atstovai tapo LR ministerijų, valdančių ir tvarkančių valstybės informacinius išteklius / atsakingų už savo sektoriaus YSI objektų ir YSII identifikavimą atstovai, kurių pareigos yra tiesiogiai susijusios su kibernetiniu saugumu, jo politikos formavimu ar praktiniu įgyvendinimu. LR ministerijų sąrašas:

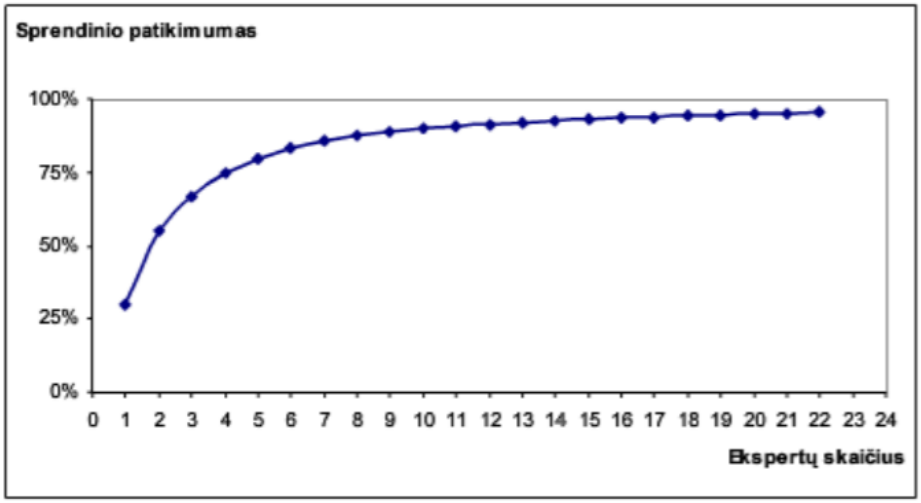
1. Krašto apsaugos ministerija (toliau – KAM);
2. Vidaus reikalų ministerija (toliau – VRM);
3. Užsienio reikalų ministerija (toliau – URM);
4. Ekonomikos ir inovacijų ministerija (toliau – EIMIN);
5. Energetikos ministerija (toliau – ENMIN);
6. Aplinkos ministerija (toliau – AM);
7. Sveikatos apsaugos ministerija (toliau – SAM);
8. Kultūros ministerija (toliau – KM);
9. Švietimo, mokslo ir sporto ministerija (toliau – ŠMSM);
10. Socialinės apsaugos ir darbo ministerija (toliau – SOCMIN);
11. Žemės ūkio ministerija (toliau – ŽŪM);
12. Teisingumo ministerija (toliau – TM);
13. Finansų ministerija (toliau – FINMIN);
14. Susisiekimo ministerija (toliau – SUMIN).

Siekiant identifikuoti priežastinius ryšius ir iššūkius viešajame sektoriuje, formuojant ir įgyvendinant kibernetinio saugumo kultūrą, ekspertiniam interviu atlikti buvo parinktas Nacionalinio kibernetinio saugumo centro (toliau – NKSC), kaip pagrindinės kibernetinį saugumą reguliuojančios bei

už ypatingos svarbos informacinės infrastruktūros kibernetinį saugumą ir informacinių išteklių akreditaciją atsakingos institucijos atstovas.

Anot Valackienės ir Mikėnės (2008), naudojant interviu metodą galima atrinkti respondentų sąrašą, į kurį patenka žmonės, kurie yra vieninteliai galimi informacijos šaltiniai, kadangi jie yra šios sferos ekspertai arba įvykių liudininkai. Sudarant ekspertų grupę daugelio mokslininkų nuomone, optimalus grupės dydis yra 8-10 ekspertų. Yra įrodyta, kad nedidelės ekspertų grupės sprendimų ir vertinimų tikslumas nenusileidžia didelės ekspertų grupės sprendimų ir vertinimų tikslumui. Todėl didinant ekspertų imtį tyrimo tikslumas didėja (žr. pav. 4).

5 pav. Ekspertų skaičiaus įtaka vertinimo patikimumui



Šaltinis: Augustinaitis, 2009.

Tyrimo apribojimai: kibernetinio saugumo kultūra yra ganėtinai nauja tyrimo sritis Lietuvoje, o ypač viešajame sektoriuje. Dėl egzistuojančios kibernetinio saugumo kultūros požymių apimties, tikėtina, kad dalies LR ministerijose parinktų ekspertų žinios gali būti ribotos.

2.2. Empirinio tyrimo organizavimas ir loginė eiga

Empirinio kokybinio tyrimo loginę schemą sudaro trys sąveikaujantys etapai:

1 etape buvo išsamiai analizuojama mokslinė literatūra ir ankstesni tyrimai, atskleidžiantys kibernetinio saugumo kultūros teorinį pagrindą, jos formavimo poreikį ir problemas, su kuriomis susiduriama tai įgyvendinant organizacijoje. Metodas – mokslinės literatūros turinio analizė. Šiame etape taip pat buvo išskiriami esminiai tyrimo objekto kriterijai bei indikatoriai, kurie yra reikalingi kibernetinio saugumo kultūros formavimo ir įgyvendinimo sėkmingoje praktikoje, konkrečiai viešajame sektoriuje. Pirmam etapui atlikti buvo pasirinktas mokslinės literatūros analizės metodas.

2 etape visų pirma, taikant kokybinio tyrimo dokumentų analizės metodą, bus nagrinėjami Lietuvos valstybinėms institucijoms taikomi ir kibernetinį saugumą reglamentuojantys norminiai

dokumentai. Analizės tikslas: išsiaiškinti kibernetinio saugumo kultūros formavimo ir įgyvendinimo reglamentavimą LR viešajame sektoriuje. Vėliau šiame etape, naudojant turinio analizės metodą, bus nagrinėjamos kibernetinio saugumo pratybų ataskaitos, veiklos planai, su kibernetinio saugumo plėtra susiję dokumentai. Analizės tikslas: atskleisti praktinį kibernetinio saugumo kultūros formavimo procesą valstybinėse institucijose. Taip pat bus atliekamas ekspertinis vertinimas, pasitelkiant apklausos anketavimo būdu metodą: apklausiamos 14 Lietuvos Respublikos ministerijų, kurios valdo ir tvarko valstybės informacinius išteklius ar YSII, o taip pat, remiantis LR nutarimu „Dėl ypatingos svarbos informacinės infrastruktūros identifikavimo metodikos patvirtinimu (2018 m. gruodžio 5 d. Nr. 1209), yra atsakingos už ypatingos svarbos infrastruktūros objektų ir ypatingos svarbos informacinės infrastruktūros savo funkcinėse srityse identifikavimą. Apklausos tikslas – nustatyti, kokie veiksniai, pasak LR ministerijų kibernetinio saugumo ekspertų, daro įtaką šių valstybinių institucijų kibernetinio saugumo kultūros formavimui. Ekspertams elektroniniu paštu bus pateikta 10 klausimų (8 uždari ir 2 atviri), iš kurių 7 klausimai buvo skirti kibernetinio saugumo kultūros formavimo požymių atskleidimui ir 3 klausimai probleminių sričių identifikavimui (žr. 2 lentelę). Metodas buvo pasirinktas, kadangi darbuotojai, kurių pareigos yra tiesiogiai susijusios su kibernetiniu saugumu, yra vienas iš pagrindinių kibernetinio saugumo kultūros įgyvendinimo subjektų, kurie tiesiogiai koreliuoja su tyrime išsikeltų tikslų pasiekimu. Apklausa sudaryta remiantis bendraisiais etikos reikalavimais: motyvuotai paaiškinama, kodėl atliekamas tyrimas; pateikti klausimai yra konkretūs, todėl respondento pastangos atsakyti yra minimalios; respondentui nereikia daug rašyti, kas, tikėtina, prideda anonimiškumo; anketa yra trumpa ir apipavidalinta taip, kad neatbaidyti respondento; apklausoje nėra klausimų, kurie stumtų respondentą į vieną atsakymą. (Valackienė ir Mikėnė, 2008, p. 100). Apklausos forma pateikta 2 priede.

2 lentelė. Ekspertinio vertinimo apklausos klausimų sudarymo instrumentarijus

KIBERNETINIO SAUGUMO KULTŪROS FORMAVIMO YPATUMŲ ATSKLEIDIMAS			
Eil. Nr.	**Kibernetinio saugumo kultūros požymis**	**Klausimas**	**Tikslas**
1.	Strategijos kūrimas ir politikos formavimas	Jūsų atstovaujama institucija (galimi keli atsakymų variantai): a) Įgyvendina kibernetinio saugumo priemones, kurios viešajam sektoriui yra reglamentuotos LR teisės aktuose; b) Turi patvirtintą institucijos kibernetinio saugumo strategiją / politiką; c) Turi patvirtintas standartinės veiklos procedūras, susijusias su	Nustatyti, ar ir kokiu būdu institucija yra reglamentavusi kibernetinio saugumo įgyvendinimą.

		kibernetinio saugumo įgyvendinimu organizacijoje; d) Visi punktai aukščiau.	
2.	Kibernetinio saugumo higiena	Jūsų nuomone, ar atstovaujamoje institucijoje yra tinkamai palaikoma kibernetinio saugumo higiena? a) Taip; b) Iš dalies; c) Ne.	Nustatyti, ar organizacinių ir techninių kibernetinio saugumo reikalavimų kibernetinio saugumo subjektams aprašas yra efektyviai pritaikytas institucijos kibernetinio saugumo higienos palaikymo kontekste.
3.	Kibernetinio saugumo švietimas	Ar jūsų institucijoje yra organizuojami kibernetinio saugumo mokymai darbuotojams? a) Taip; b) Ne.	Išsiaiškinti, ar institucijoje vykdomas kibernetinio saugumo švietimas.
4.		Ar jūsų institucijoje yra sudarytos sąlygos kelti personalo, kurio funkcijos tiesiogiai susijusios su kibernetiniu saugumu, kvalifikaciją? a) Taip; b) Ne.	Nustatyti, ar institucijoje yra vykdomas RIS ir saugos personalo kvalifikacijos kėlimas ir žinių vertinimas.
5.		Kaip dažnai jūsų institucija dalyvauja NKSC organizuojamose kibernetinio saugumo pratybose? a) Dalyvauja visose pratybose, į kurias yra kviečiama; b) Dalyvauja tik kai kuriose pratybose; c) Nedalyvauja.	Atskleisti, ar institucija dalyvauja kibernetinio saugumo pratybose, organizuojamose NKSC.
6.	Bendradarbiavimas kibernetinio saugumo klausimais	Kokias jūsų atstovaujamos institucijos bendradarbiavimo formas su kitomis institucijomis (tiek viešojo, tiek	Nustatyti, ar ir kokiais būdais vykdomas bendradarbiavimas

		privataus sektoriaus) kibernetinio saugumo klausimais galite įvardinti? a) Nacionaliniu lygmeniu – b) Tarptautiniu lygmeniu –	kibernetinio saugumo klausimais.
7.	Vadovavimas ir valdymas	Jūsų nuomone, ar visų lygmenų vadovai yra įsitraukę į kibernetinio saugumo kultūros formavimą jūsų atstovaujamoje institucijoje? Jei taip, kokiais būdais?	Atskleisti institucijos visų lygmenų vadovų indėlį kibernetinio saugumo kultūros formavimo kontekste.
KIBERNETINIO SAUGUMO KULTŪROS FORMAVIMO IŠŠŪKIŲ IR PROBLEMINIŲ SRIČIŲ IDENTIFIKAVIMAS			
Eil. Nr.	**Klausimas**		**Tikslas**
8.	Kaip manote, kas paskatintų darbuotojo, kurio tiesioginės funkcijos nėra susijusios su kibernetiniu saugumu, įsitraukimą į organizacijos kibernetinio saugumo kultūros formavimą? Galimi keli atsakymų variantai. a) Vadovų motyvacija ir lyderystė šiuo klausimu; b) Mokymai skaitmeninei brandai didinti; c) Aiškiai organizacijos politikoje apibrėžta privalomoji kibernetinė higiena ir elgesio elektroninėje erdvėje taisyklės; d) Sankcijos dėl kibernetinio saugumo priemonių netaikymo; e) Kita (įvardinkite):		Nustatyti faktorius, skatinančius darbuotojų įsitraukimą į kibernetinio saugumo kultūros formavimą.
9.	Jūsų nuomone, kokios priežastys lemia žemą valstybinių institucijų dalyvavimo NKSC organizuojamose pratybose statistinį rodiklį? Galimi keli atsakymo variantai. a) Personalo stoka; b) Kvalifikacijos ir žinių stoka; c) Vadybos ir motyvacijos stoka; d) Institucijos užimtumas; e) Kita (įvardinkite):		Nustatyti, dėl kokių priežasčių viešojo sektoriaus institucijos pasyviai dalyvauja NKSC organizuojamose pratybose.
10.	Jūsų nuomone, kokie yra pagrindiniai iššūkiai Lietuvos viešojo sektoriaus institucijoms, įgyvendinant kibernetinio saugumo kultūrą?		Išsiaiškinti, kokie yra pagrindiniai iššūkiai formuojant kibernetinio saugumo kultūrą viešajame sektoriuje.

Analizuojant valstybės institucijų ekspertų apklausos rezultatus bus pasitelktas turinio analizės metodas, kuris bus atliekamas trimis etapais:

1) Analizės vienetų išskyrimas – vertinami ekspertų atsakymai pagal raktinius žodžius;
2) Jų indikatorių suradimas tekste – identifikuojami pagrindiniai ;
3) Statistinis apdorojimas – atliekamas atsakymų palyginimas ir statistinis atsakymų pasirinkimo vertinimas.

Toliau antrajame tyrimo etape bus organizuojamas neformalus struktūrizuotas interviu su Nacionalinio kibernetinio saugumo centro (toliau – NKSC) atstovu, siekiant išsiaiškinti kokių veiksmų jau yra imtasi kibernetinio saugumo kultūros formavime ir su kokiomis jo manymu problemomis susiduria valstybinės institucijos, formuodamos kibernetinio saugumo kultūrą. Svarbu pabrėžti ir tai, kad tyrimą atliekantis autorius yra taip pat viešojo sektoriaus institucijos darbuotojas, kurio pareigos yra tiesiogiai susijusios su kibernetiniu saugumu Krašto apsaugos sistemoje. Anot Rupšienės (2007), „interviu metu tyrimo dalyviai visada geriau jaučiasi, jei priklauso tam pačiam socialiniam sluoksniui ir turi tam tikrų panašumų. Tai padeda tyrėjui gauti kokybiškesnių duomenų.” (p. 29). Ekspertiniam interviu parinkta 11 atvirų klausimų, kurie papildo ir sustiprina kokybinio tyrimo rezultatų validumą (žr. 3 lentelę). Interviu protokolas pateiktas 1 priede.

3 lentelė. Ekspertinio interviu klausimų sudarymo instrumentarijus

Eil. Nr.	Klausimas	Tikslas
1.	Vadovaujantis LR teisės aktais, kibernetinio saugumo subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojai suderinę su Nacionaliniu kibernetinio saugumo centru, tvirtina kibernetinio saugumo politikos ir jos įgyvendinimo dokumentus. Kaip manote, ar visi institucijos darbuotojai turėtų būti skatinami dalyvauti rengiant kibernetinio saugumo politiką, siekiant efektyvaus politikos įgyvendinimo praktikoje ar visgi tik tie darbuotojai, kurių funkcijos yra tiesiogiai susijusios su kibernetiniu saugumu? Savo atsakymą pagrįskite.	Patvirtinti arba paneigti darbuotojų, kurių pareigos nėra tiesiogiai susijusios su kibernetiniu saugumu įsitraukimo poreikį, rengiant institucijos kibernetinio saugumo politikos ir jos įgyvendinimo dokumentus.
2.	Jūsų nuomone, ar visų lygmenų vadovai turėtų įsitraukti į kibernetinio saugumo kultūros formavimą valstybinėse institucijose? Ar sutinkate, kad kibernetinis saugumas yra	Identifikuoti priežastis, dėl kurių kibernetinis saugumas ir jo įgyvendinimas nėra visų

	dažnai įvardijamas kaip IT departamento reikalas? Savo atsakymą pagrįskite.	lygmenų institucijos vadovų darbotvarkėje.
3.	Kaip vertinate valstybinių institucijų, valdančių ar tvarkančių valstybės informacinius išteklius ar YSII kibernetinio saugumo higienos lygį? Jūsų manymu, kokie pagrindiniai veiksniai jį lemią?	Įvertinti, ar organizacinių ir techninių kibernetinio saugumo reikalavimų kibernetinio saugumo subjektams aprašas yra efektyviai taikomas Lietuvos viešajame sektoriuje kibernetinio saugumo higienos palaikymo kontekste.
4.	Kaip manote ar visose valstybinėse institucijose, valdančiose ar tvarkančiose valstybės informacinius išteklius ar YSII, yra organizuojami kibernetinio saugumo mokymai? Ar galėtumėte įvardinti pagrindines (jums žinomas) tokių mokymų pateikimo formas, būdus Lietuvos viešajame sektoriuje? Jūsų vertinimu, ar jie yra efektyvūs?	Atskleisti vykdomų kibernetinio saugumo mokymų darbuotojams pagrindines taikytinas formas Lietuvos valstybinėse institucijose.
5.	Kaip manote, kas paskatintų darbuotojo, kurio tiesioginės funkcijos nėra susijusios su kibernetiniu saugumu, įsitraukimą į organizacijos kibernetinio saugumo kultūros formavimą?	Nustatyti faktorius, skatinančius darbuotojų įsitraukimą į kibernetinio saugumo kultūros formavimą.
6.	Kaip vertinate LR viešajam sektoriui skiriamą finansavimą kvalifikacijos kėlimui personalo, kurio funkcijos tiesiogiai susijusios su kibernetiniu saugumu? Ar sutinkate, kad skiriamas finansavimas nėra proporcingas valdomų ar tvarkomų valstybės informacinių išteklių kibernetinėms rizikoms nacionalinio saugumo kontekste?	Patvirtinti arba paneigti finansavimo didinimo kvalifikacijos kėlimui poreikį personalui, kurio funkcijos tiesiogiai susijusios su kibernetiniu saugumu.
7.	NKSC yra pagrindinė institucija Lietuvoje, organizuojanti kibernetinio saugumo pratybas. Kaip vertinate jų adaptaciją valstybinių institucijų poreikiams, vykdomai veiklai? Kaip manote, ar dabartinis pratybų skaičius per metus yra pakankamas formuoti kibernetinio saugumo kultūrą nacionaliniu lygmeniu?	Atskleisti, ar kibernetinio saugumo pratybų skaičius per metus yra pakankamas formuoti kibernetinio saugumo kultūrą ir ar pratybų scenarijus yra pritaikytas atsižvelgiant į valstybinių institucijų poreikius.

8.	Jūsų nuomone, kokios priežastys lemia žemą valstybinių institucijų dalyvavimo NKSC organizuojamose pratybose statistinį rodiklį?	Nustatyti, dėl kokių priežasčių viešojo sektoriaus institucijos pasyviai dalyvauja NKSC organizuojamose pratybose.
9.	Kokias LR viešojo sektoriaus bendradarbiavimo formas su kitomis organizacijomis (tiek viešojo, tiek privataus sektoriaus) galite įvardinti? 1) Nacionaliniu lygmeniu – 2) Tarptautiniu lygmeniu –	Nustatyti, ar ir kokiais būdais Lietuvos viešajame sektoriuje yra vykdomas bendradarbiavimas kibernetinio saugumo klausimais.
10.	Jūsų nuomone, kokie yra pagrindiniai iššūkiai Lietuvos viešojo sektoriaus institucijoms, įgyvendinant kibernetinio saugumo kultūrą?	Išsiaiškinti, kokie yra pagrindiniai iššūkiai formuojant kibernetinio saugumo kultūrą viešajame sektoriuje.
11.	Kaip manote, ar LR teisės aktuose kibernetinio saugumo priemonės yra pakankamos ir įpareigojančios visas viešojo sektoriaus institucijas jas integruoti, formuojant kibernetinio saugumo kultūrą? Jei ne, ką jūsų nuomonę reikėtų keisti, norint sukurti efektyvų kibernetinio saugumo kultūros įgyvendinimo modelį viešajame sektoriuje?	Identifikuoti poreikį reglamentuoti kibernetinio saugumo kultūros formavimo ir įgyvendinimo procesus Lietuvos viešajame sektoriuje.

3 etape atliekama kokybinio tyrimo gautų rezultatų interpretacija. Metodas – gautų duomenų turinio analizė. Šio etapo paskirtis – atlikti išnagrinėtų kibernetinio saugumo kultūrą reglamentuojančių dokumentų turinio, ekspertinio interviu turinio ir ekspertų, atstovaujančių LR ministerijas apklausos tyrimo rezultatų analizę su tikslu įvertinti kibernetinio saugumo kultūros formavimo ypatumus ir problemas. Gautų tyrimo rezultatų interpretacija bus pagrindas empiriškai patvirtinti autoriaus atliktos teorinės analizės rezultatus bei suformuluoti siūlymus identifikuotoms kibernetinio saugumo kultūros formavimo problemos Lietuvos viešajame sektoriuje spręsti.

3. KIBERNETINIO SAUGUMO KULTŪROS FORMAVIMO LIETUVOS VIEŠAJAME SEKTORIUJE EMPIRINIS TYRIMAS

3.1. Teisinis reglamentavimas

Vis daugiau valstybių įvardija, kad kibernetinis saugumas yra viena iš priemonių užtikrinti nacionalinį saugumą, o informacinės technologijos, telekomunikacijos ir jų apsauga yra valstybės strateginiai prioritetai. Todėl siekiant efektyviai įgyvendinti kibernetinį saugumą Lietuvos viešajame sektoriuje, kibernetinis saugumas yra reglamentuotas teisės aktuose. Toliau darbe bus analizuojami LR teisės aktai bei jų turinys, siekiant atskleisti kibernetinio saugumo kultūros formavimo priemonių reglamentavimą ir taikymą Lietuvos viešojo sektoriaus institucijoms.

Vienas iš Lietuvos teisės aktų, kuris iš esmės yra pagrindinis įstatyminis dokumentas dėl savo teisinės formos įpareigojantis Lietuvos kibernetinio saugumo subjektus jį taikyti įgyvendinant kibernetinį saugumą yra *2014 m. gruodžio 11 d. Lietuvos Respublikos Seimo (toliau – LRS)* išleistas *Nr. XII-142 „Lietuvos kibernetinio saugumo įstatymas”.* Remiantis juo, kibernetinis saugumas yra apibrėžiamas kaip „visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų kibernetiniams incidentams išvengti, aptikti, analizuoti ir reaguoti į juos, taip pat įprastinei elektroninių ryšių tinklų, informacinių sistemų ar pramoninių procesų valdymo sistemų veiklai, įvykus šiems incidentams, atkurti.” (p. 2).

Sekantis ne ką mažiau svarbus kibernetinį saugumą ir jo įgyvendinimą reglamentuojantis dokumentas yra *2018 m. rugpjūčio 13 d. Lietuvos Respublikos Vyriausybės (toliau – LRV) nutarimu Nr. 818* išleista *„Nacionalinė kibernetinio saugumo strategija”.* Tačiau pats dokumentas, kaip teisės aktas, yra tik rekomendacinio pobūdžio, kuriame yra pateiktos valstybės kibernetinio saugumo formavimo kryptys ir gairės. Tai reiškia, kad norint įgyvendinti Strategijos tikslus ir uždavinius, yra reikalingi atskiri, ją lydintys veiklos planai, įpareigojantys kibernetinio saugumo subjektus vykdyti tam tikras priemones. Todėl galima teigti, kad Strategija, kaip pats vienas dokumentas, negali įpareigoti vykdyti kibernetinio saugumo ar jo kultūros formavimo ir įgyvendinimo priemonių.

Toliau kalbant apie Lietuvos kibernetinį saugumą ir jo kultūros formavimą labiausiai atspindinčius aspektus, Lietuvos įstatyminėje bazėje galima rasti labai svarbų dokumentą, reglamentuojantį būtent technines ir organizacines priemones organizacijose, kurios yra traktuojamos kaip valstybės kibernetinio saugumo subjektai – *2018 m. gruodžio 5 d. LRV nutarimu Nr. 1209* patvirtintą *„Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašą”.* Šiame apraše viešajam sektoriui yra apibrėžti tokie kibernetinio saugumo kultūros formavimo aspektai, kaip organizacijos strategijos kūrimas ir politikos formavimas, kibernetinio saugumo higiena ir su ja susijusi veikla, pavyzdžiui, rizikų valdymas.

Apie aukščiau paminėtus kibernetinio saugumo kultūros formavimo aspektus, taip pat apie vadovavimą ir valdymą Lietuvos teisinėje sistemoje egzistuoja *2011 m. gruodžio 15 d. LRS išleistas Nr. XI-1807 „Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas“*, kurio tikslas yra užtikrinti tinkamą valstybės informacinių išteklių kūrimą, tvarkymą, valdymą, naudojimą, priežiūrą, sąveiką, planavimą, finansavimą ir saugą. „Šis įstatymas taikomas valstybės institucijoms, valstybės įstaigoms, valstybės įmonėms, viešosioms įstaigoms, steigiančioms, kuriančioms ir (arba) tvarkančioms valstybės registrus (kadastrus), žinybinius registrus, valstybės informacines sistemas ir kitas informacines sistemas, finansuojamoms iš valstybės biudžeto, Valstybinio socialinio draudimo fondo biudžeto, Privalomojo sveikatos draudimo fondo biudžeto ir kitų valstybės pinigų fondų ir Lietuvos Respublikos viešojo administravimo įstatymo nustatyta tvarka įgaliotoms atlikti viešąjį administravimą.“ (p. 1). Taip pat šio įstatymo pagrindu yra suformuojamas kolegialus patariamasis organas, Valstybės informacinių išteklių valdymo taryba, kurios pagrindinė darbo specifika – teikti siūlymus ir rekomendacijas Vyriausybei valstybės informacinių išteklių valdymo ir plėtros klausimais. Taip pat labai svarbus dokumentas, kurio metodika yra identifikuojami valstybės YSI objektai ir YSII yra *2018 m. gruodžio 5 d. LRV nutarimu Nr. 1209* patvirtinta *„Ypatingos svarbos informacinės infrastruktūros identifikavimo metodika“*. Ši metodika ir ją taikyti įpareigotos institucijos, konkrečiai LR ministerijos, yra vienas esminių Lietuvos žingsnių, siekiant apsaugoti valstybės kritinės svarbos sektorius ir subsektorius, jų kibernetinę erdvę bei formuoti YSI objektų ir YSII kibernetinio saugumo politiką, reglamentuoti jiems aiškiais technines ir organizacines priemones su tikslu stiprinti valstybės nacionalinį saugumą.

Kalbant apie dar vieną labai svarbų aspektą, formuojantį kibernetinio saugumo kultūrą nacionaliniame kontekste, vienas pirmųjų Nacionalinės kibernetinio saugumo strategijos praktinio įgyvendinimo žingsnių, siekiant bendrų kibernetinio saugumo tikslų – *2019 m. liepos 3 d. LRV nutarimu Nr. 709 patvirtintas „Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinis veiklos planas“.* Šiame plane bendradarbiavimas kibernetinio saugumo klausimais yra išreikštas ne tik gerųjų praktikų perėmimu ir patirties dalijimusi tarp Lietuvos organizacijų, bet ir kibernetinio švietimo skatinimo, organizavimo ir praktikavimo aspektu. Planas svarbus tuo, kad įpareigoja konkrečias institucijas konkrečiose sferose įgyvendinti kibernetinio saugumo kultūros palaikymo priemones, skatina viešojo sektoriaus atskaitomybę ir generuoja tarpusavio supratimą nacionalinio kibernetinio saugumo kontekste.

Galiausiai, *2018 m. gruodžio 5 d. LRV nutarimu Nr. 1209 yra parengtas ir išleistas „Nacionalinis kibernetinių incidentų valdymo planas“,* kuris reglamentuoja ne tik tarpinstitucinio bendradarbiavimo aspektus kibernetinių incidentų valdymo metu, bet ir nustato pagrindines kibernetinių incidentų valdymo procedūras kibernetinio saugumo subjektams.

Kaip galima pastebėti iš atliktos Lietuvos teisinės bazės, reglamentuojančios Lietuvos kibernetinį saugumą ir jo įgyvendinimo formas bei metodus, analizės, visi kibernetinio saugumo kultūros formavimo teoriniai aspektai, išskirti nagrinėjant mokslinę literatūrą ir ekspertų įžvalgas, yra pastaruosiuose LR dokumentuose paminėti, o dalis ir aiškiai bei detaliai išrašyti. Tačiau, išsiaiškinti, ar visi jie yra įpareigojantys valstybines institucijas juos taikyti formuojant kibernetinio saugumo kultūrą, o gal kaip tik paliekantys veikimo laisvę priimti individualius sprendimus institucijų viduje, reikalinga būtent šių dokumentų išsamesnė turinio analizė, kuri toliau bus atvaizduojama valstybinių institucijų įpareigojimų taikant kibernetinio saugumo kultūros priemones principu (žr. 4 lentelę).

4 lentelė. Lietuvos viešojo sektoriaus institucijų pareigos Lietuvos kibernetinio saugumo įstatyminiame kontekste

Kibernetinio saugumo kultūros formavimo aspektas	Formuluotė dokumente
Strategijos kūrimas ir politikos formavimas	1. 2018 m. gruodžio 5 d. LRV nutarimo Nr. 1209 „Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo" III skyriaus 5 punktas: „*Subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojai <...> tvirtina kibernetinio saugumo politikos ir jos įgyvendinimo dokumentus, <...>."* (p. 3). 8 punktas: *„Kibernetinio saugumo politikos ir jos įgyvendinimo dokumentai turi būti peržiūrimi (persvarstomi) ne rečiau kaip kartą per metus <...>."* (p. 4). 9 punktas: *„Ne rečiau kaip kartą per metus turi būti organizuojamas ir atliekamas valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros atitikties Reikalavimams vertinimas."* (p. 4).
Vadovavimas ir valdymas	1. 2011 m. gruodžio 15 d. LRS Nr. XI-1807 „Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo" III skyriaus 7 straipsnis: *„Valstybės informacinių išteklių valdymo taryba yra kolegialus patariamasis organas, ją sudaro valstybės informacinių išteklių politiką formuojančių institucijų, <...> ir kiti atstovai, kompetentingi informacinių ir ryšių technologijų srityje."* (p. 7). ***4 lentelės tęsinys kitame puslapyje***

	2. 2014 m. gruodžio 11 d. LRS Nr. XII-1428 ,,Lietuvos kibernetinio saugumo įstatymo" II skyriaus 9 straipsnis: ,,*Kibernetinio saugumo taryba yra nuolatinė kolegiali institucija, analizuojanti kibernetinio saugumo užtikrinimo būklę Lietuvos Respublikoje ir teikianti pasiūlymus kibernetinio saugumo dalyviams dėl šios būklės gerinimo.*" (p. 5).
Kibernetinio saugumo švietimas	1. 2018 m. rugpjūčio 13 d. LRV nutarimo Nr. 818 ,,Nacionalinės kibernetinio saugumo strategijos" Trečiasis skirsnis: *,,Trečiasis Strategijos tikslas – skatinti kibernetinio saugumo kultūrą ir inovacijų plėtrą. Pirmasis trečiojo tikslo uždavinys – plėtoti mokslinius tyrimus ir didelę pridėtinę vertę kuriančias veiklas kibernetinio saugumo srityje <...>; Antrasis trečiojo tikslo uždavinys – ugdyti kūrybiškumą, pažangius gebėjimus ir rinkos poreikius atitinkančius kibernetinio saugumo įgūdžius ir kvalifikaciją <...>; Trečiasis trečiojo tikslo uždavinys – skatinti viešojo ir privataus sektorių bei mokslo ir studijų institucijų bendradarbiavimą, kuriant kibernetinio saugumo srities inovacijas <...>"* (p. 10-11). 2. 2019 m. liepos 3 d. LRV nutarimo Nr. 709 ,,Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio veiklos plano" 5.6 punktas: *,,Krašto apsaugos ministerija, Lietuvos kariuomenė, Nacionalinis kibernetinio saugumo centras, Lietuvos Respublikos Vyriausybės kanceliarija – siekdami kelti <...> kibernetinio saugumo kultūrą, organizuoti kibernetinio saugumo mokymus ir vykdyti kitas kibernetinio saugumo švietimo iniciatyvas, skirtas kibernetinio saugumo aplinkai gerinti."* (p. 3).
Kibernetinio saugumo higiena	1. 2018 m. gruodžio 5 d. LRV nutarimo Nr. 1209 ,,Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo" III skyriaus 5.1 punktas: *,,Ne rečiau kaip kartą per metus arba po esminių organizacinių ar sisteminių pokyčių Aprašo II skyriuje nustatyta tvarka organizuoja ir atlieka rizikos vertinimą."* (p. 2). IV skyriaus 14 punktas: *,,Techniniai kibernetinio saugumo* ***4 lentelės tęsinys kitame puslapyje***

	reikalavimai subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius, ir ypatingos svarbos informacinės infrastruktūros valdytojams nustatomi pagal valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros svarbą <...>." (p. 5). 2. 2019 m. liepos 3 d. LRV nutarimo Nr. 709 „Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio veiklos plano" 5.5 punktas: *„Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos – siekdamas plėtoti kompleksines ankstyvojo perspėjimo priemones, diegti ir valdyti technines kibernetinio saugumo priemones ypatingos svarbos informacinėje infrastruktūroje ir valstybės informaciniuose ištekliuose."* (p. 3).
Bendradarbiavimas kibernetinio saugumo klausimais	1. 2011 m. gruodžio 15 d. LRS Nr. XI-1807 „Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo" III skyriaus 7 straipsnis: *„Valstybės informacinių išteklių valdymo taryba <...> sudaro valstybės informacinių išteklių politiką formuojančių institucijų, Vyriausybės kanceliarijos, Lietuvos Respublikos Seimo kanceliarijos (toliau – Seimas), Respublikos Prezidento kanceliarijos, Nacionalinės teismų administracijos, Lietuvos savivaldybių asociacijos ir kiti atstovai, kompetentingi informacinių ir ryšių technologijų srityje."* (p. 7). 2. 2014 m. gruodžio 11 d. LRS Nr. XII-1428 „Lietuvos kibernetinio saugumo įstatymo" II skyriaus 9 straipsnis: *„Kibernetinio saugumo taryba yra sudaroma iš kibernetinio saugumo politiką formuojančių ir įgyvendinančių valstybės institucijų, informacinių technologijų srityje veiklą vykdančių verslo subjektų atstovų, mokslo ir studijų 6 institucijų atstovų, ypatingos svarbos informacinės infrastruktūros valdytojų, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų, elektroninės informacijos prieglobos paslaugų teikėjų atstovų, o prireikus ir iš kitų asmenų."* (p. 5-6). ***4 lentelės tęsinys kitame puslapyje***

	IV skyriaus 17 straipsnis: ,,*Kibernetinio saugumo informacinis tinklas <...> yra saugi informacijos mainų platforma, kurios paskirtis yra dalytis informacija apie galimus ir įvykusius kibernetinius incidentus <...> tarp kibernetinio saugumo informacinio tinklo narių kibernetinio saugumo srityje. 3. Kibernetinio saugumo informaciniame tinkle skelbiama aktuali viešojo administravimo subjektų, valdančių ir (arba) tvarkančių valstybės informacinius išteklius, <...> ir ypatingos svarbos informacinės infrastruktūros valdytojų paskirtų asmenų ar padalinių, atsakingų už kibernetinio saugumo organizavimą ir kibernetinių incidentų valdymą, kontaktinė informacija.*" (p. 13). 18 straipsnis: ,,*1. Nacionalinis kibernetinio saugumo centras, Ryšių reguliavimo tarnyba, Policijos departamentas ir kitos policijos įstaigos bendradarbiauja tiriant kibernetinius incidentus, <...>. 2. Valstybinė duomenų apsaugos inspekcija bendradarbiauja su Nacionalinio kibernetinio saugumo centru ir Ryšių reguliavimo tarnyba tiriant kibernetinius incidentus, susijusius su asmens duomenų saugumo pažeidimais, <...>."* (p. 13-14). 3. 2018 m. rugpjūčio 13 d. LRV nutarimo Nr. 818 ,,Nacionalinės kibernetinio saugumo strategijos" Ketvirtasis skirsnis: ,,*Ketvirtasis Strategijos tikslas – stiprinti glaudų viešojo ir privataus sektorių bendradarbiavimą"* (p. 11). Penktasis skirsnis: ,,*Penktasis Strategijos tikslas – stiprinti tarptautinį bendradarbiavimą ir užtikrinti tarptautinių įsipareigojimų kibernetinio saugumo srityje vykdymą."* (p. 12). 4. 2019 m. liepos 3 d. LRV nutarimo Nr. 709 ,,Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio veiklos plano" atskaitingos ir įpareigotos LR ministerijos dėl bendradarbiavimo skatinimo kibernetinio saugumo klausimais: *Lietuvos Respublikos krašto apsaugos ministerija, Vidaus reikalų ministerija ir Lietuvos Respublikos užsienio reikalų ministerija*.

Šaltinis: parengta autorės, remiantis nurodytais LR teisės aktais.

Atlikus kibernetinį saugumą reglamentuojančių dokumentų turinio analizę, matyti, kad visgi autorės išskirti kibernetinio saugumo kultūros formavimo teoriniai aspektai yra „privalomi“ arba „privalomi tik iš dalies“ valstybinėms institucijoms, įgyvendinant kibernetinį saugumą Lietuvoje. Visų pirma, Lietuvos Respublikos įstatymai reglamentuoja, kad kibernetinio saugumo subjektai, šiuo atveju valstybinės institucijos, yra atsakingos už vidinės organizacijos strategijos ir kibernetinio saugumo politikos formavimą, suderinimą su Nacionaliniu kibernetinio saugumo centru (toliau – NKSC), patvirtinimą ir nuolatinį atnaujinimą. ***Vadinasi, kibernetinio saugumo kultūros formavimui organizacijoje reikalingas aspektas – strategijos kūrimas ir politikos formavimas – remiantis teisės aktais, yra privalomas.*** Toliau, kalbant apie kibernetinę higieną, t. y. kibernetinių rizikų valdymą, techninių ir organizacinių priemonių įvedimą į institucijos kibernetinio saugumo palaikymo praktiką, LR teisės aktai taip pat šioje vietoje nepalieka viešajam sektoriuj, valdančiam / tvarkančiam valstybės informacinius išteklius ar atsakingam už YSI objektus ir YSII, laisvos terpės interpretacijoms ir galimybei taikyti kitokius saugumo mechanizmus. ***Dėl šios priežasties galima teigti, kad kibernetinės higienos palaikymas taip pat yra privalomas viešojo sektoriaus institucijoms.***

Tačiau pastebėta, kad ***likusi dalis aspektų kibernetinio saugumo kultūros formavimo kontekste yra netinkamai reglamentuota arba neįpareigojantys visų valstybinių institucijų*** būti atskaitingoms už jų įgyvendinimą. LR įstatymuose bendradarbiavimas kibernetinio saugumo klausimais yra reglamentuotas daugiau ***formaliuoju būdu***, t. y. valstybinės institucijos ***nacionaliniu lygmeniu*** yra įpareigotos bendradarbiauti tokiais klausimais, kaip kibernetinių incidentų valdymas, svarbios / skubios informacijos perdavimas identifikavus sistemų, įrangos pažeidžiamumus, taip pat bendradarbiavimas yra vykdomas dalyvaujant skirtingų institucijų atstovams Kibernetinio saugumo tarybos ir Valstybės informacinių išteklių valdymo tarybos veiklose. ***Taip pat svarbu pabrėžti, kad tarptautinio bendradarbiavimo palaikymas yra paskirtas tik KAM, URM ir VRM.*** Nors LR teisės aktuose apie bendradarbiavimą kibernetinio saugumo klausimais yra įvardintos tiek nacionalinio, tiek tarptautinio lygmens bendradarbiavimo formos, tačiau ***valstybės siektinas viešo ir privataus sektoriaus bei Lietuvos mokslo ir studijų institucijų bendradarbiavimas, viešojo-privataus sektorių institucijų bendradarbiavimas tarptautiniu lygmeniu su užsienio valstybių institucijomis / organizacijomis iš skirtingų sektorių, nėra reglamentuotas ir įpareigojantis visų viešojo sektoriaus institucijų skirti, konkrečiai už kibernetinį saugumą atsakingus valstybės tarnautojus, ar darbuotojus, dirbančius pagal darbo sutartis, dalyvauti tokio tipo bendradarbiavimo renginiuose.*** Dėl šios priežasties bendradarbiavimas kibernetinio saugumo klausimais, kaip kibernetinio saugumo kultūros formavimo aspektas, Lietuvos valstybinėms institucijoms gali būti traktuojamas, kaip privalomas tik iš dalies. Tęsiant mokymų ir pratybų temą, kitas ne ką mažiau svarbus aspektas yra kibernetinio saugumo švietimas. Apie saugos personalo ir darbuotojų žinias, kompetencijas, mokymų programas, organizuojamas pratybas ir personalo kvalifikacijos kėlimo kursus / renginius, prisidedant prie

kibernetinio saugumo kultūros formavimo ne tik viešojo sektoriaus institucijų viduje, bet ir valstybiniu lygmeniu, yra reglamentuota ganėtinai abstrakčiai. Pavyzdžiui, ***įgyvendinant kibernetinio saugumo kultūros plėtrą per švietimą ir mokymą yra atsakingos tik 3 valstybinės institucijos: KAM, turint omenyje NKSC, kuriam suformuluotos užduotys susijusios su nacionalinio ir tarptautinio lygmens kibernetinio saugumo pratybų organizavimu, VRM – sukurti valstybės tarnautojų informacinės sistemos modulį kibernetinio saugumo mokymams rengti, ir ŠMSM – atnaujinti ir plėsti saugesnio interneto ambasadorių tinklą Lietuvoje.*** Vadinasi, kitos viešojo sektoriaus institucijos gali pasinaudoti ankstesnių institucijų sukurtomis priemonėmis šviesti darbuotojus kibernetinio saugumo klausimais, tačiau pačios ***nėra įpareigotos institucijų viduje skatinti skaitmeninę brandą, supratimą apie kibernetines grėsmes, saugumo priemonių taikymą per kibernetinio saugumo švietimo programas ar pasitelkiant kitas mokymo bei kvalifikacijos kėlimo formas, metodus.*** Derėtų pabrėžti ir tai, jog institucijų įsitraukimas į kibernetinio saugumo kultūros įgyvendinimą tiek individualiai, tiek prisidedant nacionaliniu lygmeniu, priklauso ne tik nuo išorės veiksnių, tokių kaip teisiniai įsipareigojimai, bet ir nuo vidinių veiksnių, pavyzdžiui, vadovavimo ir valdymo. Kitaip tariant, viešojo sektoriaus institucijose visų lygmenų vadovų indėlis skatinti ir motyvuoti darbuotojus savo kasdienę veiklą derinti su kibernetinio saugumo principais yra neatsiejama kibernetinio saugumo kultūros formavimo dalis. Pavyzdžiui, Lietuvos teisinėje bazėje vadovavimo ir valdymo aspektas, apibrėžtas „Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme“ ir „Kibernetinio saugumo įstatyme“ yra pritaikytas nacionaliniu lygmeniu. Tai reiškia, kad ***valstybinės institucijos turi įsipareigojimą dalyvauti Valstybės informacinių išteklių valdymo tarybos ir Kibernetinio saugumo tarybos veikloje, taip skatinant formuoti vieningą kibernetinio saugumo valdymą nacionaliniu lygmeniu, tačiau tiesioginės funkcijos vadovauti ir valdyti kibernetinio saugumo kultūros formavimo kontekste šioms taryboms nėra suteiktos.*** Todėl galima teigti, kad taryba veikia kaip patariamasis organas Vyriausybei, o jos ***veikla tikėtina, tiesiogiai nekoreliuoja su pačių dalyvaujančių valstybinių institucijų vidine vadovavimo ir valdymo politika.***

Kibernetinio saugumo kultūros įgyvendinimas Lietuvos viešajame sektoriuje nėra svetimas, o anaiptol, nacionaliniu lygmeniu sprendžiamas klausimas. Nors teorijos išskirti kibernetinio saugumo kultūros formavimo tiriamieji aspektai, tokie kaip strategijos kūrimas ir politikos formavimas, vadovavimas ir valdymas, kibernetinio saugumo švietimas, kibernetinio saugumo higiena ir bendradarbiavimas kibernetinio saugumo klausimais yra vienaip ar kitaip reglamentuoti LR teisinėje bazėje, tačiau kibernetinio saugumo kultūros formavimo tendencijų Lietuvos viešajame sektoriuje neatspindi. Dėl šios priežasties svarbu analizuoti praktinį tokio pastarųjų aspektų reglamentavimo pritaikomumą, įgyvendinimą, ypatumus ir problemas, su kuriomis susiduria valstybinės institucijos.

3. 2. NKSC vaidmuo Lietuvos kibernetinio saugumo kultūros formavime

Lietuvoje nuo 2018 m. prie KAM veikiantis NKSC yra pagrindinė valstybinė institucija, atsakinga už kibernetinio saugumo valdymą, reguliavimą, stebėseną ir kontrolę nacionaliniu lygmeniu. Todėl toliau darbe bus analizuojamos NKSC veiklos sritys, uždaviniai ir jų praktinis įgyvendinimas nacionalinio kibernetinio saugumo kultūros formavimo kontekste.

Vadovaujantis 2017 m. rugpjūčio 31 d. KAM įsakymu Nr. V-804 „Dėl nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos nuostatų ir struktūros patvirtinimo" NKSC pagrindiniai tikslai ir uždaviniai, susiję su kibernetinio saugumo kultūros formavimu yra:

1. **Nacionalinės kibernetinio saugumo politikos įgyvendinimas:**

- Organizacinių ir techninių kibernetinio saugumo reikalavimų valstybės informaciniams ištekliams ir YSII rengimas ir atitikties jiems stebėsena;
- Tipinių kibernetinių incidentų valdymo planų YSII rengimas;
- Kibernetinės gynybos planų YSII rengimas;
- Kibernetinio saugumo informacinio tinklo (toliau – KSIT) valdymas;
- Reagavimas į kibernetinius incidentus valstybės informaciniuose ištekliuose ir YSII;
- Techninių kibernetinio saugumo priemonių diegimas valstybės informaciniuose ištekliuose ir YSII.

2. **Saugumo priežiūros tarnybos funkcijų atlikimas:**

- Žinybinės saugumo priežiūros tarnybos funkcijų, susijusių su įslaptintos informacijos ryšių ir informacinių sistemų (toliau – ĮIRIS) nuostatų ir specifikacijų vertinimu, vykdymas pagal poreikį;
- Žinybinės saugumo priežiūros tarnybos funkcijų, susijusių su ĮIRIS atitikties vertinimu, vykdymas pagal poreikį;
- Žinybinės saugumo priežiūros tarnybos funkcijų, leidimų naudoti ĮIRIS išdavimu ir ĮIRIS apsaugos priežiūra, vykdymas pagal poreikį;
- Žinybinių saugumo priežiūros tarnybų apskaitos vykdymas;
- Žinybinių saugumo priežiūros tarnybų veiklos, susijusios su ĮIRIS apsaugos priežiūra ir leidimų naudoti ĮIRIS išdavimu, koordinavimas;
- Metodinių rekomendacijų teikimas paslapčių subjektams.

3. **Nacionalinės komunikacijų apsaugos tarnybos funkcijų atlikimas:**

- Kriptografinių metodų ir produktų tvirtinimas;
- ĮIRIS nuostatų, specifikacijų ir jų atitikties nustatytiems teisės aktų reikalavimams vertinimas;
- Paslapčių subjektų konsultavimas ĮIRIS klausimais;
- Institucijų laikymosi Lietuvos Respublikos Vyriausybės nustatytų ĮIRIS telekomunikacijų apsaugos reikalavimams, priežiūra.

4. Informacijos sklaidos, tyrimų ir analizės kibernetinio saugumo srityje veiklos vykdymas:

- Nacionalinės kibernetinio saugumo situacijos analizės ir saugumo būklės ataskaitos parengimas;
- Informacijos kibernetinio saugumo klausimais sklaidos užtikrinimas; vykdo informacijos sklaidą kibernetinio saugumo klausimais;
- Konsultacijų ir rekomendacijų kibernetinio saugumo klausimais teikimas valstybės informacinių išteklių ir YSII valdytojams;
- Kibernetinio saugumo projektų plėtojimas.

Be visa to, remiantis 2019 m. liepos 3 d. LRV nutarimu Nr. 709 patvirtintu „Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstituciniu veiklos planu“, kurio tikslas yra praktinis Nacionalinės kibernetinio saugumo strategijos tikslų ir uždavinių jiems pasiekti įgyvendinimas, NKSC turi ir daugiau strategiškai svarbių uždavinių. Visų pirma, su tikslu kurti sisteminį požiūrį į kibernetinį saugumą ir prevencinę veiklą, NKSC yra atsakinga už Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimų stebėsenos sistemos (toliau – ARSIS) atnaujinimą. NKSC paskyrus ARSIS tvarkytoju, institucijai yra suteiktos teisės reguliuoti valstybės informacinių išteklių atitikimą teisės aktuose reglamentuotiems reikalavimams, kas iš esmės stipriai prisideda prie kibernetinio saugumo kultūros formavimo vadovavimo ir valdymo mechanizmo užtikrinimo. Visų antra, NKSC nuostatuose nepaminėta, tačiau labai svarbi institucijai paskirta užduotis, siekiant kelti kibernetinio saugumo kultūrą nacionaliniu lygmeniu – „organizuoti kibernetinio saugumo mokymus ir vykdyti kitas kibernetinio saugumo švietimo iniciatyvas, skirtas kibernetinio saugumo aplinkai gerinti.” (p. 3). Pastarajam uždaviniui įgyvendinti NKSC, bendradarbiaudamas su Kauno technologijos universitetu, rengia vieną kartą į metus vykstančias nacionalines kibernetinio saugumo pratybas „Kibernetinis skydas“. Pratybomis yra siekiama formuoti kibernetinio saugumo subjektų gebėjimus valdyti kibernetinius incidentus, atskleisti jų saugumo žinias ir įgūdžius bei skatinti institucijų bendradarbiavimą. Svarbu paminėti, kad pratybų formatas yra pritrauktas prie tarptautinės NKSC patirties dalyvaujant tokio tipo mokymuose užsienyje, dėl to buvo nuspręsta, kad kibernetinio saugumo subjektai bus treniruojami realistiškiausiomis sąlygomis, t. y. su turimais techniniais pajėgumais, personalu, procedūromis. Kitas ne ką mažiau svarbus NKSC paskirtas projektas, susijęs su nacionaline kibernetinio saugumo kultūra ir inovacijų plėtra – „Kompleksiniai kibernetinės saugos mokymai valstybės ir savivaldybių institucijų ir įstaigų dirbantiesiems“. Remiantis KAM (2020) pranešimu, projektu siekiama suteikti valstybinių institucijų darbuotojams žinių kibernetinio saugumo srityje. Projekto įgyvendinimo terminas yra 2022 m. balandžio 1 d. Tikėtina, kad tokio tipo mokymai prisidės prie bendro kibernetinio saugumo paveikslo stiprinimo viešajame sektoriuje. Taip pat NKSC vykdo ir kitas kibernetinio saugumo švietimo iniciatyvas, skirtas kibernetinio saugumo aplinkai gerinti, tokias

kaip kibernetinio saugumo pagrindų ir specializuotus techninio pobūdžio mokymus valstybinėms institucijoms, pranešimų socialiniuose tinkluose talpinimas kibernetinio saugumo temomis, kibernetinio saugumo biuletenių ir kibernetinių incidentų bei tyrimo ataskaitų parengimas ir viešas paskelbimas. Todėl galima teigti, kad ***NKSC turi labai svarbų vaidmenį žinių apie kibernetinį saugumą suteikimą Lietuvos valstybinėms institucijoms, o tai reiškia, kad kibernetinio saugumo švietimo lygis viešajame sektoriuje stipriai priklauso nuo NKSC organizuojamų mokymų kokybės.***

Toliau analizuojant NKSC vaidmenį Lietuvos kibernetinio saugumo kultūros formavime, svarbu paminėti ir viešojo-privataus sektorių bendradarbiavimo nacionaliniu ir tarptautiniu lygiu skatinimo iniciatyvas, tokias kaip:

- KSIT, skirtą informacijos mainams apie kibernetinio saugumo grėsmes ar įvykusius incidentus;
- Pažeidžiamumų vertinimo kampanijos, skirtos viešojo ir privataus sektorių organizacijų interneto svetainių saugumui nustatyti;
- Galimybių studija, skirta atsakingo viešojo ir privataus sektoriaus informacinių ir ryšių technologijų (toliau – IRT) saugumo spragų atskleidimo praktikai įteisinti;
- Informacinė sistema (MAPPI (*MAP of Public Internet*)), kuri, pasiekus visišką funkcionalumą, padėtų NKSC efektyviai koordinuoti ir valdyti kibernetinius incidentus, grėsmes, užtikrinti glaudesnį tarptautinį ir nacionalinį bendradarbiavimą;
- NKSC dalyvavimas tarptautinėse kibernetinio saugumo pratybose („Suremti skydai“, „Blue OLEx“, „Kibernetinis skydas“, „EuroSOPex“).

Pastarosios iniciatyvos atskleidžia NKSC, kaip pagrindinės kibernetinį saugumą reguliuojančios institucijos vaidmenį bendradarbiavimo kibernetinio saugumo klausimais kontekste, kas akivaizdu, kad yra ***viena didžiausių paskatų ar net įpareigojimų viešojo sektoriaus institucijoms komunikuoti tarpusavyje, skatinti vieningą kibernetinio saugumo aplinkos atsparumo užtikrinimo praktiką nacionaliniu lygmeniu bei pačiai NKSC ir tarptautiniu lygmeniu, perimant geriausias praktikas ir pritaikant jas vėliau nacionalinėje plotmėje.***

Detalizuojant NKSC vaidmenį kibernetinio saugumo higienos taikymo kontekste, svarbu pabrėžti, kad centro indėlis yra nekvestionuojamas. Tai yra, kad ***techninių kibernetinio saugumo priemonių įvedimo ir taikymo valstybės informaciniuose ištekliuose ir YSII yra ne kieno kito, bet NKSC atsakomybė.*** Antrinant institucijos nuostatuose išrašytus uždavinius, susijusius su kibernetine higiena, šiems uždaviniams įgyvendinti NKSC ne tik teikia siūlymus su techniniais reikalavimais susijusiems teisės aktams, bet ir pati praktiškai įgyvendina iniciatyvas, skatinančias kibernetinės higienos palaikymą nacionalinėje kibernetinio saugumo aplinkoje. Remiantis „Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio veiklos plano 2019 metų asignavimų panaudojimo detaliąja ataskaita“, NKSC:

- Pradėjo naudoti daugiau kibernetinio saugumo technologijų, susijusių su kibernetinių incidentų aptikimu, rizikų kontrole ir valdymu;
- Savivaldos, Respublikos Prezidento ir Europos Parlamento rinkimų metu užtikrinimo elektroninį saugumą;
- Įdiegė naują įrangą, leidžiančią pasitikrinti Lietuvoje registruotos internetinės svetainės saugumą;
- Pradėjo vykdyti du inovatyvius kibernetinio saugumo srities projektus: saugūs kriptografiniai mainai ir ankstyvųjų kibernetinių grėsmių aptikimo ir užkardymo sistema.

Susisteminus NKSC uždavinius ir veiklos sritis, galima teigti, kad institucijos pagrindinis veiklos laukas yra viešasis sektorius ir YSI objektai. NKSC stipriai prisideda prie viešojo sektoriaus kibernetinio saugumo strategijos kūrimo ir politikos formavimo, institucijų kibernetinio švietimo didinimo, nacionalinio kibernetinio saugumo valdymo, taip pat vieningų kibernetinio saugumo higienos priemonių įvedimo. Visa tai duoda gaires kibernetinio saugumo subjektams, formuojant jų organizacijų viduje bendrą ir sisteminį požiūrį į kibernetinį saugumą. Todėl galima teigti, kad ***Lietuvos valstybinių institucijų kibernetinio saugumo kultūros įgyvendinimo pradžios taškas yra būtent NKSC formuojama kibernetinio saugumo politika ir jos pritaikomumui nustatyti mechanizmai.***

3.3. LR ministerijų kibernetinio saugumo kultūros formavimo tiriamieji aspektai

Lietuvoje kibernetinis saugumas yra neatsiejama nacionalinio saugumo įgyvendinimo dalis. Pats nacionalinis saugumas negali egzistuoti be vieningo, konstruktyvaus ir sisteminio požiūrio į saugumo užtikrinimo priemones, konkrečiai į kibernetinio saugumo kultūrą. Todėl visų pirma vienu iš pagrindinių tikslų valstybei tampa siekis formuoti atitinkamą kibernetinio saugumo politiką valstybiniams sektoriams, valdantiems ir tvarkantiems valstybės informacinius išteklius ar YSII, kurių saugumas yra valstybės strateginiai prioritetai. Taigi toliau skyriuje bus analizuojamas valstybinių institucijų, konkrečiai LR ministerijų, kibernetinio saugumo kultūros formavimo ypatumai jų institucijų viduje bei indėlis nacionaliniu lygmeniu, siekiant identifikuoti koreliaciją ir priežastinius ryšius nacionalinio saugumo stiprinimo kontekste.

Remiantis LR kibernetinio saugumo įstatymu (2014), „kibernetinio saugumo politikos strateginius tikslus ir jiems pasiekti būtinas priemones nustato Lietuvos Respublikos Vyriausybė.” (p. 3). LR Vyriausybei, siekiant apimti pagrindinius valstybinius sektorius, jos pavaldume yra įsteigta 14 ministerijų, kurių pagrindinė užduotis yra formuoti valstybės politiką, taip pat organizuoti, koordinuoti ir kontroliuoti jos įgyvendinimą pavestose valdymo srityse. LR ministerijų vaidmuo kibernetinio saugumo kultūros formavime nacionaliniu lygmeniu gali būti traktuojamas ir išskiriamas remiantis kiekvienai ministerijai pavestomis užduotimis, susijusiomis su valstybės informacinių išteklių ir YSII steigimu, valdymu, tvarkymu, modernizavimu, apsauga bei kibernetine gynyba (žr. 5 lentelę).

5 lentelė. LR ministerijų uždaviniai kibernetinio saugumo kultūros formavime nacionaliniu lygmeniu

Eil. Nr.	Ministerija	Uždaviniai
1.	KAM	➢ Rengia organizacinius ir techninius kibernetinio saugumo reikalavimus valstybės informaciniams ištekliams ir YSII; ➢ Rengia Nacionalinį kibernetinių incidentų valdymo planą; ➢ Rengia tipinius kibernetinių incidentų valdymo YSII planus; ➢ Tvirtina YSII kibernetinės gynybos planus; ➢ Rengia ir tvirtinti Kibernetinio saugumo informacinio tinklo nuostatus; ➢ Atlieka Nacionalinės kibernetinio saugumo strategijos įgyvendinimo ir vertinimo kriterijų pasiekimų stebėseną; ➢ Nustato savo sektoriaus ir subsektoriaus YSI objektus / YSII, įvertina ir teikia tvirtinti; ***5 lentelės tęsinys kitame puslapyje***

		➢ Nustato krašto apsaugos sistemos valstybės institucijų atsakomybę ir funkcijas valstybės kibernetinės gynybos pajėgumų plėtros srityje; ➢ Plėtoja tarptautinį bendradarbiavimą su užsienio valstybių kompetentingomis institucijomis kibernetinio saugumo srityje; ➢ Tobulina kibernetinio saugumo srities teisinį reglamentavimą ir organizuoja praktikinio taikymo seminarus; ➢ Rengia privataus sektoriaus bei Lietuvos mokslo ir studijų institucijų vykdomų priemonių kibernetinio saugumo srityje planą; ➢ Rengia Lietuvos viešojo-privataus sektorių tarptautinio bendradarbiavimo kibernetinio saugumo srityje formų sąrašą; ➢ Organizuoja kibernetinio saugumo mokymus ir kitas kibernetinio saugumo švietimo iniciatyvas, skirtas kibernetinio saugumo aplinkai gerinti; ➢ Periodiškai vykdo kibernetinio saugumo būsenos tyrimus, pažangos matavimus; ➢ Rengia kibernetinio saugumo gaires nacionalinės pramonės skaitmeninimo iniciatyvoms įgyvendinti; ➢ Dalyvauja kibernetinio saugumo Taryboje.
2.	VRM	➢ Rengia YSII identifikavimo metodiką ir identifikuoja YSII bei šios infrastruktūros valdytojų sąrašą; ➢ Nustato savo sektoriaus ir subsektoriaus YSI objektus / YSII, įvertina ir teikia tvirtinti; ➢ Stiprina teisėsaugos institucijų darbuotojų profesinius gebėjimus; ➢ Propaguoja visuomenės savisaugos kultūrą bei plėtoja tarptautinį bendradarbiavimą; ➢ Dalyvauja kibernetinio saugumo Taryboje; ➢ Įgyvendina projektus, susijusius valstybės pajėgumo ir gebėjimo kovoti su nusikalstamomis veikomis kibernetinėje erdvėje stiprinimu; ➢ Dalyvauja nusikalstamų veikų kibernetinėje erdvėje prevencijos ir tyrimo tarptautiniuose renginiuose ir darbo grupėse; ➢ Dalyvauja tarptautinėse operacijose, tiriant nusikalstamas veikas kibernetinėje erdvėje; ➢ Užtikrina tvarkomų ir valdomų valstybės informacinių išteklių ir vidaus reikalų srities informacinių sistemų, valstybės ir žinybinių registrų tvarkymą, technologinį suderinamumą ir kibernetinę saugą; ***5 lentelės tęsinys kitame puslapyje***

		➢ Vykdo Lietuvos viešojo saugumo ir pagalbos tarnybų skaitmeninio mobiliojo radijo ryšio tinklo plėtrą ir modernizavimą; ➢ Kuria elektronines paslaugas ikiteisminio tyrimo proceso dalyviams.
3.	URM	➢ Nustato savo sektoriaus ir subsektoriaus YSI objektus / YSI, įvertina ir teikia tvirtinti; ➢ Rengia Lietuvos viešojo-privataus sektorių tarptautinio bendradarbiavimo kibernetinio saugumo srityje formų sąrašą; ➢ Atstovauja Lietuvos Respublikai ir įgyvendina kibernetinio saugumo nacionalinius interesus ES, NATO, Jungtinių Tautų, Europos saugumo ir bendradarbiavimo organizacijos, Baltijos regiono ir kitų tarptautinių organizacijų veikloje; ➢ Dalyvauja kibernetinio saugumo Taryboje.
4.	AM	➢ Nustato savo sektoriaus ir subsektoriaus YSI objektus / YSII, įvertina ir teikia tvirtinti; ➢ Valdo ir vysto informacines sistemas aplinkosaugos, teritorijų planavimo ir statybos valstybinės priežiūros srityje bei užtikrina jų kibernetinį saugumą.
5.	EIMIN	➢ Nustato savo sektoriaus ir subsektoriaus YSI objektus / YSI, įvertina ir teikia tvirtinti; ➢ Rengia kibernetinio saugumo gaires nacionalinės pramonės skaitmeninimo iniciatyvoms įgyvendinti; ➢ Formuoja valstybės skaitmeninę politiką; ➢ Organizuoja ir vykdo valstybės informacinių išteklių pertvarką, modernizavimą; ➢ Dalyvauja kibernetinio saugumo Taryboje.
6.	ENMIN	➢ Nustato savo sektoriaus ir subsektoriaus YSI objektus / YSII, įvertina ir teikia tvirtinti; ➢ Skatina IT ir kibernetinio saugumo inovacijas energetikos srityje; ➢ Kontroliuoja Nacionalinės energetinės nepriklausomybės strategijoje nurodytus kibernetinio saugumo kultūros įgyvendinimo procesus; ➢ Dalyvauja kibernetinio saugumo Taryboje.
7.	SAM	➢ Nustato savo sektoriaus ir subsektoriaus YSI objektus / YSII, įvertina ir teikia tvirtinti; ➢ Užtikrina valstybėje naudojamų e. sveikatos sprendimų valdymo kokybę, siekiant įgyvendinti informacijos ir kibernetinės saugos reikalavimus. ***5 lentelės tęsinys kitame puslapyje***

8.	KM	➢ Steigia ir modernizuoja valstybės informacines sistemas, susijusius su kultūros paveldo skaitmeninimu; ➢ Užtikrina visuomenės informacinio raštingumo plėtrą ir skatina atsparumo informacinėms grėsmėms gebėjimų ugdymą.
9.	ŠMSM	➢ Atnaujina ir plečia saugesnio interneto ambasadorių tinklą Lietuvoje; ➢ Valdo Studijų, mokymo programų ir kvalifikacijų registrą, steigia ir valdo žinybinius registrus ir valstybės informacines sistemas bei užtikrina jų kibernetinį saugumą; ➢ Prisideda prie visuomenės atsparumo informacinėms grėsmėms stiprinimo ir informacinio raštingumo ugdymo; ➢ Dalyvauja kibernetinio saugumo Taryboje.
10.	SOCMIN	➢ Remia bendrus jaunimo ir vyresnio amžiaus žmonių nevyriausybinių organizacijų projektus, ugdant vyresnio amžiaus žmonių gebėjimus informacinių technologijų srityje; ➢ Valdo, prižiūri ir modernizuoja darbo ir socialinės apsaugos valstybės informacinę sistemą.
11.	ŽUM	➢ Nustato savo sektoriaus ir subsektoriaus YSI objektus / YSII, įvertina ir teikia tvirtinti; ➢ Atsako už valstybės žemės ūkio sektoriaus informacinių sistemų diegimą ir vystymą, kibernetinį saugumą.
12.	TM	➢ Nustato savo sektoriaus ir subsektoriaus YSI objektus / YSII, įvertina ir teikia tvirtinti; ➢ Valdo 14 valstybės registrų ir 8 valstybės informacines sistemas bei užtikrina jų funkcionavimą, saugumo reikalavimų atitikimą ir kibernetinį saugumą; ➢ Rengia ir priima teisės aktus, susijusius su registrų ir valstybės informacinių sistemų kibernetiniu saugumu; ➢ Formuoja valstybės politiką registrų teisinio reguliavimo srityje; ➢ Organizuoja specializuotus mokymus, siekiant tobulinti teismo ekspertų gebėjimus tirti nusikalstamas veikas kibernetinėje erdvėje; ➢ Dalyvauja kibernetinio saugumo Taryboje.
13.	FINMIN	➢ Nustato savo sektoriaus ir subsektoriaus YSI objektus / YSII, įvertina ir teikia tvirtinti; ➢ Steigia, plečia ir modernizuoja valstybės finansų, audito ir mokesčių valdymo bei prižiūri e.muitinės informacines sistemas, užtikrina jų kibernetinį saugumą. ***5 lentelės tęsinys kitame puslapyje***

14.	SUMIN	➢ Nustato savo sektoriaus ir subsektoriaus YSI objektus / YSII, įvertina ir teikia tvirtinti; ➢ Formuoja valstybės politiką elektroninių ryšių srityje; ➢ Prisideda prie Lietuvos junglumo su ES šalimis informaciniais infrastruktūros keliais; ➢ Dalyvauja kibernetinio saugumo Taryboje.

Šaltinis: lentelė sudaryta autorės, remiantis LR teisės aktais, ministerijų strateginiais veiklos planais, bei viešai ministerijų tinklalapiuose skelbtinais duomenimis.

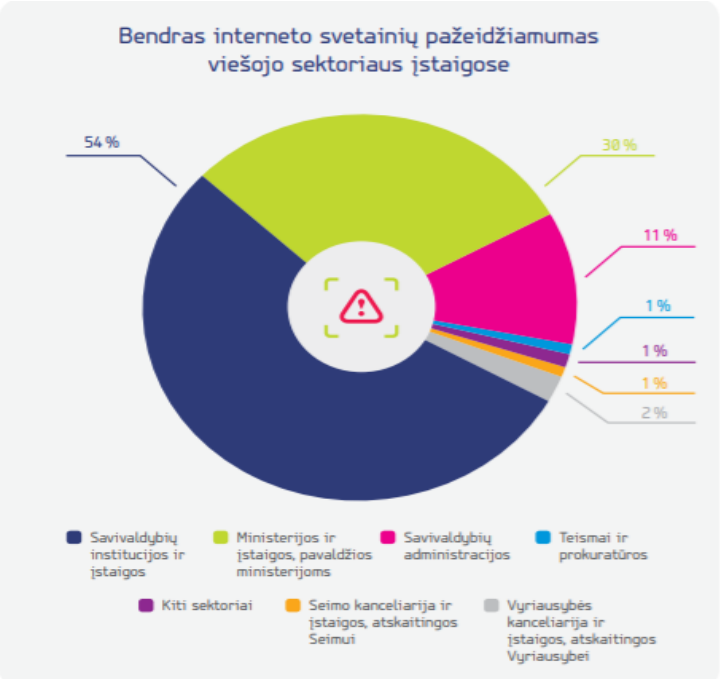
Apžvelgus LR ministerijų kibernetinio saugumo palaikymo ir kultūros formavimo uždavinius valstybiniu lygmeniu, pastebėta, kad didžiausią kiekį įgaliojimų ir pavestų užduočių turi ***KAM, VRM ir TM***. Šių trijų ministerijų vaidmuo kibernetinio saugumo kontekste yra siejamas ne tik su jų pavesta valdymo sritimi, bet ir nacionaliniu mastu. T. y. šios institucijos yra ***pagrindinės kibernetinio saugumo politikos, teisinio, techninio ir organizacinio pagrindo formuotojos bei steigėjos***. Taip pat svarbu paminėti, kad pateikti uždaviniai atskleidė, jog visos institucijos valdo ir tvarko valstybės informacinius išteklius, tokius kaip valstybės gynybos, teisėsaugos, finansų, sveikatos, kultūros, švietimo, darbo, energetikos, susisiekimo, žemės ūkio, aplinkosaugos bei kitas informacinės sistemas, valstybinius ir žinybinius registrus, taip pat prisideda prie savo sektorių informacinės politikos formavimo, pertvarkymo. Vadinasi, ***LR ministerijos atsako už didžiosios dalies valstybės informacinių išteklių kibernetinį saugumą bei jų atitikimą teisės aktuose nurodytiems techniniams ir organizaciniams reikalavimams.*** Kitas svarbus identifikuotas dalykas yra tai, kad nors visos ministerijos valdo ir tvarko valstybės informacinius išteklius, taip pat, remiantis institucijų strateginiais veiklos planais, prisideda prie kibernetinio saugumo įgyvendinimo ir palaikymo nacionaliniu lygmeniu, tačiau Kibernetinio saugumo valdymo tarybos veikloje nedalyvauja (Tarybą sudaro tik 8 iš 14 ministerijų). Tai reiškia, ***kad iš bendradarbiavimo kibernetinio saugumo klausimais nacionaliniu lygmeniu prizmės, beveik pusei ministerijų nėra suteiktos galimybės plėsti savo žinias, bendrą supratimą ir formuoti vieningą požiūrį šios srities klausimais tarp pagrindinių valstybės politiką formuojančių organų.*** Dėl šios priežasties, tikėtina, nukenčia ir institucijos vidinė politika bei veiklos procesų derinimas su kibernetine sauga. Taip pat svarbu paminėti, kad ***tarptautinį bendradarbiavimą kibernetinio saugumo klausimais, remiantis viešai skelbtina informacija, vysto tik 4 ministerijos (KAM, VRM, URM ir SUMIN).***

Apibendrinant LR ministerijų vaidmenį kibernetinio saugumo kultūros formavime valstybiniu lygmeniu galima teigti, kad institucijos yra nacionalinio saugumo stiprinimo paveikslo dalis dėl jų valdomų ir tvarkomų valstybės informacinių išteklių, jautrių asmens duomenų ir apdorojamos informacijos svarbos. Todėl pastarųjų RIS kibernetinio saugumo užtikrinimas yra neatsiejama nacionalinio saugumo palaikymo priemonė, kuri turi būti kokybiškai ir efektyviai įgyvendinama. Dėl šios priežasties yra svarbu formuoti kibernetinio saugumo kultūrą, visų pirma, institucijų viduje, norint,

kad valstybės informacinių išteklių saugumas būtų užtikrintas ir nacionalinėje plotmėje. Taigi toliau skyriuje bus analizuojami LR ministerijų vidiniai kibernetinio saugumo palaikymo ypatumai.

Remiantis NKSC nacionalinio kibernetinio saugumo būklės vertinimo ataskaita (2019), per 2019 metus buvo nustatytas 413 kenkimo PĮ kibernetinių incidentų skaičius ypatingos svarbos paslaugas teikiančių kibernetinio saugumo subjektų informacinėse sistemose (tuo tarpu 2018 m. – 470). „Daugiausiai jų buvo užfiksuota krašto apsaugos sistemoje (49 proc.), valstybės valdymo (13 proc.) bei užsienio reikalų ir saugumo politikos (12 proc.) sektoriuose.” (ten pat, p. 26). Svarbu pabrėžti, kad remiantis 2018 m. NKSC nacionalinio kibernetinio saugumo būklės vertinimo ataskaita, tokio tipo incidentai dominavo finansų sektoriuje (39 proc.), o 2020 m. tendencijos pakito – labiausiai nukentėjo interneto paslaugų ir prieglobos paslaugų teikėjai. Nors naujausioje NKSC kibernetinio saugumo būklės vertinimo ataskaitoje (2020) nėra akcentuojama apie YSII ir valstybės informacinių išteklių kibernetinio saugumo incidentų tendencijų pokyčius, galima teigti, kad bendra kibernetinio saugumo būklė signalizuoja apie kibernetinių atakų vektorių pokytį ir poreikį institucijoms išlaikyti budrumą ir sąmoningumą diegiant programinę įrangą, o ypač į valstybės informacinę infrastruktūrą bei YSII. Taip pat svarbu suprasti, kad kenkimo PĮ rizika valstybiniame sektoriuje daro didžiulę įtaką nacionaliniam saugumui. Tad nors statistinis kibernetinių incidentų rodiklis anot NKSC mažėja, tačiau negalima teigti, kad valstybinės institucijos geba efektyviai tvarkytis elektroninėje erdvėje. Tai liudijantis dar vienas faktas yra tai, kad NKSC atlikus viešojo sektoriaus interneto svetainių pažeidžiamumo vertinimą, nustatyta, kad labiausiai pažeidžiamos interneto svetainės priklauso savivaldybėms ir ministerijoms (žr. pav. 6).

6 pav. Viešojo sektoriaus institucijų interneto svetainių pažeidžiamumas



Šaltinis: Nacionalinio kibernetinio saugumo būklės ataskaita (2020).

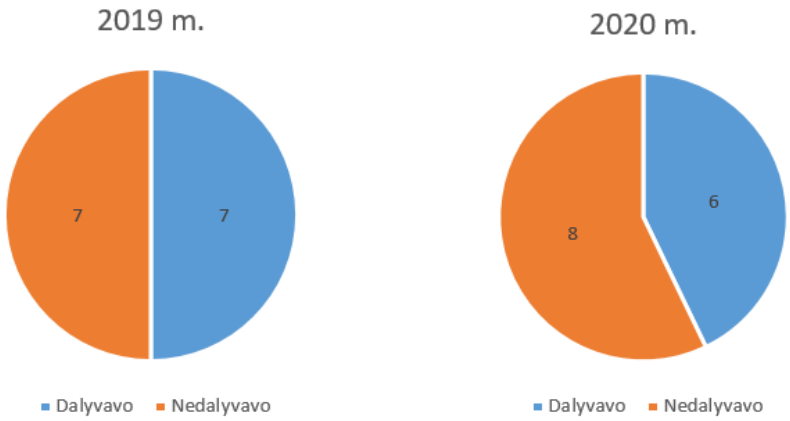
Sekantis faktas, liudijantis kibernetinio saugumo organizacinių ir techninių priemonių įgyvendinimo spragas valstybės informacinius išteklius valdančiose / tvarkančiose institucijose yra NKSC kibernetinio saugumo būklės ataskaitose pateiktas pastarųjų reikalavimų įgyvendinimo vertinimas, konkrečiai vertinant paskutinių trijų metų laikotarpį. Taigi, nors atliktas vertinimas atskleidė ir gerąsias kibernetinio saugumo palaikymo praktikas YSII, kurios išaugo iki 80 proc., tačiau valstybiniame sektoriuje situacija pasirodo negerėja: 2018 m. įgyvendintų reikalavimų skaičius tesiekė 24 proc., o 2019 m. – 22 proc. Tuo tarpu 2020 m. NKSC ataskaitoje buvo nustatyta, kad tik pusė visų valstybės informacinių išteklių valdytojų vadovaujasi su NKSC suderintais saugos dokumentais, o kibernetinio saugumo būklė YSII ir valstybės informaciniuose ištekliuose nėra tokia, kokią ją deklaruoja pastarųjų sistemų valdytojai. Pasak NKSC, ,,tokiam vangiam ir gana ilgam saugos dokumentų derinimo procesui įtakos turi ne tik aplaidus VII valdytojų požiūris į reikalavimų įgyvendinimą, kompetentingų kibernetinio saugumo, informacinių technologijų specialistų ir (ar) reikalingos kompetencijos trūkumas, bet ir pačių informacinių sistemų bei registrų sudėtingumas, kurį, savo ruožtu, lemia nuolatinė IRT plėtra.” (*ten pat*, p. 44). Todėl remiantis statistika galima teigti, kad ***techniniai ir organizaciniai reikalavimai valstybės informaciniams ištekliams nėra efektyvūs, t. y. jie yra interpretuojami, per retai audituojamas jų atitikimas, jų neįgyvendinimo faktoriaus nelydi sankcijos, o galiausiai, tikėtina, jie nėra pritaikyti institucijų poreikiams arba nekoreliuoja su veiklos procesais dėl žinių bei kvalifikacijos stokos.*** Remiantis Valstybinio audito ataskaita (2018), kurioje pateikti SUMIN, KAM ir VRM atlikto audito vertinimo rezultatai, buvo nustatyta, kad:

- Valstybės informacinių išteklių valdymo brandos pokyčių tendencijos gerėja per lėtai progresuojančių kibernetinių grėsmių akivaizdoje;
- Egzistuoja valstybės informacinių išteklių atitikimo gerosioms IT valdymo praktikoms / standartams stoka;
- Nepakankamai veiksmingai įgyvendinamos kibernetinio saugumo priemonės atsparumo kibernetinėms grėsmėms didinimo kontekste.

Apžvelgus aukščiau pateiktą valstybinių institucijų statistiką ir tendencijų analizę, akivaizdu, jog pastarieji faktai signalizuoja apie probleminių sričių viešajame sektoriuje egzistavimą. Su tikslu nustatyti viso to priežastinius ryšius, visų pirma, aktualu nagrinėti LR ministerijų indėlį darbuotojų požiūrio į kibernetinį saugumą formavime, suteikiamas sąlygas ir pasinaudojamas galimybes kelti skaitmeninę brandą. Vienas iš pavyzdžių, kuris tikėtina, yra vienas pagrindinių efektyvų kibernetinio saugumo kultūros palaikymą LR ministerijose lemiančių veiksnių – institucijų dalyvavimas kibernetinio saugumo mokymuose / pratybose nacionaliniu lygmeniu. Remiantis pratybų „Kibernetinis Skydas“ ataskaitomis visuomenei, pastebėta, kad LR ministerijų dalyvavimas yra labai pasyvus (žr. pav. 7). Svarbu paminėti, kad NKSC, 2019 m. identifikavus žemą LR ministerijų dalyvavimo rodiklį jų organizuotose pratybose,

ataskaitoje paminėjo, kad ieškos būdų, kaip padidinti pastarųjų institucijų įsitraukimą kitais metais. Visgi, 2020 m. rodiklis dar labiau suprastėjo, kas įrodo, jog efektyvių priemonių nebuvo imtasi.

7 pav. LR ministerijų dalyvavimo statistika nacionalinėse kibernetinio saugumo pratybose „Kibernetinis skydas“ 2019 m. ir 2020 m.



Šaltinis: sudaryta autorės, remiantis nacionalinių kibernetinio saugumo pratybų „Kibernetinis skydas“ 2019 m. ir 2020 m. ataskaitomis visuomenei.

Su tikslu identifikuoti galimas institucijų pasyvaus dalyvavimo priežastys, galima peržvelgti pratybų scenarijų ir pratybų vertinimo apklausos rezultatus. Pratybų scenarijus tiek vienais, tiek kitais metais buvo ganėtinai lankstus, t. y. NKSC pateikia keletą siužeto linijų, susijusių su kibernetinio saugumo grėsmėmis ir leidžia kibernetinio saugumo subjektams pasirinkti pagal jų institucijų poreikius jiems priimtiniausius siužetus. Visgi, pastebėtina, kad siužetai dviejų metų perspektyvoje yra ganėtinai panašūs ir labiau techninio profilio, kas tikėtina, atbaido institucijų IT ar aukštesniuosius vadovus nuo įsitraukimo į pratybas dėl techninių žinių stokos. Taip pat galima teigti, kad ***pratybose trūksta organizacinio lygmens siužeto pateikimo, t. y. kaip kibernetinis incidentas paveikia visos organizacijos veiklos procesus, kuomet turi sprendimus priimti ne IT saugos personalas, bet visų lygmenų vadovai bei kartu suvaldyti iškilusias rizikas***. Toliau analizuojant NKSC institucijų atstovams pateiktus klausimynus dėl pratybų vertinimo, galima pastebėti, kad apklausos vertinimo formatas yra pritaikytas tirti socialiniams reiškiniams, nes atsakymų pasirinkimo variantai nėra konkretūs, kas iš esmės neleidžia identifikuoti tikslių probleminių sričių. Pavyzdžiui, paklausus respondentų, kaip jie vertina teiginį, kad pasiruošimas pratyboms buvo organizuotas tinkamai, iš pateiktų atsakymų variantų („visiškai teisingai“, „labiau teisingas“, „nei teisingas, nei neteisingas“, „labiau neteisingas“, „visiškai neteisingas“) didžioji dalis pasirinko atsakymą, jog teiginys yra „labiau teisingas“, kas neatskleidžia iš esmės nieko. ***Dėl tokio pratybų vertinimo klausimyno formato, tikėtina, NKSC ir toliau turės keblumų ir iššūkių atrandant institucijų pasyvaus dalyvavimo priežastinius ryšius***. Toliau vertinant pratybų ataskaitas, buvo identifikuota, kad dalyvaujančių institucijų atstovų gretas sudarė didžiąja dalimi IT specialistai

(procentas per du metus išaugo nuo 94 iki 98). Tuo tarpu, aukščiausios vadovybės dalyvavimo procentas sumažėjo, tikėtina, dėl prieš tai minėtos priežasties – per daug techninių pratybų siužetų. Tai parodo, jog viešojo sektoriaus ***institucijose kibernetinis saugumas yra IT departamento ir jo specialistų kompetencijos laukas, kas iš esmės lemia ir institucijos veiklos procesų nesuderinamumą su kibernetinio saugumo priemonėmis. Tuo tarpu aukštesnio lygmens vadovybė, panašu, kad ir toliau nemato kibernetinio saugumo kaip prioriteto institucijos veiklos strategijoje ir darbotvarkėje, įtraukiant ir darbuotojus, kurių pareigos nėra tiesiogiai susijusius su institucijos kibernetiniu saugumu.*** Faktą sustiprinantis argumentas yra toks, jog tik 50 proc. respondentų, vienais ir kitai metais, nurodė, kad jų institucijos vadovybė palankiai žiūrėjo į kibernetinio saugumo pratybas ir sudarė tinkamas sąlygas joms pasiruošti.

Kur kas gilesnę viešojo sektoriaus IT ūkio valdymo problematiką Delfi portalui duotame interviu (Valstybinis IT ūkis žaidžia brangią ruletę, 2021) išryškino AM patarėjas Eimantas Norkūnas. Jo teigimu viešojo sektoriaus institucijos savo vidiniuose valstybės informacinių išteklių valdymo procesuose susiduria su tokiomis problemomis, kaip:

- Valstybė stipriai permoka už nereikalingomis funkcijomis apkrautą produktą dėl viešųjų pirkimų procedūrų stagnacijos: dėl decentralizuoto viešojo sektoriaus IT ūkio, institucijų specialistai naudojasi senesnių sistemų kūrimo dokumentų pavyzdžiais, juos tiesiog nukopijuodami su tikslu nerizikuoti ir gauti jau žinomą rezultatą, nepaisant to, ar jis yra tinkamiausias ir palankiausias institucijos poreikiams;
- Kuriant naujas IT sistemas, kurios iš esmės turėtų apjungti kelių institucijų veiklos procesus, susiduriama su bendradarbiavimo stoka: užsakančioji įstaiga susikoncentruoja tik į savo problemos sprendimą, o kiti dalyviai į šį procesą įtraukiami dažniausiai tik tada, kada jau sunkiai gali ką nors pakeisti;
- Į kompetencijų kėlimą investuojama labai menkai: valstybiniame sektoriuje dirba itin daug IT projektų vadovų, kurie neišmano savo pagrindinių funkcijų, o tai dažnai lemia IT priemonių nesuderinamumą su institucijos veiklos procesais, poreikiais ir pan.

Susisteminus interviu pateiktą medžiagą galima teigti, kad šie ***iššūkiai signalizuoja apie problemas, kurių sprendimas yra priklausomas būtent nuo aukštesniųjų institucijos vadovų požiūrio, kompetencijų ir supratimo apie kibernetinio saugumo rizikas, efektyvų biudžeto panaudojimą, institucijos vidinę komunikaciją, poreikį skatinti skaitmeninį brandą ir žinių kėlimo metodus bei apie kibernetinio saugumo priemonių įtraukimą į darbuotojų kasdienes veiklos funkcijas.***

Iš pateiktos viešai institucijų skelbtinos informacijos ir jos analizės galima teigti, kad LR institucijų indėlis nacionalinio kibernetinio saugumo kultūros formavime yra aiškiai įvardintas LR teisės aktuose bei pačių institucijų strateginės veiklos planuose. Visgi, panašu, kad nors LR ministerijos *de*

jure kibernetinio saugumo kultūrą savo veiklos uždaviniais, panašu, kad siekia palaikyti tiek institucijų viduje, tiek nacionaliniu lygmeniu, kuomet kalba eina apie YSII ir valstybės informacinių išteklių valdymą ir tvarkymą, tačiau *de facto* galima teigti, kad vis gi egzistuoja ne mažai probleminių sričių efektyviai kibernetinio saugumo kultūrai palaikyti. Vienos pagrindinių identifikuotų problemų yra susijusios su per menku visų LR ministerijų įtraukimu į kibernetinio saugumo valdymą nacionaliniu lygmeniu, kas iš esmės nekonstruoja vieningo ir sisteminio viso viešojo sektoriaus požiūrio į kibernetinį saugumą; su imperatyvumo trūkumu tiek nacionaliniu, tiek instituciniu lygmeniu kibernetinio saugumo mokymų ir treniruočių kontekste; su aukštesniųjų vadovų įsitraukimo į kibernetinio saugumo palaikymą institucijose stoka; su darbuotojų žinių ir kvalifikacijos stoka, kas lemia techninių ir organizacinių priemonių žemą įgyvendinimo lygį. Galiausiai, dėl vadybos stokos nėra efektyviai išnaudojamas kibernetinio saugumo palaikymui skiriamas valstybės biudžetas. Tad galima teigti, kad viešojo sektoriaus institucijų vidinės kibernetinio saugumo kultūros palaikymo problemos lemia tokią pačią problematiką ir nacionaliniu lygmeniu.

3. 4. Tyrimo gautų rezultatų interpretacija

2021 m. vasario – kovo mėn. buvo atlikta ekspertų apklausa, kurios tikslas – ištirti kibernetinio saugumo kultūros formavimo procesus ir problemas Lietuvos viešajame sektoriuje. Vienas iš uždavinių minėtam tikslui pasiekti – atskleisti kibernetinio saugumo kultūros formavimo būdus ir procesus valstybinėse institucijose, valdančiose bei tvarkančiose valstybės informacinius išteklius / atsakingose už savo sektoriaus ypatingos svarbos infrastruktūros objektus (toliau YSI objektai) ir ypatingos svarbos informacines infrastruktūras (toliau YSII). Pagrindiniai tiriamieji aspektai: vadovų indėlis (kibernetinio saugumo valdymas, darbuotojų požiūrio į kibernetinį saugumą formavimas, motyvacija integruoti kibernetinį saugumą į darbo aplinką), kibernetinio saugumo švietimas (IT saugos personalo kvalifikacijos kėlimas, mokymai darbuotojų skaitmeninei brandai ugdyti, institucijos dalyvavimas kibernetinio saugumo pratybose), bendradarbiavimas kibernetinio saugumo klausimais (bendradarbiavimo formos su viešuoju ir privačiuoju sektoriumi tiek nacionaliniu, tiek tarptautiniu lygmeniu).

Tyrime buvo numatytas 15 institucijų dalyvavimas. Kiekvieną instituciją atstovavo vienas ekspertas, kurio pareigos yra tiesiogiai susijusios su institucijos kibernetinio saugumo palaikymu ir kuris turi geriausią kompetenciją tyrimo problemai analizuoti. Kiekvienam respondentui buvo paaiškintas tyrimo tikslas bei kur ir kaip bus panaudota iš jų gauta informacija. Tyrimui buvo parinktas ekspertinis vertinimas, pasitelkiant apklausos anketavimo būdu metodą ir interviu metodą. LR ministerijų atstovams elektroniniu paštu buvo pateikta 10 klausimų (8 uždari ir 2 atviri), o NKSC atstovui – 11 atvirų klausimų. Kiekvienam ekspertui elektroniniu paštu buvo siunčiamas klausimynas ir prašoma jį užpildyti.

3. 4. 1. Lietuvos Respublikos ministerijų ekspertinio vertinimo rezultatai

Tyrimo metu siekiant atskleisti praktinę pusę, įgyvendinant kibernetinio saugumo kultūrą Lietuvos valstybinėse institucijose buvo pasirinktos LR ministerijos, formuojančios valstybės politiką pavestose valdymo srityse, taip pat pačios valdančios / tvarkančios valstybės informacinius išteklius arba atsakingos už YSI objektų ir YSII identifikavimą savo valdomuosiuose sektoriuose. Tyrime dalyvavo 11 iš 14 LR ministerijų (tyrime atsisakė dalyvauti TM, FINMIN ir SUMIN). Tyrimas atliktas taikant ekspertinio vertinimo metodą ir respondentais parenkant LR ministerijų atstovus, kurių pareigos yra tiesiogiai susijusios su kibernetiniu saugumu (ministrų patarėjai, IT departamentų direktoriai ar skyrių vedėjai).

Pirmuoju klausimu buvo ketinama nustatyti, ar ir kuo vadovaujantis, LR ministerijos įgyvendina kibernetinį saugumą institucijos viduje. Tyrimo metu atskleista, kad tik 5 iš 11 institucijų kibernetinį saugumą yra reglamentavusios pagal LR teisės aktus ir papildomas ekspertų rekomendacijas (žr. lentelę 6). Remiantis kitais atsakymais galima teigti, ***kad kibernetinis saugumas ir jo taikymo politika viešajame sektoriuje yra traktuojama dviprasmiškai:***

- ***Tai turi būti maksimaliai reglamentuota nacionalinėje kibernetinio saugumo politikoje;***
- ***Tai turi būti lanksčiai pritaikoma institucijų standartinėse veiklos procedūrose, įgyvendinant kibernetinį saugumą.***

6 lentelė. 1 klausimas: Jūsų atstovaujama institucija:

Respondentas / Atsakymas	KAM	VRM	URM	EIMIN	ENMIN	AM	SAM	KM	ŠMSM	SOCMI	ŽŪM	TM	FINMIN	SUMIN
a) *Įgyvendina kibernetinio saugumo priemones, kurios viešajam sektoriui yra reglamentuotos LR teisės aktuose;*			X				X		X	X				
b) *Turi patvirtintą institucijos kibernetinio saugumo strategiją / politiką;*						X								
c) *Turi patvirtintas standartinės veiklos procedūras, susijusias su kibernetinio saugumo įgyvendinimu organizacijoje;*			X			X					X			
d) *Visi punktai aukščiau;*	X	X		X	X			X						

e) *Kita (įvardinkite):*														

Toliau tyrime buvo vertinama kibernetinio saugumo higiena, kuri pasak respondentų yra tinkamai palaikoma tik 3 iš 11 ministerijų (žr. lentelę 7). ***Vadinasi, taikomos techninės ir organizacinės kibernetinio saugumo įgyvendinimo priemonės institucijose nėra visiškai efektyvios arba vartotojams yra suteikta per daug teisių / laisvių institucijos elektroninėje erdvėje.***

7 lentelė. 2 klausimas: Jūsų nuomone, ar atstovaujamoje institucijoje yra tinkamai palaikoma kibernetinio saugumo higiena?

Respondentas / Atsakymas	KAM	VRM	URM	EIMIN	ENMIN	AM	SAM	KM	ŠMSM	SOCMI	ŽŪM	TM	FINMIN	SUMIN
a) *Taip;*					X		X		X					
b) *Iš dalies;*	X	X	X	X		X		X		X	X			
c) *Ne.*														

Kalbant apie kibernetinio saugumo mokymus darbuotojams, svarbu pabrėžti, kad tik 2 iš 11 ministerijų jie nėra organizuojami (žr. lentelę 8). Tai reiškia, kad ***LR ministerijos atsakingai žiūrį į darbuotojų skaitmeninės brandos lygio ir bendro suvokimo į kibernetinį saugumą kėlimo poreikį, siekiant valdyti institucijos kibernetines rizikas.***

8 lentelė. 3 klausimas: Ar jūsų institucijoje yra organizuojami kibernetinio saugumo mokymai darbuotojams?

Respondentas / Atsakymas	KAM	VRM	URM	EIMIN	ENMIN	AM	SAM	KM	ŠMSM	SOCMI	ŽŪM	TM	FINMIN	SUMIN
a) *Taip;*	X	X		X	X	X	X	X		X	X			
b) *Ne.*			X						X					

Svarbu pabrėžti, kad tyrimo metu buvo siekta atskleisti ne tik kibernetinio saugumo mokymų organizavimo institucijos viduje faktą, tačiau identifikuoti ir kitas priemones, kurios paskatintų visus darbuotojus įsitraukti į kibernetinio saugumo kultūros formavimą. Anot ekspertų (7 iš 11), viena pagrindinių priemonių yra vadovų motyvacija ir lyderystė kibernetinio saugumo formavimo kontekste (žr. lentelę 9). ***Vadinasi, viešojo sektoriaus institucijose darbuotojų požiūrio į kibernetinį saugumą formavime vadovų indėlis daro didžiulę įtaką, t. y. jei vadovų požiūris yra atsainus, tokį jį perims ir kiti institucijos darbuotojai.***

9 lentelė. 4 klausimas: Kaip manote, kas paskatintų darbuotojo, kurio tiesioginės funkcijos nėra susijusios su kibernetiniu saugumu, įsitraukimą į organizacijos kibernetinio saugumo kultūros formavimą?

Respondentas / Atsakymas	KAM	VRM	URM	EIMIN	ENMIN	AM	SAM	KM	ŠMSM	SOCMI	ŽŪM	TM	FINMIN	SUMIN
a) *Vadovų motyvacija ir lyderystė šiuo klausimu;*	X	X	X	X		X	X			X				
b) *Mokymai skaitmeninei brandai didinti;*	X	X	X				X	X	X					
c) *Aiškiai organizacijos politikoje apibrėžta privalomoji kibernetinė higiena ir elgesio elektroninėje erdvėje taisyklės;*	X		X		X					X	X			
d) *Sankcijos dėl kibernetinio saugumo priemonių netaikymo;*	X		X	X										
e) *Kita (įvardinkite):*														

Deja, tačiau 7 iš 11 institucijų, nėra arba yra sudarytos tik iš dalies sąlygos kelti kvalifikaciją personalo, kurio funkcijos tiesiogiai susijusios su kibernetiniu saugumu (žr. lentelę 10). ***Vadinasi, LR ministerijose IT saugos personalas nėra nuolatos motyvuojamas bei panašu, kad ir ne visais atvejais kompetentingas, efektyviai įgyvendinti kibernetinio saugumo priemones. Galiausiai, tai skatina nekonkurencingą darbo poziciją visoje rinkoje.***

10 lentelė. 5 klausimas: Ar jūsų institucijoje yra sudarytos sąlygos kelti personalo, kurio funkcijos tiesiogiai susijusios su kibernetiniu saugumu, kvalifikaciją?

Respondentas / Atsakymas	KAM	VRM	URM	EIMIN	ENMIN	AM	SAM	KM	ŠMSM	SOCMI	ŽŪM	TM	FINMIN	SUMIN
a) *Taip;*					X		X		X		X			
b) *Iš dalies;*	X	X	X	X						X				
c) *Ne.*						X		X						

Toliau tyrime buvo nustatyta, kad beveik pusė LR ministerijų pasyviai dalyvauja kibernetinio saugumo pratybose (žr. lentelę 11). ***Taip galima teigti dėl to, jog tokio tipo pratybos, kuomet kviečiamos dalyvauti viešojo sektoriaus institucijos, nacionaliniu lygmeniu vyksta tik vieną arba du kartus į***

metus, o LR ministerijos, atsakiusios, kad dalyvauja tik dalyje pratybų tik patvirtina pastarąjį pasyvaus dalyvavimo faktą.

11 lentelė. 6 klausimas: Kaip dažnai jūsų institucija dalyvauja NKSC ar kitų institucijų organizuojamose kibernetinio saugumo pratybose?

Respondentas / Atsakymas	KAM	VRM	URM	EIMIN	ENMIN	AM	SAM	KM	ŠMSM	SOCMI	ŽŪM	TM	FINMIN	SUMIN
a) *Dalyvauja visose pratybose, į kurias yra kviečiama;*	X			X		X		X	X		X			
b) *Dalyvauja tik dalyje pratybų;*		X	X		X		X			X				
c) *Nedalyvauja.*														

Siekiant identifikuoti pasyvaus dalyvavimo kibernetinio saugumo pratybose priežastis, didžioji dalis ministerijų įvardijo, kad tokį statistinį rodiklį sąlygoja tokie pagrindiniai vidiniai veiksniai, kaip personalo, žinių ir kvalifikacijos stoka bei institucijos užimtumas (žr. lentelę 12). Svarbu pabrėžti, kad 2 institucijos įvardijo ir išorės veiksnius, galimai darančius įtaką institucijų dalyvavimui tokio tipo pratybose: pratybų kokybė, adaptacija institucijų poreikiams ir pratybų formatas, kuris nėra skirtas mokymuisi. ***Tad galima teigti, kad žemas viešojo sektoriaus institucijų dalyvavimo rodiklis kibernetinio saugumo pratybose yra priklausomas ne tik dėl institucijų vidinių priežasčių, bet ir nuo pačių pratybų organizavimo, scenarijaus bei siekinių.***

12 lentelė. 7 klausimas: Jūsų nuomone, kokios priežastys lemia žemą valstybinių institucijų dalyvavimo NKSC ar kitų institucijų organizuojamose statistinį rodiklį?

Respondentas / Atsakymas	KAM	VRM	URM	EIMIN	ENMIN	AM	SAM	KM	ŠMSM	SOCMI	ŽŪM	TM	FINMIN	SUMIN
a) *Personalo stoka;*	X		X	X			X	X	X	X				
b) *Žinių ir kvalifikacijos stoka;*	X			X	X	X		X		X				
c) *Vadybos ir motyvacijos stoka;*			X	X										
d) *Institucijos užimtumas*	X	X	X	X	X		X				X			
e) *Kita (įvardinkite):*		X	X											

Nustatyta, kad visos 11 LR ministerijų (žr. lentelę 13) bendradarbiauja kibernetinio saugumo klausimais su kitomis institucijomis ***nacionaliniu lygmeniu.*** Įvardintos bendradarbiavimo formos:

- *Konsultavimas, konsultavimasis, koordinavimas, kontroliavimas, išvadų ir siūlymų teikimas, pristatymų, kalbų, tezių pažymų rengimas (konkrečiai tik KAM);*
- *Informacijos keitimasis kibernetinio saugumo informaciniu tinklu;*
- *Bendradarbiavimas valdant kibernetinius incidentus;*
- *Nacionalinės kibernetinio saugumo pratybos;*
- *Teisės aktų projektų rengimas ir derinimas su KAM, NKSC;*
- *IT saugos/kibernetinio saugumo srities konferencijos, seminarai ir vebinarai, organizuojami valstybės institucijų ir privataus sektoriaus;*
- *Dalyvavimas Kibernetinio saugumo taryboje.*

Tačiau tik 4 LR ministerijų bendradarbiavimo formatas yra persikėlęs ir į ***tarptautinį lygmenį*** sekančiomis formomis:

- *Lietuvos atstovavimas, konsultavimasis, koordinavimas, siūlymų teikimas, pristatymų, kalbų, tezių rengimas (konkrečiai tik KAM);*
- *Bendradarbiavimas su Europos didelės apimties IT sistemų laisvės, saugumo ir teisingumo erdvėje operacijų valdymo agentūra (eu-LISA), pratybos (konkrečiai tik VRM);*
- *Konferencijos, seminarai ir vebinarai.*

Galima teigti, kad LR ministerijos nėra įstatymiškai įpareigotos, o galiausiai, tikėtina, kad dėl to ir pačios nemato poreikio tarptautiniu lygmeniu plėsti savo kibernetinio saugumo žinių lauką, keistis gerosiomis praktikomis su panašaus ar identiško tipo užsienio valstybių institucijomis.

13 lentelė. 8 klausimas: Kokias jūsų atstovaujamos institucijos bendradarbiavimo formas kibernetinio saugumo klausimais su kitomis institucijomis (tiek viešojo, tiek privataus sektoriaus) galite įvardinti?

Respondentas / Atsakymas	KAM	VRM	URM	EIMIN	ENMIN	AM	SAM	KM	ŠMSM	SOCMI	ŽŪM	TM	FINMIN	SUMIN
a) *Nacionaliniu lygmeniu;*	X	X	X	X	X	X	X	X	X	X	X			
b) *Tarptautiniu lygmeniu.*	X	X	X				X							

Remiantis ekspertiniu vertinimu, tik dvejose ministerijose yra juntamas visų lygmenų vadovų įsitraukimas į kibernetinio saugumo kultūros formavimą, tačiau konkrečių formų respondentai negalėjo įvardinti (žr. lentelę 14). ***Ekspertinis vertinimas tik paantrina autoriaus išvadą, jog viešajame sektoriuje kibernetinis saugumas yra IT departamento kompetencijoje, o jo sprendimai, tikėtina, daro įtaką ne tik visos organizacijos veiklos procesams, kas iš esmės jau yra tarpusavyje nesuderinama dėl***

skirtingų funkcinių sričių, bet ir valstybinės institucijos kibernetinio saugumo politikai nacionalinio kibernetinio saugumo kultūros formavimo kontekste.

14 lentelė. 9 klausimas: Jūsų nuomone, ar visų lygmenų vadovai yra įsitraukę į kibernetinio saugumo kultūros formavimą jūsų atstovaujamoje institucijoje? Jei taip, kokiais būdais?

Respondentas / Atsakymas	KAM	VRM	URM	EIMIN	ENMIN	AM	SAM	KM	ŠMSM	SOCMI	ŽŪM	TM	FINMIN	SUMIN
Yra					X	X								
Nėra	X	X	X	X			X	X	X	X	X			

10 klausimas: Jūsų nuomone, kokie yra pagrindiniai iššūkiai Lietuvos viešojo sektoriaus institucijoms, įgyvendinant kibernetinio saugumo kultūrą?

Susisteminus tyrimo aspektus, respondentai buvo paprašyti įvardinti pagrindinius ***iššūkius*** Lietuvos viešojo sektoriaus institucijose, įgyvendinant kibernetinį saugumą:

- **Vadybos stoka:** *„Trūksta supratimo, kad kibernetinis saugumas yra kiekvieno reikalas ir atsakomybė*; *„Reikalingas rimtas strateginis požiūris į kibernetinio saugumo reikalavimus ir priemones juos įgyvendinti.“*;
- **Žemas finansavimas:** *„Aukščiausio lygio vadovybė nemato kibernetinio saugumo palaikymo priemonių įdiegimo į veiklos procesus, kaip prioriteto.“*; *„Nekonkurencingas IT personalo atlyginimas.“*;
- **Darbuotojų žinių stoka:** *„Nepakankama darbuotojų skaitmeninė branda, kibernetinio saugumo žinios ir atsparumas socialinės inžinerijos metodų atakoms.“*;
- **Saugos personalo kompetencijos stoka:** *„IT personalo išsilavinimo ir IT kvalifikacijos kėlimo problemos.“*; *„Iššūkis yra efektyviai ir laiku identifikuoti kibernetinius incidentus, užkertant kelią jų atsiradimui ir plitimui, o vėliau ir valdant kibernetinių incidentų sukeltas pasekmes.“;*
- **Kibernetinio saugumo pareigūno etato nebuvimas:** *„Mažinant viešojo sektoriaus darbuotojų skaičių ir nemažinant funkcijų dėmesys tokioms akivaizdžiai „nematomoms“ funkcijoms kaip IT sauga tik mažėja ir mažės.“*;
- **Saugumo priemonių ir veiklos procesų derinimas:** *„Saugos stiprinimas tik „apsunkina“ IT veiklą ir reikalauja didesnių išteklių, tad tuo pačiu apsunkina ir politikų siekį „efektyviau“ tvarkytis viešajame sektoriuje.“*; *„Kas patogu nėra saugu ir atvirkščiai.“*;
- **Rinkos pasiūla kibernetinio saugumo priemonėms:** *„Itin brangios ir ne visada kokybiškos IT srities paslaugos rinkoje (kainos ir kokybės santykis dažnai liūdina).“*.

3.4.2. Nacionalinio kibernetinio saugumo centro ekspertinio vertinimo rezultatai

Siekiant identifikuoti priežastinius ryšius ir iššūkius viešajame sektoriuje, formuojant ir įgyvendinant kibernetinio saugumo kultūrą, ekspertiniam interviu atlikti buvo parinktas Nacionalinio kibernetinio saugumo centro (toliau – NKSC) Kibernetinio saugumo valdymo departamento atstovas. Ekspertinis vertinimas padėjo identifikuoti ir patvirtinti tyrimo problemines sritis, kibernetinio saugumo kultūros formavimo iššūkius Lietuvos viešajame sektoriuje.

Reflektuojant eksperto interviu rezultatus buvo nustatyta, kad į institucijos kibernetinio saugumo strategijos kūrimą ir politikos formavimą turi įsitraukti visi darbuotojai, siekiant efektyvaus politikos įgyvendinimo praktikoje bei bendro rizikų paveikslo atvaizdavimo organizacijos viduje: *Vadovaujantis LR teisės aktais, kibernetinio saugumo subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojai suderinę su Nacionaliniu kibernetinio saugumo centru, tvirtina kibernetinio saugumo politikos ir jos įgyvendinimo dokumentus. Kaip manote, ar visi institucijos darbuotojai turėtų būti skatinami dalyvauti rengiant kibernetinio saugumo politiką, siekiant efektyvaus politikos įgyvendinimo praktikoje ar visgi tik tie darbuotojai, kurių funkcijos yra tiesiogiai susijusios su kibernetiniu saugumu?* Atsakymas: ***„Kibernetinio saugumo politikos formavimas apima procesų apibrėžimą ir jų įgyvendinimą. Procesų apibrėžimas yra susijęs su LR teisės aktuose nustatyta kibernetinio saugumo politika, informacijos saugumo standartais, kurių reglamentavimas reikalauja specifinių žinių bei įgūdžių. Tačiau efektyvi kibernetinio saugumo politika turi tiesiogiai sietis su organizacijos priimtinomis rizikomis, kas yra per se susiję su visos organizacijos darbuotojų veikla. Dėl šios priežasties yra svarbu įtraukti darbuotojus, gebančius identifikuoti organizacijoje veikiančius procesus, darbuotojų vykdomas funkcijas, nes tik tokiu būtų galima identifikuoti kibernetinio saugumo rizikas, jų įtaką, bei būtinąsias kibernetinio saugumo kontrolės priemones.”***

Toliau buvo nustatyta, kad yra būtinas visų lygmenų institucijos vadovų indėlis kibernetinio saugumo kultūros formavimo kontekste, siekiant optimizuoti institucijos veiklos procesus, juos susiejant su kibernetinio saugumo rizikomis ir jų mažinimui dedikuotomis techninėmis ir organizacinėmis priemonėmis. Ekspertas patvirtina, kad kibernetinis saugumas neturėtų būti tik IT departamento / skyriaus reikalas, norint efektyvios kibernetinio saugumo politikos organizacijoje: *Jūsų nuomone, ar visų lygmenų vadovai turėtų įsitraukti į kibernetinio saugumo kultūros formavimą valstybinėse institucijose? Ar sutinkate, kad kibernetinis saugumas yra dažnai įvardijamas kaip IT departamento reikalas?* Atsakymas: ***„Vadovai turėtų įsitraukti pagal kompetenciją įvertindami, kokią informaciją valdo, koks būtų informacijos praradimo poveikis, kokias priemones taiko informacijai apsaugoti. Pagal šiuos kriterijus vadovai turėtų įsitraukti į kibernetinio saugumo kultūros formavimą, nes kitu atveju kibernetinio saugumo kontrolės priemonės gali suvaržyti veiklos procesus. Tenka nuogąstauti, kad vis dar yra gajus požiūris kibernetinio saugumo klausimus priskirti pavieniams IT specialistams***

ar IT struktūriniams padaliniams, neįtraukiant kitų organizacijos darbuotojų neva dėl nereglamentuotų atsakomybių arba žinių bei įgūdžių trūkumo. Tokiu atveju dažnai yra sukuriamas pretekstas galimam interesų konfliktui, kada IT padalinyje už kibernetinį saugumą atsakingas asmuo turi koordinuoti kolegų arba tiesioginio vadovo veiklas arba šios veiklos trūkumus. Dar daugiau, dažnai pavieniai IT specialistai nežino visa apimančių organizacijos procesų, todėl negeba įvertinti taikomų rizikos kontrolės priemonių proporcingumo ir efektyvumo kriterijų.“

Kibernetinio saugumo higienos lygis viešajame sektoriuje yra vertinamas dvejopai, t. y. panašu, jog ne visos valstybinės institucijos yra oficialiai įteisinusios valdomas informacines sistemas, dėl ko kibernetinė higiena yra neįtraukta į veiklos prioritetų sąrašą, o jos lygis gali stipriai keistis nuo kitų viešojo sektoriaus institucijų, kurių valstybės informacinių išteklių, YSII valdymas ir tvarkymas yra teisiškai reglamentuotas ar oficialiai įformintas. Vadinasi, viešajame sektoriuje nėra bendrinės, privalomos ar minimalius kibernetinės higienos reikalavimus atitinkančios sistemos, todėl negalima atlikti sisteminio viešojo sektoriaus kibernetinės higienos lygio vertinimo: *Kaip vertinate valstybinių institucijų, valdančių ar tvarkančių valstybės informacinius išteklius ar YSII kibernetinio saugumo higienos lygį? Jūsų manymu, kokie pagrindiniai veiksniai jį lemią?* Atsakymas: ***„Kibernetinio saugumo sąmoningumo lygis tiesiogiai koreliuoja su žiniomis, įgūdžiais, bei jų lavinimu. YSII valdantys subjektai, arba ypatingos svarbos valstybės informacinius išteklius valdančios organizacijos turi aukštesnį kibernetinio saugumo sąmoningumo lygį dėl aiškių atsakomybių, periodiško mokymų organizavimo. Valstybinės institucijos neįsiteisinusios informacinių sistemų arba tą padarę formaliai – dažniausiai turi nepakankamą kibernetinio saugumo lygį. Pagrindiniai tai lemiantys veiksniai – ne gebėjimas identifikuoti kibernetinių incidentų, nesupratimas kibernetinių incidentų poveikio, nežinojimas kokie įvykiai vyksta ryšių ir informacinėse sistemose, nepakankamas darbuotojų įsitraukimas informacijos saugumo klausimų tema.”***

Toliau interviu metu buvo nustatyta, kad ne visose viešojo sektoriaus institucijose, valdančiose ar tvarkančiose valstybės informacinius išteklius ar YSII, yra vykdomi kibernetinio saugumo mokymai. Tuo tarpu pačioms institucijoms yra organizuojami mokymai / pratybos iš išorės – NKSC – kuris pratybų metu siekia treniruoti tokio tipo institucijas kibernetinių incidentų valdymo tema. Visgi ekspertas patvirtina faktą, jog mokymai privalo būti organizuojami ir institucijų viduje, pritraukiant jų formas ir metodus arčiau savo institucijos veiklos specifikos ir poreikių: *Kaip manote ar visose valstybinėse institucijose, valdančiose ar tvarkančiose valstybės informacinius išteklius ar YSII, yra organizuojami kibernetinio saugumo mokymai? Ar galėtumėte įvardinti pagrindines (jums žinomas) tokių mokymų pateikimo formas, būdus Lietuvos viešajame sektoriuje? Jūsų vertinimu, ar jie yra efektyvūs?* Atsakymas: ***„Ne visose. Viena iš pagrindinių formų – kasmetinės NKSC organizuojamos pratybos „Kibernetinis skydas” kada YSII ir VII organizacijos kviečiamos peržaisti incidentų valdymo procedūras. NKSC taip pat organizuoja atskirus mokymus organizacijoms, privataus sektoriaus***

organizacijos taip pat teikia tokio pobūdžio paslaugas. Mokymai dažniausiai apima incidentų simuliacijas, medžiagos pateikimą. NKSC vertinimu, organizacijos pačios turėtų daugiau dėti pastangų mokydamos savo darbuotojus, nes kibernetinių incidentų patirtys rodo, kad dažniausiai incidentų priežastimi būna nesudėtingi kibernetinių incidentų vektoriai, orientuoti į naudotojų sąmoningumo stoką.“; *NKSC yra pagrindinė institucija Lietuvoje, organizuojanti kibernetinio saugumo pratybas. Kaip vertinate jų adaptaciją valstybinių institucijų poreikiams, vykdomai veiklai? Kaip manote, ar dabartinis pratybų skaičius per metus yra pakankamas formuoti kibernetinio saugumo kultūrą nacionaliniu lygmeniu?* Atsakymas: ***„NKSC organizuojamos pratybos yra susijusios su kibernetinių incidentų valdymo procedūromis, jos vykdomos kartą per metus. Tačiau organizacijose kibernetinio saugumo kultūrai suformuoti yra reikalingos dažnesnės vidinės pratybos, įtraukiančios visus darbuotojus.“***

Taip pat svarbu išskirti, kad eksperto vertinimu, kibernetinio saugumo mokymai ne tik skatina institucijos veiklos procesų tęstinumą kibernetinių grėsmių kontekste, bet ir kelia bendrą organizacijos sąmoningumo lygį, skatina visų darbuotojų įsitraukimą į rizikų valdymą ir efektyvų kibernetinio saugumo užtikrinimą: *Kaip manote, kas paskatintų darbuotojo, kurio tiesioginės funkcijos nėra susijusios su kibernetiniu saugumu, įsitraukimą į organizacijos kibernetinio saugumo kultūros formavimą?* Atsakymas: ***„Bazinių žinių suteikimas, situacijos sugrėsminimas (grėsmės, jų valdymo būdai, rizikos valdymo procesas).“***

Toliau buvo nustatyta, kad aukščiau įvardintos probleminės sritys ir žinių bei kvalifikacijos kėlimo institucijų viduje stoka, galimai prisideda ir prie žemo valstybinių institucijų įsitraukimo į NKSC organizuojamas pratybas statistinio rodiklio. Galima teigti, kad tai atspindi ne tik kibernetinių incidentų poveikio nuvertinimą, bet tuo pačiu ir institucijų abejingumą, formuojant kibernetinio saugumo kultūrą nacionaliniu lygmeniu: *Jūsų nuomone, kokios priežastys lemia žemą valstybinių institucijų dalyvavimo NKSC organizuojamose pratybose statistinį rodiklį?* Atsakymas: ***„Nepakankamas dalyvavimo skaičius susijęs su kibernetinių incidentų poveikio nuvertinimu.”***

Būtina pabrėžti, kad interviu metu buvo identifikuoti priežastiniai ryšiai dėl LR viešojo sektoriaus IT personalo kvalifikacijos kėlimui skiriamo finansavimo ne proporcingumo valdomų ar tvarkomų valstybės informacinių išteklių kibernetinėms rizikoms nacionalinio saugumo kontekste. Finansavimo stokos faktas buvo patvirtintas, tačiau svarbiausia, nurodyta ir visai kita šios problemos egzistavimo priežastis – institucijų ne gebėjimas pagrįsti kibernetinio saugumo įgyvendinimo priemonių poreikio: *Kaip vertinate LR viešajam sektoriui skiriamą finansavimą kvalifikacijos kėlimui personalo, kurio funkcijos tiesiogiai susijusios su kibernetiniu saugumu? Ar sutinkate, kad skiriamas finansavimas nėra proporcingas valdomų ar tvarkomų valstybės informacinių išteklių kibernetinėms rizikoms nacionalinio saugumo kontekste?* Atsakymas: ***„Finansavimas neproporcingas, tačiau tai taip pat yra susiję su organizacijų ne gebėjimu pagrįsti tokių išteklių reikalingumo.“***

Identifikuojant LR viešojo sektoriaus bendradarbiavimo kibernetinio saugumo klausimais formas su kitomis valstybinėmis institucijomis ir privataus sektoriaus organizacijomis, buvo nustatyta, kad bendradarbiavimas yra vykdomas tiek nacionaliniu, tiek tarptautiniu lygmeniu: *Kokias LR viešojo sektoriaus bendradarbiavimo formas su kitomis organizacijomis (tiek viešojo, tiek privataus sektoriaus) galite įvardinti?* Atsakymas: ***„Nacionaliniu lygmeniu – – pratybos, mokymai, konferencijos – ESET, ATEA, NRDCS, Kauno kolegija, Santa Monica, NKSC „Kibernetinis skydas", kiekvieną ketvirtį NKSC organizuojami kibernetinio saugumo pusryčiai su Kibernetinio saugumo subjektais (įskaitant YSII valdytojus, viešojo sektoriaus organizacijas). Tarptautiniu lygmeniu – pratybos, mokymai, konferencijos – ENISA, EU NIS Cooperation group, NATO ENSECCOE, CCDCOE."***

Susisteminant prieš tai atsakytus klausimus, anot NKSC atstovo, pagrindinis iššūkis Lietuvos viešojo sektoriaus institucijoms, įgyvendinant kibernetinio saugumo kultūrą yra žinių, įgūdžių ir sąmoningumo stoka*: Jūsų nuomone, kokie yra pagrindiniai iššūkiai Lietuvos viešojo sektoriaus institucijoms, įgyvendinant kibernetinio saugumo kultūrą?* Atsakymas: ***„Žinių, įgūdžių, sąmoningumo stoka."*** Tuo tarpu paklausus apie LR kibernetinio saugumo teisinio reglamentavimo įgyvendinimą ir jo pritaikomumą valstybinėse institucijose, eksperto teigimu pagrindinis efektyvios kibernetinio saugumo kultūros formavimą lemiantis dokumentas yra Nacionalinė kibernetinio saugumo strategija, kurią yra reikalinga atnaujinti: *Kaip manote, ar LR teisės aktuose kibernetinio saugumo priemonės yra pakankamos ir įpareigojančios visas viešojo sektoriaus institucijas jas integruoti, formuojant kibernetinio saugumo kultūrą? Jei ne, ką jūsų nuomonę reikėtų keisti, norint sukurti efektyvų kibernetinio saugumo kultūros įgyvendinimo modelį viešajame sektoriuje?* Atsakymas: ***„Norint turėti efektyvų kibernetinio saugumo kultūros įgyvendinimo modelį reikėtų atnaujinti Kibernetinio saugumo strategiją."***

NKSC ekspertinio vertinimo metu nustatyta, kad kibernetinio saugumo kultūra viešajame sektoriuje yra būtina. Eksperto teiginiai koreliuoja su tyrimo autoriaus atliktomis analizėmis bei atskleidžia priežastinius ryšius ir pagrindinius iššūkius, darančius įtaką viešojo sektoriaus institucijų kibernetinio saugumo kultūros įgyvendinimo praktikoje. NKSC eksperto vertinimas padės suformuluoti siūlymus ir rekomendacijas Lietuvos viešojo sektoriaus institucijų kibernetinio saugumo kultūros palaikymo problematikai spręsti.

Taigi apibendrinant tyrimo rezultatus, buvo atskleista, kad Lietuvos viešasis sektorius, formuodamas kibernetinio saugumo kultūrą, susiduria su kur kas daugiau problemų, nei yra viešai žinoma. Todėl siekiant efektyvaus kibernetinio saugumo kultūros įgyvendinimo, ***kiekvienai problemai yra siūlomas sekantis sprendimo būdas***:

- ***Vadybos stoka*** – norint skatinti visų lygmenų vadovų įsitraukimą į institucijos kibernetinio saugumo kultūros formavimą yra būtina organizuoti tiek nacionalinio, tiek sektorinio ar institucinio

lygmens mokymus, seminarus bei kitokio pobūdžio šviečiamąsias veiklas konkrečiai vadovams, siekiant kelti jų žinias bei skatinti skaitmeninę brandą kibernetinio saugumo klausimais. Čia taip pat padėtų ir praktinio pobūdžio mokymai, kurių metu būtų suteiktos galimybės institucijų vadovams organizaciniu lygmeniu taikyti kibernetinio saugumo rizikų mažinimo priemones, pavyzdžiui, institucijos veiklos procesų derinimą su kibernetinio saugumo priemonėmis, taip pat kaip motyvuoti darbuotojus susidraugauti su kibernetine higiena, ar kaip visų lygmenų vadovams komunikuoti su IT skyriumi, siekiant institucijos veiklos tęstinumo kibernetinių grėsmių kontekste. Vienas iš siūlymų būtų nacionalinių kibernetinio saugumo pratybų „Kibernetinis skydas“ siužeto linijų išplėtimas, įtraukiant daugiau reikalaujančių institucijų organizacinių priemonių taikymo siužetų, kuomet IT skyrius nebėra kompetentingas priimti sprendimų kibernetinių grėsmių ir rizikų kontekste. Tai tikėtina paskatintų vadovybės indėlį strategiškai pažvelgti į kibernetinį saugumą ir suprasti, kad kibernetinės erdvės saugumą kuria visi organizacijos darbuotojai. Taip pat derėtų į darbuotojų pareiginius nuostatus įtraukti kibernetinio saugumo priemonių taikymą ir darbuotojo nešamą atsakomybę, kuomet minimali kibernetinio saugumo higiena nėra integruojama į jo kasdienių funkcijų vykdymą.

- ***Žemas finansavimas ir rinkos pasiūla kibernetinio saugumo priemonėms*** – svarbu suprasti, kad valstybės biudžetas yra ribotas, o tai reiškia, kad skiriamą finansavimą institucijų kibernetinio saugumo palaikymui dažniausiai yra maža tikimybė padidinti. Tačiau sprendimo būdų šiai opiai problemai mažinti yra. Visų pirma, konstatuojant faktą, kad institucijos dažnai nemoka pagrįsti poreikio kibernetinio saugumo sprendimams įsigyti, reikėtų pradėti nuo svarių argumentų pateikimo institucijos vadovybei, kurie neturėtų apimti tik techninio kibernetinio saugumo profilio, tačiau turėtų atspindėti ir galutinį rezultatą, susijusį su institucijos veiklos saugumu elektroninėje erdvėje, su sistemų funkcionalumu ir darbuotojų aplinkos gerinimu. Visų antra, labai svarbu diskutuoti ir apie viešųjų pirkimų procedūras, kurios panašu, yra per daug miglotos ir nederinamos su ekonominio naudingumo rodikliu. Ši problema turėtų būti sprendžiama nacionaliniu lygmeniu, koreguojant viešųjų pirkimo tvarką, taip skatinant ne tik inovacijas įsigyjant techninius sprendimus, bet ir kibernetinio atsparumo didinimą progresuojančių kibernetinių grėsmių kontekste. Taip pat turi būti nuolatos įvertinama galimybė naudoti daugiau atvirojo kodo programinės įrangos, kuri labai dažnai atitinka ir mokamos įrangos funkcionalumą, kas dar labiau padėtų efektyviau įsisavinti valstybės skiriamą limituotą biudžetą.

- ***Personalo kvalifikacijos ir žinių stoka*** – šiai problemai spręsti, panašu, kad visų pirma trūksta nacionalinio lygmens sprendimų. LR teisinėje bazėje nėra institucijoms įpareigojimo organizuoti mokymų, susijusių su personalo kvalifikacijos ir žinių kėlimu, dalyvauti nacionalinėse kibernetinio saugumo pratybose ar kitose panašaus pobūdžio veiklose. Taip pat panašu, kad valstybinių institucijų IT saugos personalui yra taikomi per maži kvalifikaciniai standartai, dėl ko ir nėra sudaromos sąlygos pastarosioms kompetencijoms įgyti. Kibernetinio saugumo švietimas nacionaliniu lygmeniu turėtų būti imperatyvus. Pavyzdžiui, KAM, kaip pagrindinė kibernetinio saugumo švietimą skatinanti institucija

turėtų teikti LR Vyriausybei siūlymą, griežtinti institucijų dalyvavimą nacionalinėse kibernetinio saugumo pratybose, įgyvendinant tai kaip privalomąjį teisės akto punktą, o taip pat ir įvedant institucijoms sankcijas dėl šviečiamosios veiklos vengimo. Taip pat, siekiant skatinti kibernetinio saugumo švietimą nacionaliniu lygmeniu, būtina didinti nacionalinių kibernetinio saugumo pratybų metinį skaičių ir į jų planavimą įtraukti visas LR ministerijas, kad pratybų scenarijus atitiktų visų institucijų poreikius ir pageidaujamą mokymosi formatą.

- ***Kibernetinio saugumo pareigūno etato nebuvimas*** – tyrimo metu buvo identifikuota, kad LR ministerijų struktūrose nėra kibernetinio saugumo pareigūno etato, todėl kibernetinio saugumo politika dažnai yra atsainiai įgyvendinama ir kontroliuojama. Vadinasi, LR Vyriausybė turi priimti sprendimą ir persvarstyti galimybę institucijų viduje turėti ne atsakingą asmenį, kuriam kibernetinio saugumo politikos įgyvendinimo kontrolė būtų tik kaip papildoma funkcija, bet atskirą etatą, kuomet darbuotojas būtų pilnai atskaitingas ir galėtų efektyviai skatinti kibernetinio saugumo kultūrą institucijų viduje bei nacionaliniu lygmeniu, dalyvaujant įvairių tarybų veikloje, taip pat būtų kertinis tarpininkas tarp aukščiausios vadovybės ir IT vadovo, kuomet reikalingas kibernetinio saugumo priemonių integravimas į institucijos veiklos procesus. Todėl šios problemos sprendimas, tikėtina, išspręstų ir identifikuotą saugos priemonių ir veiklos procesų derinimo problematiką.

- ***Bendradarbiavimo kibernetinio saugumo klausimais stoka*** – nors institucijos šios srities neįvardino kaip probleminės, tačiau atliekant dokumentų turinio analizę atskleista, kad reikalingas strateginis institucijų bendradarbiavimo kibernetinio saugumo klausimais sprendimas. Visų pirma, siekiant vieningo kibernetinio saugumo kultūros formavimo ir įgyvendinimo valstybės kritinės svarbos sektoriuose, Kibernetinio saugumo Tarybos veikloje turėtų dalyvauti visų LR ministerijų atstovai. Be visa to, tarptautinio bendradarbiavimo formos LR teisės aktuose neturėtų būti įvardintos tik 3 ministerijoms, siekiant paskatinti visas LR ministerijas dalintis / perimti gerąsias kibernetinio saugumo praktikas iš to paties sektoriaus užsienio šalių institucijų. Todėl labai svarbu būtų tiek Vyriausybei, tiek KAM, persvarstyti LR teisinėje bazėje reglamentavimo poreikį formalaus bei neformalaus bendradarbiavimo kibernetinio saugumo klausimais tiek nacionaliniu, tiek tarptautiniu lygmeniu.

- ***Pasyvus Nacionalinės kibernetinio saugumo strategijos atnaujinimo procesas*** – tyrimo metu buvo nustatyta, kad pagrindinės kibernetinio saugumo įgyvendinimo gairės ir LR kibernetinio saugumo teisinio įgyvendinimo pagrindas yra Nacionalinė kibernetinio saugumo strategija. Pagal Europos Sąjungos reikalavimus, valstybių kibernetinio saugumo strategijos yra rengiamos penkeriems metams. Tačiau Strategijos punktai, tam tikri tikslai ar kita svarbi informacija gali būti atnaujinama ir dažniau. Visgi panašu, kad Strategijoje nėra per 3 metus atliktų esminių pokyčių. Todėl siūlymas būtų išplėsti kibernetinio saugumo kultūros sąvoką ir jos formavimą sąlygojančių priemonių taikymą tiek kibernetinio saugumo subjektuose, tiek valstybiniu lygmeniu, neapsiribojant tik švietimo ir inovacijų

plėtra, tačiau integruojant kitų faktorių tarpusavio priklausomybę, pavyzdžiui, vadovavimo ir valdymo skatinimo poreikį siekiant strategijos tikslų pasiekimo efektyvumo.

IŠVADOS

1. Išanalizavus kibernetinio saugumo kultūros, kaip reiškinio, raidos istoriją, paaiškėjo, jog pati sąvoka kilo iš informacinio saugumo kultūros koncepcijos, t. y. organizacijos informacinio saugumo kultūros konceptualizavimui taikytas trijų pagrindinių sluoksnių mechanizmas (tylių prielaidų, vertybių ir artefaktų) buvo išplėstas iki keturių, pridėjus ***žinių sluoksnį***, kuris leidžia kultūrai vystytis natūraliai. Nepaisant to, jog akademinėje bendruomenėje kibernetinio saugumo kultūra yra dažnai interpretuojama subjektyviai arba neinformatyviai kibernetinio saugumo kultūrą galima apibrėžti, kaip ***žinių, įsitikinimų, darbuotojų suvokimo, bei organizacijoje taikomų normų ir vertybių apie kibernetinį saugumą visumą, kuri atsiskleidžia ir pasireiškia žmonių elgesiu elektroninėje erdvėje.*** Visgi, nors kibernetinis saugumas ir jo palaikymo priemonės, remiantis pasauline patirtimi, turėtų būti vienodos visose organizacijose, tyrime buvo atskleista, kad viešojo sektoriaus institucijų kibernetinio saugumo kultūros formavimo ypatumai dažnai gali skirtis dėl tokio tipo organizacijas lydinčių aplinkybių: reikšmės valstybės nacionaliniam saugumui, politinės įtakos, kaštų, teisinio reglamentavimo bei taikomų organizacinių ir techninių priemonių reikalavimų. Todėl darbe sukonstruotas teorinis modelis, kurio pagrindiniai kriterijai yra strategijos kūrimas ir politikos formavimas, vadovavimas ir valdymas kibernetinio saugumo higienos palaikymas, kibernetinio saugumo švietimas bei bendradarbiavimas kibernetinio saugumo klausimais, įgalina kibernetinio saugumo kultūrą viešojo sektoriaus organizacijose ir leidžia įvertinti jos formavimo ypatumų ir problemų koreliaciją su nacionaliniu saugumu bei jam daromą įtaką.

2. Atlikta Lietuvos kibernetinį saugumą reglamentuojančių dokumentų turinio analizė atskleidė, jog ***Lietuvoje kibernetinio saugumo kultūra, kaip reiškinys, yra įvardintas tik iš kibernetinio saugumo švietimo ir inovacijų prizmės*, *o tuo tarpu kiti kibernetinio saugumo kultūros formavimui reikalingi aspektai yra LR teisinėje bazėje reglamentuoti atskirai ir nesiejami tarpusavyje.*** Visgi pagrindinis dėmesys yra skiriamas valstybės informacinių išteklių ir YSII valdymo bei tvarkymo procedūroms nustatyti, kas leidžia teigti, jog Lietuvos kibernetinį saugumą reglamentuojantys teisės aktai yra dedikuoti labiau techninių ir organizacinių reikalavimų nustatymui, nepriklausomai nuo to, jog jų įgyvendinimui didžiulę įtaką daro ***teisinėje bazėje pasigendami švietimo, vadybos ir bendradarbiavimo sferų baigtiniai, imperatyvūs ir visas LR ministerijas bei pavaldžius kibernetinio saugumo subjektus įpareigojantys reikalavimai.*** Dėl šios priežasties nacionalinė kibernetinio saugumo kultūra stipriai priklauso nuo kibernetinio saugumo subjektų, šiuo atveju viešojo sektoriaus institucijų, vidinės kibernetinio saugumo kultūros ir jos palaikymui taikomų priemonių interpretacijos.

3. Atlikus LR ministerijų ir NKSC ekspertinio vertinimo bei viešai prieinamų pastarųjų institucijų duomenų analizę, identifikuoti procesai liudija, kad ***LR ministerijos yra nacionalinio saugumo stiprinimo paveikslo dalis dėl jų valdomos ir tvarkomos valstybės informacinės infrastruktūros, joje saugomų ir apdorojamų jautrių asmens duomenų ir kitos valstybinės reikšmės informacijos.*** Nors

valstybės informacinių išteklių ir YSII kibernetinis saugumas bei gynyba, kaip strateginiai prioritetai ir neatsiejama nacionalinio saugumo palaikymo priemonė, yra įvardijami didžiąja dalimi NKSC kompetencijos ribose, visgi, konstatuojant faktą, kad dauguma LR ministerijų yra kritinės svarbos informacinių sistemų ir registrų valdytojos, galima teigti, kad pastarųjų sistemų kibernetinio saugumo praktinis palaikymas ir LR teisės aktuose nustatytų reikalavimų atitikimas yra ne kieno kito, bet valdytojų, t. y. LR ministerijų pareiga. Kalbant apie problemas, su kuriomis susiduria viešojo sektoriaus institucijos, įgyvendindamos veiklos procesus, susijusius su valstybės informacinės infrastruktūros kibernetiniu saugumu ir efektyvios kibernetinio saugumo kultūros formavimu, tyrimas atskleidė, kad ***pagrindinės problemos yra: vadybos stoka, žemas finansavimas, kvalifikacijos ir žinių stoka, kibernetinio saugumo pareigūno etato nebuvimas, bendradarbiavimo kibernetinio saugumo klausimais stoka bei pasyvus Nacionalinės kibernetinio saugumo strategijos atnaujinimo procesas.*** Todėl tyrime iškelta ***hipotezė***, jog kibernetinio saugumo kultūros formavimo neefektyvumą Lietuvos viešajame sektoriuje lemia vadybos stoka, ***pasitvirtina tik iš dalies***.

4. **Siekiant mažinti viešojo sektoriaus kibernetinio saugumo kultūros formavimo problematiką, siūlymai yra sekantys:**

1) Organizuoti institucijų visų lygmenų vadovams kibernetinio saugumo mokymus su tikslu kelti jų savimonę kibernetinio saugumo taikymo srityje;

2) Išplėsti nacionalinių kibernetinio saugumo pratybų „Kibernetinis skydas“ siužeto linijų sąrašą, įtraukiant daugiau organizacinių priemonių taikymo reikalaujančių siužetų, kuomet IT skyrius nebėra kompetentingas priimti sprendimų ir yra reikalingas vadovų strateginis įsitraukimas;

3) Į darbuotojų pareiginius nuostatus įtraukti kibernetinio saugumo priemonių taikymą ir darbuotojo nešamą atsakomybę, siekiant valdyti kibernetines rizikas;

4) IT vadovams teikti ir formuluoti svarius, kibernetinio saugumo priemonių poreikį pagrindžiančius argumentus aukštesniųjų vadovų sluoksniui, siekiant pabrėžti teigiamą įtaką institucijos veiklos procesams;

5) Inicijuoti viešųjų pirkimų procedūrų pakeitimus, siekiant įvesti ekonominio naudingumo faktorių;

6) Dažniau persvarstyti atvirojo kodo programinės įrangos integravimo galimybes;

7) KAM, kaip pagrindinei kibernetinio saugumo švietimą skatinančiai institucijai, teikti siūlymą LR Vyriausybei dėl ministerijų ir pavaldžių įstaigų dalyvavimo nacionalinėse kibernetinio saugumo pratybose griežtinimo bei sankcijų įvedimo;

8) Didinti nacionalinių kibernetinio saugumo pratybų metinį skaičių;

9) Svarstyti apie galimybę įsteigti kibernetinio saugumo pareigūno etatą LR ministerijų struktūrose;

10) Išplėsti Kibernetinio saugumo tarybą, įtraukiant visas LR ministerijas;

11) Reglamentuoti tarptautinį bendradarbiavimą kibernetinio saugumo klausimais, įpareigojant visas LR ministerijas dalyvauti gerųjų praktikų pasidalinimo su identiško ar panašaus tipo užsienio šalių institucijomis;

12) Nuolatos atnaujinti Nacionalinę kibernetinio saugumo strategiją, jos pakeitimus susiejant su kibernetinio saugumo kultūros formavimo procesais, t. y. jei yra probleminių sričių indikacija, tų problemų sprendimo variantas turi būti pateiktas strategijoje;

13) Išplėsti kibernetinio saugumo kultūros sąvoką ir jos formavimą sąlygojančių priemonių taikymą Nacionalinėje kibernetinio saugumo strategijoje, neapsiribojant tik švietimo ir inovacijų plėtra.

LITERATŪROS SĄRAŠAS

1. Augustinaitis A., Rudzkienė V., Petrauskas R. A. ir kiti. (2009). *Kolektyvinė monografija: Lietuvos e. valdžios gairės: ateities įžvalgų tyrimas.* Vilnius: Mykolo Romerio universitetas.
2. Ashenden D. (2008). Information Security management: A human challenge? *Information Security Technical Report,* 13, 195-201.
3. Ashenden D., Sasse A. (2013). CISOs and organizational culture: Their own worst enemy? *Computers & Security,* 39, 396-405.
4. Barton K.A., Tejay G., Lane M., Terrell, S. (2016). Information system security commitment: A study of external influences on senior management. *Computers & Security,* 59, 9-25.
5. Brook C. (2020, spalio 6). What is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best Practices, and More. *Data Insider: Data Protection 101*. Prieiga per internetą: https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more.
6. Choi J., Nazareth D. L. (2015). A system dynamics model for information security management. Information *& Management,* 52, 123-134.
7. Cone W. D., Irvine C. E., Thompson M. F., Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers & Security*, 26, 63-72.
8. Eminagaoglu M., Ucar E., Eren, S. (2009). The positive outcomes of information security awareness training in companies – A case study. *Information Security Technical Report,* 14, 223-229.
9. ENISA (2016). *Review of Cyber Hygiene practices.* Prieiga per internetą: https://www.enisa.europa.eu/publications/cyber-hygiene.
10. ENISA (2017). *Cyber Security Culture in organisations,* EU. Prieiga per internetą: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations.
11. Flores W.R., Antonsen E., Ekstedt M. (2014). Information security knowledge sharing in organizations: investigating the effect of behavioral information security governance and national culture. *Computers & Security,* 43, 90-110.
12. Fruhlinger J. (2020). What is information security? Definition, principles, and jobs. *CSO Online.* Prieiga per internetą: https://www.csoonline.com/article/3513899/what-is-information-security-definition-principles-and-jobs.html.
13. Harkins R., English E. (2018). Guarding the Public Sector: Seven Ways State Governments Can Boost Their Cybersecurity. *Marsh & Mclennan Companies*. Prieiga per internetą: https://www.mmc.com/insights/publications/2018/oct/guarding-the-public-sector--seven-ways-state-governments-can-boo.html.

14. Hatch M. J. (1993). The dynamics of organizational culture. *The Academy of Management Review*, 18, 657-693.
15. Hedstrom K., Kolkowska E., Karlsson F., Allen J.P. (2011). Value conflicts for information security management. *Journal of Strategic Information Systems*, 20, 373-384.
16. IT Security Specialist – Information Technology (2021, kovo 23). *Paylab*. Prieiga per internetą: https://www.paylab.com/report/professional/it-security-specialist/information-technology/lithuania/98d76b7870aecd50d307b347e63da74bb45c7eb4.
17. Yeager J. (2020, lapkričio 9). With transition coming, what lessons can public and private sector organizations share on cybersecurity? *FedScoop*. Prieiga per internetą: https://www.fedscoop.com/transition-coming-lessons-can-public-private-sector-organizations-share-cybersecurity.
18. Ypatingos svarbos informacinės infrastruktūros identifikavimo metodika (2018). Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/e16e7761fc4b11e89b04a534c5aaf5ce.
19. Jurkonienė I. ir Karčiauskienė R. (2017). *Tarpinstitucinio bendradarbiavimo stiprinimo koncepcija*. Prieiga per internetą: http://kurklt.lt/wp-content/uploads/2016/10/tarpinstitucinio-bendradarbiavimostiprinimo-koncepcija-final.pdf.
20. KAM (2018). *Nacionalinio kibernetinio saugumo būklės vertinimo ataskaita*. Prieiga per internetą: https://www.nksc.lt/doc/NKSC_ataskaita_2018.pdf.
21. KAM (2019). *Nacionalinio kibernetinio saugumo būklės vertinimo ataskaita*. Prieiga per internetą:https://www.nksc.lt/doc/Nacionalinio_kibernetinio_saugumo_bukles_ataskaita_2019.pdf.
22. KAM (2020). *Nacionalinio kibernetinio saugumo būklės vertinimo ataskaita*. Prieiga per internetą:https://www.nksc.lt/doc/nacionalinio_kibernetinio_saugumo_bukles_ataskaita_2020.pdf.
23. Karlsson F., Hedstrom K. (2014). End User Development and Information Security Culture., *Springer*, 246–257.
24. Kearney P. (2010). *Security: The Human Factor*. United Kingdom, Cambridgeshire: IT Governance Publishing.
25. Kearney P., Kruger H.A. Can perceptual differences account for enigmatic information security behaviour in an organization? *Computers & Security*, 61, 46-58.
26. Knapp K. J., Morris R.F., Marshall T.E., Byrd T.A. (2009). Information security policy: An organizational-level process model. *Computers & Security*, 28, 493-508.
27. Kolkowska E., Dhillon G. (2013). Organizational power and information security rule compliance. *Computers & Security*, 33, 3-11.

28. Kompleksiniai kibernetinės saugos mokymai valstybės ir savivaldybių institucijų ir įstaigų dirbantiesiems (2020, gegužės 19). Prieiga per internetą: https://kam.lt/lt/veikla_576/es_projektai/kompleksiniai_mokymai.html.
29. Lietuvos Respublikos aplinkos ministro valdymo sričių 2021-2023 metų strateginis veiklos plano projektas (2021). Prieiga per internetą: https://am.lrv.lt/uploads/am/documents/files/Strateginis%20planavimas/AM_2021_2023_SVP_tvirtinimas_galutinis_pateiktasMP.docx.
30. Lietuvos Respublikos finansų ministro valdymo sričių 2021-2023 metų strateginis veiklos planas (2020). Prieiga per internetą: https://finmin.lrv.lt/uploads/finmin/documents/files/FM%202021-2023%20_SVP_projektas(2).pdf.
31. Lietuvos Respublikos ekonomikos ir inovacijų ministro valdymo sričių 2021-2023 metų strateginis veiklos plano projektas (2021). Prieiga per internetą: https://eimin.lrv.lt/lt/ekonomikos-ir-inovaciju-ministerija/administracine-informacija/planavimo-dokumentai/strateginiai-veiklos-planai/ekonomikos-ir-inovaciju-ministerijos-2021-2023-m-strateginis-veiklos-planas.
32. Lietuvos Respublikos energetikos ministro valdymo sričių 2021-2023 metų strateginis veiklos plano projektas (2021). Prieiga per internetą: https://enmin.lrv.lt/uploads/enmin/documents/files/2021%2003%2023%20EM%202021-2023%20m_%20SVP%20(Patvirtintas).pdf.
33. Lietuvos Respublikos kibernetinio saugumo įstatymas (2018). Prieiga per internetą: https://eseimas.lrs.lt/portal/legalAct/lt/TAD/15e540727ac211e89188e16a6495e98c.
34. Lietuvos Respublikos kultūros ministro valdymo sričių 2021–2023 m. strateginis veiklos planas (2021). Prieiga per internetą: https://lrkm.lrv.lt/uploads/lrkm/documents/files/KM%202021%E2%80%932023%20m_%20SVP.pdf.
35. Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos 2021-2023 metų strateginio veiklos planas (2021). Prieiga per internetą: https://socmin.lrv.lt/uploads/socmin/documents/files/SADM_SVP_2021-2023_A1-204.pdf
36. Lietuvos Respublikos susisiekimo ministro valdymo sričių 2021-2023 metų strateginis veiklos plano projektas (2021). Prieiga per internetą: https://sumin.lrv.lt/uploads/sumin/documents/files/2021-2023%20m_%20SM%20SVP%20projektas.pdf.
37. Lietuvos Respublikos sveikatos apsaugos ministerijos 2021-2023 metų strateginio veiklos plano projektas (2021). Prieiga per internetą:

https://sam.lrv.lt/uploads/sam/documents/files/Administracine_informacija/Planavimo_dokumentai/Metiniai_veiklos_planai/2021/SAM%20SVP%202021-2023%20m_%20projektas.pdf.

38. Lietuvos Respublikos švietimo, mokslo ir sporto ministerijos 2021-2023 strateginis veiklos plano projektas (2021). Prieiga per internetą: https://www.smm.lt/uploads/documents/Administracine%20informacija/planavimo%20dokumentai/SVP%202021-2023%20projektas%20(SEIME)_2020-12-02.pdf.
39. Lietuvos Respublikos teisingumo ministro valdymo sričių 2021-2023 metų strateginis veiklos plano projektas (2021). Prieiga per internetą: https://tm.lrv.lt/uploads/tm/documents/files/TM_2021-2023_SVP_projektas_skelbimui.pdf.
40. Lietuvos Respublikos užsienio reikalų ministro valdymo sričių 2021-2023 metų strateginis veiklos plano projektas (2021). Prieiga per internetą: http://www.urm.lt/uploads/default/documents/U%C5%BEsienio%20reikal%C5%B3%20ministerijos%202021-2023%20met%C5%B3%20strateginio%20veiklos%20plano%20projektas-patikslintas.pdf.
41. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas (2011). Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.415499/asr.
42. Lietuvos Respublikos valstybės kontrolė (2018). Ypatingos svarbos informacinių išteklių valdymas. *Valstybinio audito ataskaita*. Prieiga per internetą: http://www.vkontrole.lt/failas.aspx?id=3817.
43. Lietuvos Respublikos vidaus reikalų ministrui pavestų valdymo sričių 2020-202č metų strateginis veiklos planas (2020). Prieiga per internetą: https://vrm.lrv.lt/uploads/vrm/documents/files/00_2020-2022_VRM_SVP_(KEITIMAS_gruodis).pdf.
44. Lietuvos Respublikos žemės ūkio ministro valdymo sričių 2021-2023 metų strateginis veiklos plano projektas (2021). Prieiga per internetą: https://zum.lrv.lt/uploads/zum/documents/files/LT_versija/Administracine_informacija/Planavimo_dokumentai/Strateginiai_veiklos_planai/%C5%BD%C5%AAM%202021-2023%20m_%20SVP%20projektas.pdf.
45. Lin C., Wittmer J.L.S. (2017). Proactive information security behavior and individual creativity: Effects of group culture and descentralized IT governance. *IEEE International Conference on Intelligence and Security Informatics*.
46. Nacionalinė energetinės nepriklausomybės strategija (2018). Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.429490/asr.

47. Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos nuostatai (2017). Prieiga per internetą: https://e-tar.lt/acc/legalAct.html?documentId=fa16ffd08e3d11e7a3c4a5eb10f04386&lang=lt.
48. Nacionalinių kibernetinio saugumo pratybų „Kibernetinis skydas 2019“ ataskaita visuomenei (2019). Prieiga per internetą: https://www.nksc.lt/doc/KS2019_pratybu_ataskaita.pdf.
49. Nacionalinių kibernetinio saugumo pratybų „Kibernetinis skydas 2020“ ataskaita visuomenei (2019). Prieiga per internetą: https://www.nksc.lt/doc/KS2020_pratybu_ataskaita.pdf.
50. Nacionalinis kibernetinių incidentų valdymo planas (2018). Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/e16e7761fc4b11e89b04a534c5aaf5ce.
51. Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinis veiklos planas (2019). Prieiga per internetą: https://eseimas.lrs.lt/portal/legalAct/lt/TAD/faeb5eb4a6c811e9aab6d8dd69c6da66?jfwid=dg8d31595
52. Nacionalinė kibernetinio saugumo strategija (2018). Prieiga per internetą: https://eseimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f?jfwid=dg8d31595.
53. Nickols F. (2016). Strategy, Strategic Management, Strategic Planning and Strategic Thinking. *Distance Consulting*. Prieiga per internetą: https://nickols.us/strategy_etc.pdf.
54. Norkūnas E. (2021, vasario 11). Valstybinis IT ūkis žaidžia brangią ruletę. *Delfi*. Prieiga per internetą:https://www.delfi.lt/verslas/nuomones/eimantas-norkunas-valstybinis-it-ukis-zaidzia-brangia-rulete.d?id=86454781.
55. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas (2018). Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/e16e7761fc4b11e89b04a534c5aaf5ce.
56. Palmer D. (2018, spalio 12). WannaCry ransomware: Have the lessons been learned? *Zdnet.* Prieiga per internetą: https://www.zdnet.com/article/this-is-how-much-the-wannacry-ransomware-attack-cost-the-nhs/.
57. Pfleeger S. L., Caputo D. D. (2012). Leveraging behavioural science to mitigate cyber security risk. *Computers & Security*, 31, 597 – 611.
58. Rossouw von Solms, Johan van Niekerk (2010). Information security culture: A management perspective. *Computers & Security*, 29, 476-486.
59. Rossouw von Solms, Johan van Niekerk (2013). From information security to cyber security. *Computers & Security*, 38, 97–102.

60. Ruighaver A.B., Maynard S.B. (2006). Organizational Security Culture: More Than Just an End-User Phenomenon, *Conference Paper in IFIP International Federation for Information Processing*.
61. Rupšienė L. (2007). *Kokybinio tyrimo duomenų rinkimo metodologija*. Klaipėda : Klaipėdos universiteto leidykla.
62. Sanders P. (2019, rugpjūčio 21 d.). Key Cybersecurity Threat in the Public Sector. *Identifi Global*. Prieiga per internetą: https://www.identifiglobal.com/news/key-cybersecurity-threats-in-the-public-sector/39972/.
63. Schein E. H. (1996). Culture: The Missing Concept in Organization Studies. *Administrative Science Quarterly*, 41 (2), 229-240.
64. Schlienger T., Teufel S. *(2003).* Information security culture: from analysis to change. *3rd Annual Information Security South Africa Conference,* University of Fribourg.
65. Stitt A. (2020, spalio 16). Interview: How cyber hygiene supports security culture – ThreatQuotient. *Australia Security Brief*. Prieiga per internetą: https://securitybrief.com.au/story/interview-how-cyber-hygiene-supports-security-culture-threatquotient.
66. Thomson K., van Niekerk J. (2011). Combating information security apathy by encouraging prosocial organisational behavior. *Information Management & Computer Security*, 20(1), 39-46.
67. Thsohou A., Karyada M., Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers & Security*, 52, 128-141.
68. Tidikis R. (2003). *Socialinių mokslų tyrimo metodologija*. Vilnius: Lietuvos Teisės universitetas.
69. Trevors M. (2017, lapkričio 15). Cyber Hygiene: 11 Essential Practices. *Insider Threat Blog*, Carnegie Mellon University: Software Engineering Institute. Prieiga per internetą: https://insights.sei.cmu.edu/insider-threat/2017/11/cyber-hygiene-11-essential-practices.html.
70. Valackienė A., Mikėnė S. (2008). *Sociologinis tyrimas: metodologija ir atlikimo metodika.* Kaunas: KTU.
71. Valstybės informacinių išteklių valdymo pertvarka (2021, vasario 12). *EIMIN*. Prieiga per internetą: https://eimin.lrv.lt/lt/veiklos-sritys/skaitmenine-politika/valstybes-informaciniu-istekliu-valdymo-pertvarka.
72. Verizon (2020). *Data Breach Investigations Report*. Prieiga per internetą: https://enterprise.verizon.com/resources/executivebriefs/2020-dbir-executive-brief.pdf.
73. Vishwanathm A., Neo L. S., Goh P., Lee S., Khader M., Ong G., Chin J. (2020). Cyber hygiene: The concept, its measure, and its initial tests, *Elsevier: Decission Support Systems*, Volume 128.
74. World Economic Forum (2021). *The Global Risks Report 2021*. 16th Edition. Prieiga per internetą: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf.

75. What is plaguing public sector cyber readiness? (2020, vasario 28). *Help Net Security*. Prieiga per internetą: https://www.helpnetsecurity.com/2020/02/28/public-sector-cyber-readiness/.

Pocienė A. (2021). *Kibernetinio saugumo kultūros formavimo problemos Lietuvos viešajame sektoriuje* (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas.

ANOTACIJA

Magistro baigiamajame darbe pagal autorės sudarytą teorinį modelį pateiktas kibernetinio saugumo kultūros procesų koreliacijos ir įtakos nacionalinio saugumo stiprinimui vertinimas, identifikuotos kibernetinio saugumo kultūros formavimo problemos Lietuvos viešajame sektoriuje ir remiantis ekspertiniu vertinimu tikrinamos empiriškai. Pirmajame skyriuje nagrinėjama kibernetinio saugumo kultūros teorija, išanalizuoti pagrindiniai jos formavimo kriterijai ir atskleisti viešojo sektoriaus institucijų kibernetinio saugumo kultūros formavimo ypatumai. Antrame darbo skyriuje yra nustatyti pagrindiniai tyrimo uždaviniai, tikrinama hipotezė, apibrėžta tyrimo loginė eiga bei atliktas tyrimo metodikos pagrindimas. Trečiame skyriuje atskleisti kibernetinio saugumo kultūros įgyvendinimo Lietuvos viešajame sektoriuje pagrindiniai teisinio reglamentavimo aspektai, identifikuoti kibernetinio saugumo kultūros įgyvendinimo procesai, problemos ir iššūkiai Lietuvos Respublikos ministerijose. Susisteminus ekspertinio vertinimo rezultatus, patvirtinamos arba atmetamos hipotezės bei atliekama tyrimo duomenų interpretacija. Galiausiai, yra pateikiamos išvados bei siūlymai kibernetinio saugumo kultūros formavimo problematikai spręsti.

Pagrindiniai žodžiai: kibernetinis saugumas, kibernetinio saugumo kultūra, nacionalinis saugumas, viešasis sektorius.

Pocienė A. (2021). *The challenges of shaping cyber security culture in the Lithuanian public sector* (master thesis). Vilnius: Mykolas Romeris University.

ANNOTATION

In the master thesis, according to the author‘s theoretical model, the assessment of the correlation of cyber security culture processes and what kind of influence it makes regarding the national security strengthening are presented, challenges of shaping cyber security culture in the Lithuanian public sector are identified and empirically tested based on expert evaluation. In the first part of thesis, the theory of cyber security culture and the main criteria for its formation are analyzed, the peculiarities of cyber security culture formation in public sector institutions are revealed. In the second part, the main tasks of the research are identified, the hypothesis and the logical course of the research are defined, also the justification of the research methodology is performed. In the third part, the main aspects of legal regulation of the implementation of cyber security culture in the Lithuanian public sector are revealed, the processes, problems and challenges of the implementation of cyber security culture in the ministries of the Republic of Lithuania are identified. According to the summed up result of expert evaluation, the hypotheses are confirmed or rejected, the interpretation of the research data is performed. Finally, conclusions and suggestions for solving the problems of shaping cyber security culture are presented.

Key words: cyber security, cyber security culture, national security, public sector.

Pocienė A. (2021). *Kibernetinio saugumo kultūros formavimo problemos Lietuvos viešajame sektoriuje* (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas.

SANTRAUKA

Šiandieninėje visuomenėje, kuomet kibernetinės atakos ir jų parenkami vektoriai vis dažniau kelia didžiulę grėsmę ne tik individualiems subjektams, bet ir valstybinio lygmens sektoriams, o informacinės technologijos tapo įrankiu manipuliuoti informacija ir sukelti disbalansą tarptautiniuose santykiuose, vis daugiau valstybių įvardija, kad kibernetinis saugumas yra viena iš priemonių užtikrinti nacionalinį saugumą, o valstybės informacinių išteklių, kritinės svarbos sektorių informacinės infrastruktūros kibernetinis saugumas yra valstybės strateginiai prioritetai. Tam, kad apsaugoti pastarosios infrastruktūros kibernetinę erdvę, yra reikalinga formuoti vieningą ir sisteminį viešojo sektoriaus institucijų požiūrį į kibernetinį saugumą, kuris pasireiškia kibernetinio saugumo kultūros palaikymo procesuose tiek instituciniu, tiek nacionaliniu lygmeniu. Su tikslu suprasti nagrinėjamos temos aktualumą, tyrime buvo iškelta problema – kaip kibernetinio saugumo kultūros priemonių įgyvendinimas Lietuvos viešojo sektoriaus institucijose koreliuoja su nacionalinio saugumo stiprinimu? Tyrimo objektas – kibernetinio saugumo kultūra Lietuvos viešajame sektoriuje. Šio tyrimo tikslas yra ištirti kibernetinio saugumo kultūros formavimo ypatumus ir problemas Lietuvos viešajame sektoriuje. Tikslui pasiekti buvo nustatyti tyrimo uždaviniai: konceptualizuoti kibernetinio saugumo kultūros sampratą, atskleisti kibernetinio saugumo kultūros įgyvendinimo Lietuvos viešajame sektoriuje pagrindinius teisinio reglamentavimo aspektus, išanalizuoti kibernetinio saugumo kultūros formavimo procesus ir problemas Lietuvos valstybinėse institucijose ir pateikti siūlymus identifikuotoms problemoms spręsti. Tyrimo metodika: sisteminė, apibendrinimo, lyginamoji ir aprašomoji mokslinės literatūros analizė bei teisės aktų turinio analizė, ekspertinis vertinimas ir jo rezultatų interpretacija.

Empirinio tyrimo metu buvo iškelta pagrindinė hipotezė – kibernetinio saugumo kultūros formavimo neefektyvumą Lietuvos viešajame sektoriuje lemia vadybos stoka, kuri atliktus ekspertinį vertinimą buvo patvirtinta iš dalies. Tai yra, jog tyrimo metu buvo atskleista platesnė kibernetinio saugumo kultūros formavimo Lietuvos viešajame sektoriuje problematika, kuri apima ne tik vadybos stoką, bet ir tokias problemas, kaip žemas finansavimas ir neefektyvus biudžeto panaudojimas dėl viešųjų pirkimų procedūrų stagnacijos, žinių ir kvalifikacijos stoka, kuri atsiranda, visų pirma, dėl to, jog kibernetinio saugumo švietimas Lietuvos teisinėje bazėje nėra imperatyvus, taip pat kibernetinio saugumo pareigūno etato nebuvimas LR ministerijų struktūroje, bendradarbiavimo kibernetinio saugumo klausimais reglamentavimo nepakankamumas bei pasyvus Nacionalinės kibernetinio saugumo strategijos atnaujinimo procesas. Visos šios problemos institucijų kibernetinio saugumo kultūros formavimo procesuose lemia kibernetinio saugumo priemonių įgyvendinimo efektyvumą valstybės informacinėje infrastruktūroje, kas daro įtaką ir valstybės nacionaliniam saugumui.

Magistro baigiamojo darbo pabaigoje pateikiamos išvados ir siūlymai kiekvienai identifikuotai kibernetinio saugumo kultūros formavimo problemai spręsti.

Pocienė A. (2021). *The challenges of shaping cyber security culture in the Lithuanian public sector* (master thesis). Vilnius: Mykolas Romeris University

SUMMARY

In today's society, where cyber-attacks and their vectors increasingly pose a major threat not only to individuals but also to the state-level sectors, and information technology has become a tool for manipulating information and creating imbalances in international relations, more and more states are calling cyber security as a tool to ensure national security. As a result, cyber security of state's information resources, information infrastructure of critical sectors became the strategic priorities at national level. In order to protect the cyberspace of the latter infrastructure, it is necessary to develop a unified and systematic public sector institutions' approach to cyber security, which is reflected in the processes of maintaining cyber security culture at both institutional and national levels. In order to understand the relevance of the topic, the basic research problem was raised – how does the implementation of cyber security culture measures in Lithuanian public sector institutions correlate with the national security strengthening? The object of the research is cyber security culture in the Lithuanian public sector. The aim of this study is to investigate the peculiarities and problems of shaping cyber security culture in the Lithuanian public sector. Also, the main tasks were set: to define the concept of cyber security culture, to reveal the main aspects of legal regulation of cyber security culture implementation in the Lithuanian public sector, to analyze cyber security culture shaping processes and problems in the Lithuanian public sector institutions and to make suggestions for solving them. Research methodology: systematic, generalization, comparative and descriptive analysis of scientific literature and analysis of the content of legal acts, also expert evaluation and interpretation of its results.

The main hypothesis was raised – the inefficiency of shaping cyber security culture in the Lithuanian public sector is determined by the lack of management and was partially confirmed by the expert assessment. In addition, the study revealed broader challenges of shaping cyber security culture in the Lithuanian public sector, which includes not only a lack of management but also such problems as low funding and inefficient budget utilization due to stagnation of public procurement procedures, lack of personnel knowledge and qualifications due to the main fact that cyber security education in the Lithuanian legal framework is not imperative, also the lack of a cyber security officer post in the structure of ministries of the Republic of Lithuania, insufficient regulation of cooperation on cyber security issues and passive process of updating the National Cyber Security Strategy. All these problems of shaping cyber security culture in state institutions determine the efficiency of the implementation of cyber security measures in the state information infrastructure, which affects the national security of the state.

At the end of the master's thesis, conclusions and suggestions for solving each identified problem of shaping cyber security culture are presented.

PRIEDAI

Priedas 1. Ekspertinio interviu protokolas

Gerb. Eksperte, Mykolo Romerio universiteto Viešojo valdymo ir verslo fakulteto Kibernetinio saugumo valdymo programos magistrantė Aistė Pocienė atlieka tyrimą „Kibernetinio saugumo kultūros formavimo ypatumai Lietuvos viešajame sektoriuje“, kurio tikslas – ištirti kibernetinio saugumo kultūros formavimo procesus ir problemas Lietuvos viešajame sektoriuje.

Vienas uždavinių minėtam tikslui pasiekti – identifikuoti esminius iššūkius formuojant kibernetinio saugumo kultūrą Lietuvos viešajame sektoriuje, remiantis ekspertiniu interviu.

Jūsų atsakymai į klausimus padės atlikti išsamų tyrimą. Būčiau dėkinga už Jūsų išreikštą nuomonę.

BENDRIEJI DUOMENYS:

1. Vardas, pavardė:
2. Darbovietės pavadinimas ir užimamos pareigos:

EKSPERTINIS VERTINIMAS:

1. Vadovaujantis LR teisės aktais, kibernetinio saugumo subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojai suderinę su Nacionaliniu kibernetinio saugumo centru, tvirtina kibernetinio saugumo politikos ir jos įgyvendinimo dokumentus. Kaip manote, ar visi institucijos darbuotojai turėtų būti skatinami dalyvauti rengiant kibernetinio saugumo politiką, siekiant efektyvaus politikos įgyvendinimo praktikoje ar visgi tik tie darbuotojai, kurių funkcijos yra tiesiogiai susijusios su kibernetiniu saugumu? Savo atsakymą pagrįskite.
2. Jūsų nuomone, ar visų lygmenų vadovai turėtų įsitraukti į kibernetinio saugumo kultūros formavimą valstybinėse institucijose? Ar sutinkate, kad kibernetinis saugumas yra dažnai įvardijamas kaip IT departamento reikalas? Savo atsakymą pagrįskite.
3. Kaip vertinate valstybinių institucijų, valdančių ar tvarkančių valstybės informacinius išteklius ar YSII kibernetinio saugumo higienos lygį? Jūsų manymu, kokie pagrindiniai veiksniai jį lemią? ***Klausimyno tęsinys kitame puslapyje***

4. Kaip manote ar visose valstybinėse institucijose, valdančiose ar tvarkančiose valstybės informacinius išteklius ar YSII, yra organizuojami kibernetinio saugumo mokymai? Ar galėtumėte įvardinti pagrindines (jums žinomas) tokių mokymų pateikimo formas, būdus Lietuvos viešajame sektoriuje? Jūsų vertinimu, ar jie yra efektyvūs?
5. Kaip manote, kas paskatintų darbuotojo, kurio tiesioginės funkcijos nėra susijusios su kibernetiniu saugumu, įsitraukimą į organizacijos kibernetinio saugumo kultūros formavimą?
6. Kaip vertinate LR viešajam sektoriui skiriamą finansavimą kvalifikacijos kėlimui personalo, kurio funkcijos tiesiogiai susijusios su kibernetiniu saugumu? Ar sutinkate, kad skiriamas finansavimas nėra proporcingas valdomų ar tvarkomų valstybės informacinių išteklių kibernetinėms rizikoms nacionalinio saugumo kontekste?
7. NKSC yra pagrindinė institucija Lietuvoje, organizuojanti kibernetinio saugumo pratybas. Kaip vertinate jų adaptaciją valstybinių institucijų poreikiams, vykdomai veiklai? Kaip manote, ar dabartinis pratybų skaičius per metus yra pakankamas formuoti kibernetinio saugumo kultūrą nacionaliniu lygmeniu?
8. Jūsų nuomone, kokios priežastys lemia žemą valstybinių institucijų dalyvavimo NKSC organizuojamose pratybose statistinį rodiklį? ***Klausimyno tęsinys kitame puslapyje***

9. Kokias LR viešojo sektoriaus bendradarbiavimo formas su kitomis organizacijomis (tiek viešojo, tiek privataus sektoriaus) galite įvardinti? 1) Nacionaliniu lygmeniu – 2) Tarptautiniu lygmeniu –
10. Jūsų nuomone, kokie yra pagrindiniai iššūkiai Lietuvos viešojo sektoriaus institucijoms, įgyvendinant kibernetinio saugumo kultūrą?
11. Kaip manote, ar LR teisės aktuose kibernetinio saugumo priemonės yra pakankamos ir įpareigojančios visas viešojo sektoriaus institucijas jas integruoti, formuojant kibernetinio saugumo kultūrą? Jei ne, ką jūsų nuomonę reikėtų keisti, norint sukurti efektyvų kibernetinio saugumo kultūros įgyvendinimo modelį viešajame sektoriuje?

Ačiū už Jūsų laiką!

Priedas 2. LR ministerijos eksperto apklausos anketa

Gerb. Eksperte, Mykolo Romerio universiteto Viešojo valdymo ir verslo fakulteto Kibernetinio saugumo valdymo programos magistrantė Aistė Pocienė atlieka tyrimą „Kibernetinio saugumo kultūros formavimo ypatumai Lietuvos viešajame sektoriuje“, kurio tikslas – ištirti kibernetinio saugumo kultūros formavimo procesus ir problemas Lietuvos viešajame sektoriuje.

Vienas iš uždavinių minėtam tikslui pasiekti – atskleisti kibernetinio saugumo kultūros formavimo būdus ir procesus valstybinėse institucijose, valdančiose bei tvarkančiose valstybės informacinius išteklius, atsakingose už savo sektoriaus ypatingos svarbos infrastruktūros objektus (toliau YSI objektai) ir ypatingos svarbos informacines infrastruktūras (toliau YSII). Pagrindiniai tiriamieji aspektai: kibernetinio saugumo politika (kibernetinio saugumo valdymo mechanizmų egzistavimas), vadovų indėlis (darbuotojų požiūrio į kibernetinį saugumą formavimas, motyvacija integruoti kibernetinį saugumą į darbo aplinką), kibernetinė higiena (ar efektyviai pritaikomi kibernetinio saugumo techniniai reikalavimai institucijų praktikoje), kibernetinio saugumo švietimas (IT saugos personalo kvalifikacijos kėlimas, mokymai darbuotojų skaitmeninei brandai ugdyti, institucijos dalyvavimas kibernetinio saugumo pratybose), bendradarbiavimas kibernetinio saugumo klausimais (bendradarbiavimo formos su viešuoju ir privačiuoju sektoriumi tiek nacionaliniu, tiek tarptautiniu lygmeniu).

Jūsų atsakymai į klausimus padės atlikti išsamų tyrimą. Būčiau dėkinga už Jūsų išreikštą nuomonę.

1. Jūsų atstovaujama institucija (galimi keli atsakymų variantai): e) Įgyvendina kibernetinio saugumo priemones, kurios viešajam sektoriui yra reglamentuotos LR teisės aktuose; f) Turi patvirtintą institucijos kibernetinio saugumo strategiją / politiką; g) Turi patvirtintas standartinės veiklos procedūras, susijusias su kibernetinio saugumo įgyvendinimu organizacijoje; h) Visi punktai aukščiau; i) Kita (įvardinkite):
2. Jūsų nuomone, ar atstovaujamoje institucijoje yra tinkamai palaikoma kibernetinio saugumo higiena? d) Taip; e) Iš dalies; f) Ne.
3. Ar jūsų institucijoje yra organizuojami kibernetinio saugumo mokymai darbuotojams? c) Taip; d) Ne.
4. Kaip manote, kas paskatintų darbuotojo, kurio tiesioginės funkcijos nėra susijusios su kibernetiniu saugumu, įsitraukimą į organizacijos kibernetinio saugumo kultūros formavimą? Galimi keli atsakymų variantai. ***Klausimyno tęsinys kitame puslapyje***

f) Vadovų motyvacija ir lyderystė šiuo klausimu; g) Mokymai skaitmeninei brandai didinti; h) Aiškiai organizacijos politikoje apibrėžta privalomoji kibernetinė higiena ir elgesio elektroninėje erdvėje taisyklės; i) Sankcijos dėl kibernetinio saugumo priemonių netaikymo; j) Kita (įvardinkite):
5. Ar jūsų institucijoje yra sudarytos sąlygos kelti personalo, kurio funkcijos tiesiogiai susijusios su kibernetiniu saugumu, kvalifikaciją? c) Taip; d) Iš dalies; e) Ne.
6. Kaip dažnai jūsų institucija dalyvauja NKSC ar kitų institucijų organizuojamose kibernetinio saugumo pratybose? d) Dalyvauja visose pratybose, į kurias yra kviečiama; e) Dalyvauja tik dalyje pratybų; f) Nedalyvauja.
7. Jūsų nuomone, kokios priežastys lemia žemą valstybinių institucijų dalyvavimo NKSC ar kitų institucijų organizuojamose pratybose statistinį rodiklį? Galimi keli atsakymo variantai. f) Personalo stoka; g) Kvalifikacijos ir žinių stoka; h) Vadybos ir motyvacijos stoka; i) Institucijos užimtumas; j) Kita (įvardinkite):
8. Kokias jūsų atstovaujamos institucijos bendradarbiavimo formas kibernetinio saugumo klausimais su kitomis institucijomis (tiek viešojo, tiek privataus sektoriaus) galite įvardinti? c) Nacionaliniu lygmeniu – d) Tarptautiniu lygmeniu –
9. Jūsų nuomone, ar visų lygmenų vadovai yra įsitraukę į kibernetinio saugumo kultūros formavimą jūsų atstovaujamoje institucijoje? Jei taip, kokiais būdais?
10. Jūsų nuomone, kokie yra pagrindiniai iššūkiai Lietuvos viešojo sektoriaus institucijoms, įgyvendinant kibernetinio saugumo kultūrą?

Ačiū už Jūsų laiką!