MYKOLO ROMERIO UNIVERSITETAS
VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

MANTAS GABRYS

KIBERNETINIŲ ATAKŲ VALDYMO VIEŠOJO SEKTORIAUS INFORMACINĖSE SISTEMOSE MODELIAVIMAS: PASAULINĖ PATIRTIS IR LIETUVOS PERSPEKTYVA

Magistro baigiamasis darbas

Vadovas
prof. dr. T. Limba

VILNIUS, 2023

MYKOLO ROMERIO UNIVERSITETAS

VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

KIBERNETINIŲ ATAKŲ VALDYMO VIEŠOJO SEKTORIAUS INFORMACINĖSE SISTEMOSE MODELIAVIMAS: PASAULINĖ PATIRTIS IR LIETUVOS PERSPEKTYVA

CYBER ATTACK MANAGEMENT IN PUBLIC SECTOR INFORMATION SYSTEMS MODELING: GLOBAL EXPERIENCE AND LITHUANIAN PERSPECTIVE

Kibernetinio saugumo valdymo magistro baigiamasis darbas

Studijų programa

Studijų programa 6211LX066

Konsultantas

_____

2023

Vadovas

_____prof. dr. T. Limba

2023

Recenzentas

_____

2023

Atliko

KSVvmis21-1 gr. stud.

_____M. Gabrys

2023

VILNIUS, 2023

TURINYS

ĮVADAS 7
1. KIBERNETINIŲ ATAKŲ VIEŠOJO VALDYMO ĮSTAIGŲ INFORMACINĖSE SISTEMOJE VALDYMO TEORINĖ APIBRĖŽTIS 10
1.1. Kibernetinių atakų apibrėžtis ir tipologija 10
1.2. Kibernetinių atakų grėsmės viešajam sektoriui ir visuomenei 12
1.3. Kibernetinių atakų valdymo metodai ir priemonės: Lietuvos atvejis 15
1.3.1. Kibernetinio saugumo teisinės priemonės 20
1.3.2. Kibernetinio saugumo strategija ir politika 23
1.4. Kibernetinių atakų valdymo užsienio šalyse geroji patirtis 24
2. KIBERNETINIŲ ATAKŲ VIEŠOJO VALDYMO ĮSTAIGŲ INFORMACINĖSE SISTEMOSE METODOLOGIJA 30
3. KIBERNETINIŲ ATAKŲ VIEŠOJO VALDYMO ĮSTAIGŲ INFORMACINĖSE SISTEMOSE TYRIMO REZULTATAI 34
3.1. Kibernetinio saugumo statistika Lietuvoje 34
3.2. Savivaldybių atstovų interviu rezultatai 36
3.3. Kibernetinio saugumo savivaldybėje gerinimo sprendimai 47
IŠVADOS 49
REKOMENDACIJOS 51
LITERATŪRA 52
ANOTACIJA 56
ANNOTATION 57
SANTRAUKA 58
SUMMARY 59
PRIEDAI 60

PAVEIKSLŲ SĄRAŠAS

1 pav. Magistro baigiamojo darbo struktūros loginė schema 9
2 pav. Kibernetinio saugumo sritys 15
3 pav. Kibernetinio saugumo lygiai 16
4 pav. Kibernetinio saugumo sistemos dalyviai 18
5 pav. Tyrimo etapų loginė seka 33
6 pav. Kibernetinio saugumo gerinimas savivaldybėje 47

LENTELIŲ SĄRAŠAS

1 lentelė. Tyrimo dalyvių charakteristika 31
2 lentelė. Tyrimo instrumento teorinis pagrindimas 31
3 lentelė. Ekspertų nuomonė apie kibernetinio saugumo grėsmes 36
4 lentelė. Ekspertų nuomonė apie kibernetinių atakų riziką 37
5 lentelė. Ekspertų nuomonė apie taikomas kibernetinio saugumo priemones 38
6 lentelė. Ekspertų nuomonė apie taikomas asmenines saugumo priemones 40
7 lentelė. Ekspertų nuomonė apie reagavimą į kibernetines grėsmes 41
8 lentelė. Kibernetinio saugumo teisinio reguliavimo vertinimas 42
9 lentelė. Ekspertų nuomonė apie darbuotojų švietimą 43
10 lentelė. Kibernetinio saugumo sprendimai 44
11 lentelė. Kibernetinio saugumo užtikrinimo priemonės 46

PAGRINDINĖS SĄVOKOS

White hat hacker – anglų k. terminas (baltakepuris hakeris) apibūdinantis laisvai samdomą asmenį ar įmonę atliekančius pažeidžiamumo testavimus (angl. *Penetration testing*) pagal sutartį. (Dalziel H., How to Become an Ethical Hacker and Penetration Tester. *ScienceDirect*, 2015) Prieiga per: https://www.sciencedirect.com/topics/computer-science/white-hat-hacker

Grey hat hacker – anglų k. terminas (pilkakepuris hakeris) apibūdinantis nepriklausomą asmenį, naršantį internete ir ieškantį įvairių interneto portalų saugumo spragų tam, kad paskui geranoriškai apie jas pranešti (atskleisti) informacinės sistemos administratoriui (duomenų tvarkytojui). Kitaip dar vadinamas etiškas hakeris. Toks asmuo taip pat gali, už atlygį, pasisiūlyti ištaisyti rastą spragą. (Dalziel H., How to Become an Ethical Hacker and Penetration Tester. ScienceDirect, 2015) Prieiga per: https://www.sciencedirect.com/topics/computer-science/white-hat-hacker

Responsible disclosure– anglų k. terminas (atsakingas atskleidimas) apibūdinantis informacinės sistemos valdytojo/tvarkytojo informavimą apie aptiktą saugumo spragą jo valdomoje/tvarkomoje informacinėje sistemoje. (Shepherd S., How to define Responsible disclosure. *SANS White paper*, 2003)

Etiškas įsilaužimas (angl. *Ethical hacking*) – pažeidžiamumo testavimas, sąmoningai įsilaužiant į informacinės sistemos kritinę infrastruktūrą, atliekamas balta kepurių hakerių užsakomo audito metu. (Labiausiai patikęs apibrėžimas rastas Maryville universiteto svetainėje) Prieiga per: https://online.maryville.edu/blog/ethical-hacking-and-morality-the-gray-area/

ĮVADAS

Temos aktualumas. Technologijų raidą lemia socialiniai tinklai, internetinės operacijos, debesų kompiuterija ir automatizuoti procesai. Tačiau su technologine evoliucija susiduriama ir su kibernetinių nusikaltimų pažanga, kuriami nauji įrankiai ir metodai, leidžiantys prasiskverbti į sudėtingesnę arba geriau kontroliuojamą aplinką, padaryti didesnę žalą ir net likti neatsekamiems. Šiuo metu didžioji dalis ekonominės, komercinės, kultūrinės, socialinės ir vyriausybinės veiklos ir šalių sąveikos visais lygiais, įskaitant asmenis, nevyriausybines organizacijas ir valdžios bei vyriausybines institucijas, vykdoma elektroninėje erdvėje. Pastaruoju metu daugelis privačių įmonių ir vyriausybinių organizacijų visame pasaulyje susiduria su kibernetinių atakų problema.

Limba ir kt. (2017) nuomone kibernetinis saugumas šiais laikais yra svarbiausias technologiškai pagrįsto gyvenimo aspektas. Valstybės institucijos, bankų sektoriai, viešosios ir privačios tarnybos, savo kasdienėje veikloje naudoja informacines technologijas, kurios yra paremtos ryšių ir informacinėmis sistemomis, o tai reiškia, kad priklauso nuo kibernetinio saugumo. Viešasis ir privatus sektorius kasmet išleidžia dideles pinigų sumas technologijoms, saugos programinei įrangai ir aparatūros įrenginiams, kurie padidintų kibernetinį saugumą įmonėse, tačiau vis tiek yra pažeidžiami. Pagrindinė šios situacijos problema yra ta, kad kibernetinis saugumas dažniausiai traktuojamas kaip techninis aspektas ar technologija, kurią galima nesunkiai įdiegti organizacijos viduje ir šis įgyvendinimas garantuos kibernetinį saugumą. Šis požiūris turi pasikeisti, nes kibernetinis saugumas šiais laikais yra ne tik technologijos.

Kaip nurodo Štitilis, Rotomskis ir kt. (2020) kibernetinės grėsmės tapo dideliu susirūpinimu tiek nacionaliniu, tiek tarptautiniu lygiu. Moksliniai tyrimai pabrėžia globalų kibernetinės erdvės pobūdį, nulemiantį galimų grėsmių globalumą. Dėl pasaulinio pobūdžio kibernetinių incidentų ar atakų tyrimas tampa sudėtingas ir kartais neįmanomas. Tačiau reikia pažymėti, kad kibernetinės atakos iš tikrųjų vyksta tam tikroje teritorijoje, apima ir fizinius subjektus, esančius konkrečioje teritorijoje, ir jas įvykdo fiziniai ar juridiniai asmenys, priklausantys tam tikroms nacionalinėms jurisdikcijoms. Kibernetinio saugumo politikos plėtrai ES skyrė daug dėmesio. 2016 m. ES priėmė 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyvą (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti, kuri tapo pagrindine priemone, padedančia suvienodinti nacionalinių valstybių kibernetinio saugumo politiką.

Kalbant apie nacionalines kibernetinio saugumo strategijas, teigiamas dalykas yra tai, kad dauguma ES valstybių narių tokias strategijas jau yra patvirtinusios. Tačiau patvirtintos strategijos tarp ES valstybių narių labai skiriasi savo turiniu ir įgyvendinimu. Todėl analizuojant kibernetinių atakų

valdymo ypatumus aktualu nustatyti atskirų šalių nacionalinių strategijų skirtumų priežastis ir analizuoti užsienio šalių gerąją praktiką kibernetinio saugumo bei kibernetinių atakų valdymo aspektu.

Mokslinė problema. Šalys patiria didesnį kibernetinių grėsmių poveikį ir žalą, nes šalies įstatymai ir politika, susiję su kibernetiniu saugumu, nėra pakankami arba nėra veiksmingai įgyvendinami; technologijų ir infrastruktūros trūkumai ir žinių bei pasirengimo prieš kibernetines atakas trūkumas; vartotojų mokymo bei informuotumo, bei institucijų ir organizacijų koordinavimo ir bendradarbiavimo trūkumas sukelia grėsmę kibernetiniams saugumui. Darbe keliamas probleminis klausimas: kokia užsienio šalių kibernetinių atakų valdymo geroji praktika gali būti pritaikyta Lietuvos viešojo sektoriaus institucijose?

Tyrimo objektas – kibernetinių atakų viešojo valdymo įstaigose valdymas.

Tyrimo tikslas – išanalizavus kibernetinių atakų valdymo teorinius aspektus bei remiantis pusiau struktūruotos apklausos rezultatais, pritaikyti geriausią pasaulinę praktiką kibernetinių atakų valdymui viešojo sektoriaus informacinėse sistemose.

Uždaviniai:

1. Išanalizuoti kibernetinių atakų viešojo sektoriaus informacinėse sistemose valdymo problematiką.

2. Išnagrinėti užsienio šalių gerąją patirtį ir kibernetinių atakų viešojo sektoriaus informacinėse sistemose valdymo modelius.

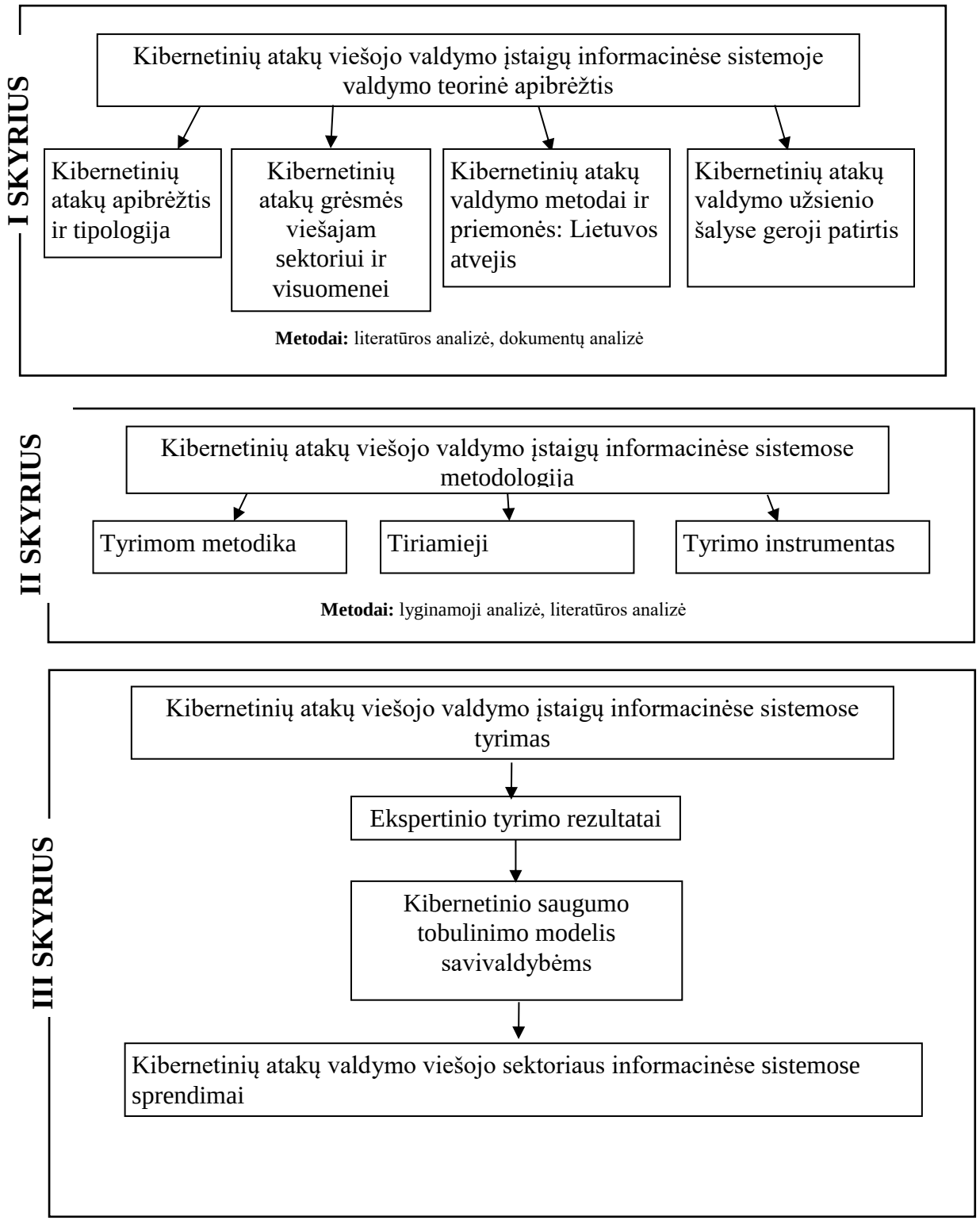
3. Remiantis empirinio tyrimo rezultatais pateikti kibernetinių atakų valdymo viešojo sektoriaus informacinėse sistemose sprendimus.

Mokslinio tyrimo metodai: mokslinės literatūros lyginamoji analizė, teisės aktų bei reglamentų lyginamoji analizė ir apibendrinimas, pusiau struktūruota apklausa, tyrimo rezultatų analizė ir apibendrinimas.

Duomenų analizės metodai.

1. Kokybinė turinio analizė
2. Atvejo studijos analizė
3. Gautų duomenų analizė

Magistro baigiamojo darbo struktūra: baigiamasis darbas sudarytas iš trijų darbo dalių. Pirmoje teorinėje darbo dalyje analizuojama kibernetinių atakų apibrėžtis, klasifikacija, aptariamos kibernetinių atakų sukeliamos grėsmės. Šioje darbo dalyje analizuojama kibernetinio saugumo valdymo įgyvendinimo situacija ir priemonės, teisinio reguliavimo nacionaliniu ir tarptautiniu lygmeniu ypatumai, apžvelgiama užsienio šalių geroji praktika, atskleidžianti taikomus modelius ir priemones. Antroje darbo dalyje pateikiama empirinio tyrimo metodologija, tyrimo loginė schema. Trečioje darbo dalyje analizuojami tyrimo rezultatai bei pateikiami sprendimai kibernetinių atakų viešojo sektoriaus institucijose valdymo tobulinimui.



Šaltinis: sudaryta autoriaus

1 pav. Magistro baigiamojo darbo struktūros loginė schema

1. KIBERNETINIŲ ATAKŲ VIEŠOJO VALDYMO ĮSTAIGŲ INFORMACINĖSE SISTEMOJE VALDYMO TEORINĖ APIBRĖŽTIS

1.1. Kibernetinių atakų apibrėžtis ir tipologija

Kibernetinės atakos vis labiau tampa kasdienine realybe tiek įvairaus dydžio įmonėse, tiek pavieniams asmenims, tačiau apie kibernetinius nusikaltimus visuotinai žinoma mažai. Bendovschi (2015) nurodo, kad stinga bendro supratimo apie skirtingus kibernetinių atakų tipus, charakteristikas ir galimas pasekmes, o tai gali tapti kliūtimi bandant užtikrinti informacijos saugumą. Tarptautinėje literatūroje galima rasti keletą terminų „kibernetinė ataka“, „kibernetinis nusikaltimas“ ir kt. apibrėžimų, kurių bendras tikslas yra pakenkti duomenų konfidencialumui, vientisumui ir prieinamumui.

Analizuojant kibernetines atakas tikslinga apibrėžti ir kibernetinę erdvę. Bendro kibernetinės erdvės apibrėžimo nebuvimas yra kliūtis formaliam ir teisiniam kibernetinio saugumo reguliavimui tiek nacionaliniu, tiek tarptautiniu lygiu. Tarptautinių reglamentų deficitas yra ir valstybių santykių problema. Sąvoka „kibernetinė“ buvo naudojama apibūdinti beveik viską, kas yra susiję su duomenų tinklais ir kompiuteriais, ypač saugumo srityje. Tačiau, deja, nėra sutarimo, kas yra „kibernetinė erdvė“, jau nekalbant apie kibernetinių atakų apibrėžtį bei sukeliamas pasekmes (Jacuch, 2021).

Lan ir Inkster (2020) teigia, kad kibernetinė erdvė pasižymi unikalumu bei apima tiek virtualią, žmogaus sukurtą pusę, kuriai būdingas išskirtinis techninis įgalinimas ir itin sudėtingas veikimo mechanizmas, tiek integracija su tradiciniu realiu pasauliu. Europos Sąjunga kibernetinę erdvę apibrėžia kaip nuo laiko priklausomą materialaus ir nematerialaus turto rinkinį, kuriame saugoma ir (arba) perduodama elektroninė informacija. Kibernetinis saugumas apima visas veiklas, būtinas siekiant apsaugoti kibernetinę erdvę, jos naudotojus ir kibernetinių grėsmių paveiktus asmenis (ENISA 2017).

Teisės ir techninių sričių specialistai pateikė įvairius kibernetinės atakos apibrėžimus, iš kurių svarbiausi yra aptariami šiame darbo poskyryje. Richardas Clarkas pateikė kibernetinių atakų koncepciją, kurioje nurodoma, kad kibernetinės atakos yra veiksmai, kurių šalys imasi siekdamos prasiskverbti į šalies ar kitų šalių kompiuterius ar kompiuterinius tinklus, kad pakenktų ar sutrikdytų įprastinę veiklą (Motsch ir kt., 2020). Analizuojant ir kritikuojant šį apibrėžimą, galima teigti, kad trys elementai, būtent išpuolio vykdytojas, išpuolio tikslas ir ketinimas, buvo naudojami kaip kriterijai, neatsižvelgiant į trikdymo formas (Cao ir kt., 2019). Be to, kalbant apie atakos vykdytoją, bendrai paminėtos tik šalys, tačiau jei šalies kontroliuojamame kontekste ir geografinėje teritorijoje (šalių valdomų tinklų kibernetinėje erdvėje) įvyksta asmenų ataka ir jei nevyriausybinės ir privačios grupės veiks prieš trečiąją šalį, tokia situacija iš esmės nepateks į minėto apibrėžimo sritį, todėl tokių išpuolių teisinėje aprėptyje turėtų būti spraga. Atsižvelgiant į šią situaciją, galima teigti, kad minėtas apibrėžimas

iš esmės yra neišsamus ir neapima dalies privačių ir nevyriausybinių grupių vykdomų išpuolių (Li, Liu, 2021).

Michaelas Haydenas kibernetines atakas apibrėžia kaip bet koks tyčinis bandymas sutrikdyti arba sunaikinti kitos šalies kompiuterių tinklus. Akivaizdu, kad šis apibrėžimas taip pat yra labai bendras ir neatskleidžia skirtumo tarp kibernetinių nusikaltimų, kibernetinių atakų ir kibernetinio karo, o riba tarp jų aptikimo yra dviprasmiška. Palyginti su pirmuoju apibrėžimu, kuris apribojo atakos vykdytojus tik vyriausybės agresorių atveju, šis apibrėžimas yra bendras, nesunkiai interpretuojamas ir, kaip minėta, gali būti pavojingas ir turėti neigiamą poveikį bei sukelti painiavą šalių santykiuose ir galiausiai grėsmę tarptautinės bendruomenės lygmeniu (Li, Liu, 2021).

Kita grupė apibrėžimų detalizuoja, kad kibernetinė ataka yra puolamoji arba gynybinė kibernetinė operacija, dėl kurios gali būti sužaloti ar mirti žmonės arba padaryta žala ar sunaikintas turtas. Šio apibrėžimo šalininkų požiūriu, kibernetinė ataka bus atakos pobūdžio, jei ji lems apibrėžime nurodytus rezultatus (t. y. asmeninės ir finansinės žalos padarymą) (Bullock ir kt., 2021). Todėl pagrindinis šios grupės apibrėžimo pagrindas yra į rezultatą orientuotas kibernetinių atakų pobūdis, o ne pačios atakos. Tokiu būdu, jei tokio pobūdžio išpuolis sukels smurto padarinius ir pasekmes, objektyvius ir apčiuopiamus, jis bus apibūdinamas kaip išpuolis (Chen ir kt., 2021).

Kibernetinės atakos yra plačiai interpretuojamos tiek moksliniuose šaltiniuose, tiek teisės aktuose pateiktose sampratose. Daugelis žmonių neįvertina, kad kibernetinės atakos - tai ne tik piktavalių žmonių, siekiančių pavogti informaciją ar sugadinti technologijas, veiksmai. Tačiau kibernetinės atakos įvairiais būdais paliečia visuomenės narių kasdienį gyvenimą. Kibernetinių atakų sąvoka dažnai laikoma tokių apibrėžimų kaip kibernetinės operacijos, kibernetiniai incidentai ir pan. sinonimu. Talino vadove 2.0 kibernetinės atakos yra apibrėžiamos kaip kibernetinės operacijos, kurios skirtos užpulti arba apsiginti, dėl kurių pagrįstai galima tikėtis žmonių sužalojimo ar mirties, objektų sugadinimo ar sunaikinimo (Schmitt, 2016). Lietuvos Respublikos kibernetinio saugumo įstatyme kibernetinės atakos yra vadinamos kibernetiniais incidentais, įvykiais ar veika kibernetinėje erdvėje, galinčiais sukelti arba sukeliantys grėsmę arba neigiamą poveikį ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, galintys trikdyti arba trikdantys ryšių ir informacinių sistemų veikimą, valdymą ir paslaugų jomis teikimą (TAR, 2021, Nr. 2021-14159). Nors ir nėra pateikiamas vieningas kibernetinių atakų apibrėžimas, tačiau galima teigti, kad kibernetinės atakos, incidentai ar operacijos yra neteisėti piktavališki veiksmai, kurie atliekami kibernetinėje erdvėje, uždaruose tinkluose ar technologiniuose objektuose, nepriklausomai nuo jų masto ar žalos dydžio.

Kibernetinis saugumas reiškia ryšį tarp skirtingų rodiklių, tokių kaip rizikos įvertinimo priemonės, rizikos valdymo metodikos, įgūdžiai ir politika siekiant bendro tikslo – turto, jautrios informacijos ar duomenų saugumo gerinimo. Be to, svarbi dalis yra užtikrinti, kad grįžtamasis ryšys apie

informacijos konfidencialumą, prieinamumą ir atitiktį būtų renkamas ir pateikiamas atsakingoms institucijoms (Cavelty, 2018). Veiksminga kibernetinio saugumo strategija reikalauja aukšto lygio visų atskaitingų organizacijos elementų įsitraukimo.

Kalbant apie kibernetinių atakų klasifikavimą, mokslinėje literatūroje siūloma daug skirtingų požiūrių, tačiau išskiriami šie bendri tipai:

1. Kibernetinės atakos klasifikavimas, susijęs su šaltiniu (tinklu, aparatine įranga, programa) arba su taikiniu arba galimu išpuoliu (pavogti neskelbtiną informaciją, perimti programos valdymą, sekti ir išfiltruoti duomenis) (Toch el al., 2018);

2. Kibernetinių atakų skirstymas į grupes pagal kibernetinio incidento priežastį (žmogaus klaida, sistemų ar įrenginių gedimai, vidinių procesų netikslumas, išorinės problemos) (Chapelle ir kt., 2018);

3. Kibernetinės atakos rūšys atakų metodų kontekste (išpirkos reikalaujančios programos, įsilaužimas, kenkėjiškos programos, kenkėjiškas kodas, socialinė inžinerija arba sukčiavimas, paslaugų atsisakymas) (Gavėnaitė – Sirvydienė, Miečinskienė, 2021).

Paprastai visi šie klasifikavimo metodai rodo, kad kibernetinės atakos charakteristika yra atakos šaltinis (išorinė, vidinė, žmogaus klaida) arba priemonė, kuri taikoma atliekant kibernetinę ataką. Nepaisant šių požiūrių skirtumų, visi jie veda į tą patį rezultatą – pavojų arba žalą jautriems duomenims, informacijai, IT infrastruktūrai ar turtui bei visuomenės ar net šalies saugumui.

Apibendrinant galima teigti, kad moksliniuose tyrimuose nėra pateikiama vieninga kibernetinių atakų samprata, dažnai naudojamos sąvokos, tokios kaip kibernetinis pavojus, kibernetinė rizika, išpuolis ar kibernetinė grėsmė yra kibernetinių atakų sąvokos sinonimai. Išanalizavus įvairius apibrėžimus galima teigti, kad kibernetinės atakos yra veiksmai, kurių šalys imasi siekdamos prasiskverbti į šalies ar kitų šalių kompiuterius ar kompiuterinius tinklus, kad pakenktų ar sutrikdytų įprastinę veiklą, kibernetinės atakos tai kibernetinės operacijos, kurios skirtos užpulti arba apsiginti, dėl kurių pagrįstai galima tikėtis žmonių sužalojimo ar mirties, objektų sugadinimo ar sunaikinimo.

1.2. Kibernetinių atakų grėsmės viešajam sektoriui ir visuomenei

Šiuolaikinės visuomenės ir verslo priklausomybė nuo kibernetinės erdvės išaugo eksponentiškai. Nors technologijos suteikė daug pranašumų privataus ir viešojo sektoriaus organizacijoms plėtoti ir tobulinti savo veiklą, atsitiktinis kompiuterių ir tinklų technologijų diegimas turi ir trūkumų. Vienas ryškus trūkumas yra tas, kad netinkamas saugumas ir verslo procesai gali sukelti didelių finansinių nuostolių organizacijai tiek materialinių, tiek nematerialinių. Nors tiesioginiai finansiniai nuostoliai dėl kibernetinių atakų dažnai kiekybiškai įvertinami, nereikšmingi nuostoliai organizacijos prestižui ir reputacijai nėra matuojami. Organizacijoms taip pat kyla keletas kibernetinių pavojų, įskaitant sukčiavimą mokėjimų nukreipimu, duomenų pažeidimus, pažangias nuolatines atakas, kibernetines

vagystes, kompiuterių saugumo pažeidimus, kibernetinį šnipinėjimą ir net kibernetinį terorizmą (Perera, Jin, 2022).

Nuolat plėtojamos informacinės technologijos (IT) ir elektroniniai ryšiai sudaro prielaidas skleisti duomenis be fizinės erdvės apribojimų ir atsirasti naujiems prieigos prie informacinėse sistemoje laikomų duomenų būdams. Kibernetinė erdvė, kuriai būdinga nuolatinė pažanga, sukurta taip, kad veiktų kaip vieta, kur galima apdoroti elektroninius duomenis, pasiekti informacines sistema, bendrauti ir dalyvauti virtualioje veikloje ir pan. Informacinės technologijos nėra paplitusios tik asmeniniuose santykiuose, versle, bet ir valstybės valdyme, karinėse sistemose (kurios istoriškai turėjo didelę įtaką šios srities raidai), moksle ir kt. (Štitilis ir kt., 2016). Tačiau kibernetinės erdvės plėtra pasižymi ir atitinkamomis grėsmėmis, ypač susijusiomis su šioje erdvėje padarytomis nusikalstamomis veikomis. Kibernetiniai nusikaltimai laikomi vienu iš pagrindinių iššūkių ir grėsmių kibernetinėje erdvėje (Tvaronavičienė, 2018), taip pat kaip viena iš neigiamų IT plėtros pasekmių (Korauš ir kt. 2019). Pavyzdžiui, neteisėta prieiga prie informacinių sistemų, gali atverti kelius neteisėtoms mokėjimo operacijoms (pinigų pervedimams į kitas banko sąskaitas, mokėjimams už pirkinius, internetinės bankininkystės naudojimui greitiesiems kreditams gauti ir kt.), teisės į privatumą pažeidimai, komercinių paslapčių atskleidimas, elektroninių dokumentų ar duomenų klastojimas ir kt. (Marcinauskaitė, Pukanasytė, 2019).

Vartotojai labai vertina savo asmenį identifikuojančių duomenų ir kitos konfidencialios informacijos saugumą, o vartotojų privatumo ir duomenų apsauga yra neatsiejama vartotojų pasitikėjimo tęstinumo dalis. Kadangi organizacijos sėkmę vertina kaip finansinę ir materialinę naudą, reputacija yra svarbus komponentas, kurį reikia valdyti siekiant užtikrinti kibernetinį saugumą visoms suinteresuotoms šalims. Reputacija yra nematerialus turtas, turintis įtakos visoms organizacijos suinteresuotosioms šalims. Daugybė veiksnių gali turėti įtakos reputacijai, vartotojų pasitikėjimui organizacija, investuotojų pasitikėjimu ir jų suvokimu apie organizaciją kaip garbingą ir patikimą subjektą (Perera, Jin, 2022).

Reikia pabrėžti, kad kibernetinis saugumas šiais laikais nėra tik techninis klausimas. Lietuvos kibernetinio saugumo įstatyme kibernetinis saugumas apibrėžiamas kaip visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, kurių reikia imtis siekiant užkirsti kelią, aptikti, analizuoti ir reaguoti į kibernetinius incidentus, kurie apibūdinami kaip įvykis ar veikla, sukelianti ar galinti sukelti arba leisti neteisėtai prieiti prie ryšių ir informacinių sistemų, elektroninių ryšių tinklų ar pramonės procesų valdymo sistemų; gali sutrikdyti arba pakeisti informacines sistemas, įskaitant valdymo perėmimą; elektroninių ryšių tinklus ar pramoninių procesų valdymo operacijas, skirtas sunaikinti, sugadinti, ištrinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti prieigą prie elektroninės informacijos, taip pat sudaryti sąlygas pašaliniams asmenims įsisavinti ar kitaip panaudoti neviešą informaciją elektroniniu formatu (Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014). Pagrindinis minėtų veiksmų tikslas – užtikrinti greitą elektroninių ryšių tinklų, informacinių sistemų ar

pramonės procesų valdymo sistemos atkūrimą kibernetinių incidentų ar kibernetinių atakų atveju (pažiūrėti įstatyme sąvokas)

Remiantis patvirtintais kibernetinio saugumo ir kibernetinių incidentų apibrėžimais, galima nustatyti svarbiausius tikslus, siekiant užtikrinti kibernetinį saugumą. Pirmasis tikslas – konfidencialumas, užtikrinantis, kad informaciją gauti, keisti ar tvarkyti galėtų tik įgalioti asmenys. Antrasis tikslas – vientisumas, užtikrinantis, kad tik įgalioti asmenys ar procesai galėtų atlikti bet kokius sistemos pakeitimus. Trečia – sistemos ir jos operatorių valdomos sistemos ir informacijos prieinamumas. Šis tikslas užtikrina, kad tik įgalioti subjektai turės prieigą prie informacijos ar išteklių, saugomų ar naudojamų organizacijų infrastruktūroje. Įstatymais pagrįstas reguliavimas aiškiai rodo, kad kibernetinis saugumas ir valdymas yra glaudžiai susiję ir labai svarbūs kiekvienos organizacijos aspektai. Siekiant užtikrinti ypatingos svarbos infrastruktūros saugumą, pripažįstama, kad kibernetinis saugumas yra toks pat svarbus kaip ir fizinis saugumas (Limba, Plėta, 2017).

Šalis patiria didesnį kibernetinių grėsmių poveikį ir žalą, nes: jos įstatymai ir politika, susiję su kibernetiniu saugumu, nėra pakankami arba nėra veiksmingai įgyvendinami; technologijų ir infrastruktūros trūkumai ir žinių bei pasirengimo prieš išpuolius trūkumas; vartotojų mokymo bei informuotumo stoka bei institucijų ir organizacijų koordinavimo ir bendradarbiavimo stoka (Senol ir Karacuha 2020).

2007 m. plataus masto kibernetinė ataka prieš Estiją paralyžiavo daugybę vyriausybės ir įmonių svetainių. Tokio pobūdžio atakų eskalavimas išryškino vyriausybių poreikį suformuluoti nacionalines kibernetines strategijas (Attatfa ir kt., 2020). Kibernetinės erdvės saugos ir saugumo kibernetinės strategijos ir taisyklės leidžia saugiau naudotis kibernetine erdve. Nacionalinės kibernetinio saugumo strategijos (NCSS) pagerina nacionalinių infrastruktūrų ir paslaugų saugumą ir atsparumą. NCSS yra nacionalinis veiksmų planas, pagrįstas nacionaline vizija, siekiant tikslų, kurie prisideda prie kibernetinės erdvės srities saugumo, rinkinio (Jacuch, 2021).

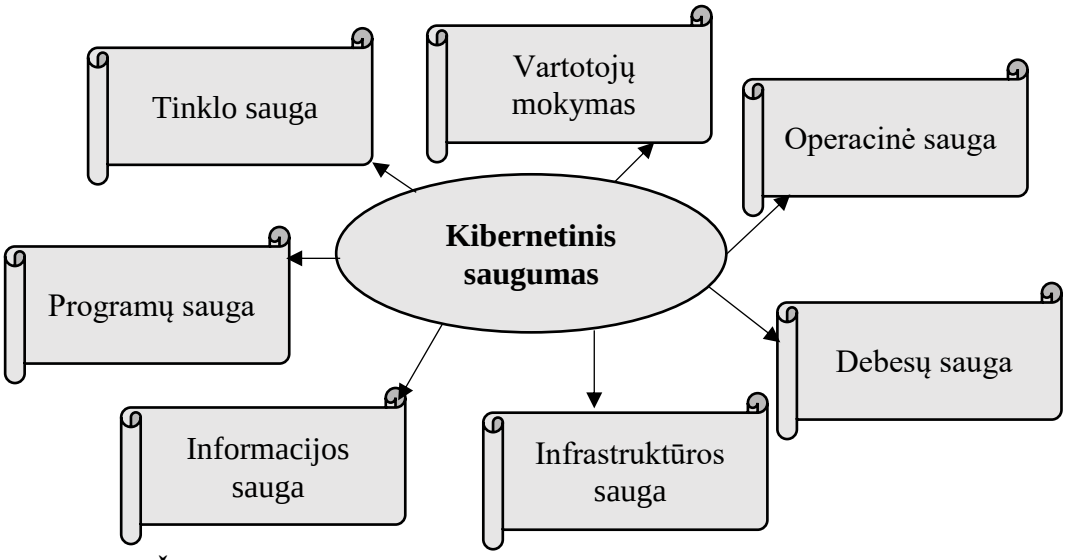
Viešajame sektoriuje saugumo pažeidžiamumas gali turėti neigiamą poveikį visiems asmenims, organizacijoms, administracijoms ir vyriausybėms. Galimos grėsmės – nuo tapatybės vagystės, sukčiavimo ir piktnaudžiavimo iki pramoninio šnipinėjimo ir teroristinės veiklos, kuri kelia grėsmę visuomenės saugumui ir tvarkai. Esant dabartinei kibernetinių grėsmių aplinkai, viešojo sektoriaus lyderiams tapo itin svarbu būti informuoti apie apsaugos priemones ir įgyvendinti šias priemones, jei jos suteikia pridėtinės vertės. Viešasis sektorius taip pat turi įgyvendinti ir tobulinti ekstremalių situacijų valdymo priemones, kad būtų sukurtas kibernetinis saugumas, o aukščiausios valdžios institucijos skatinamos priimti sprendimus sprendžiant kibernetinio saugumo problemas (Wirtz, Weyerer, 2017).

Apibendrinant galima teigti, kad kibernetinės atakos, priklausomai nuo atakos pobūdžio gali sukelti grėsmę pavieniams visuomenės asmenims, pavyzdžiui pasisavinus asmeninę informaciją ar mokėjimo duomenis, tačiau kai kurios kibernetinės atakos gali sukelti grėsmę tam tikrų institucijų

saugumui, duomenų pasisavinimui ar net šalies saugumui. Todėl valdant kibernetinių atakų keliamą riziką bei didinant kibernetinį saugumą šalys ir institucijos imasi įvairių prevencinių priemonių, užtikrinančių informacijos, duomenų, programų bei sistemų apsaugą.

1.3. Kibernetinių atakų valdymo metodai ir priemonės: Lietuvos atvejis

Kibernetinis saugumas yra svarbi kiekvienos įmonės ir organizacijos infrastruktūros problema. Kibernetinis saugumas apima praktines priemones, skirtas apsaugoti informaciją, tinklus ir duomenis nuo vidinių ar išorinių grėsmių. Kibernetinio saugumo specialistai saugo tinklus, serverius, intranetus ir kompiuterių sistemas. Kibernetinis saugumas užtikrina, kad tik įgalioti asmenys turėtų prieigą prie informacijos (Li, Liu, 2021). Norint geriau apsisaugoti, būtina žinoti kibernetinio saugumo tipus, 1 paveiksle pavaizduoti skirtingi kibernetinio saugumo tipai.



Šaltinis: sudaryta pagal Li ir Liu, 2021

2 pav. Kibernetinio saugumo sritys

Tinklo sauga apsaugo kompiuterių tinklą nuo trikdžių, kurie gali būti kenkėjiškos programos arba įsilaužimas. Tinklo sauga – tai sprendimų rinkinys, leidžiantis organizacijoms apsaugoti kompiuterių tinklus nuo įsilaužėlių, organizuotų užpuolikų ir kenkėjiškų programų (Li, Liu, 2021). Programų sauga: naudojant aparatinę ir programinę įrangą (pvz., antivirusines programas, šifravimą ir ugniasienes) sistema apsaugoma nuo išorinių grėsmių, kurios gali trukdyti kurti programas. Informacijos sauga: apsaugo fizinius ir skaitmeninius duomenis nuo neteisėtos prieigos, atskleidimo, netinkamo naudojimo, neteisėtų pakeitimų ir ištrynimo (Ogbanufe, 2021).

Operacinė sauga: apima procesus ir sprendimus, priimtus siekiant kontroliuoti ir apsaugoti duomenis. Pavyzdžiui, vartotojo leidimai prisijungiant prie tinklo arba procesai, nurodantys, kada ir kur informacija gali būti saugoma arba bendrinama (Ogbanufe, 2021). Debesų sauga: apsaugo debesyje esančią informaciją (pagal programinę įrangą). Vartotojų mokymas: susiję su nenuspėjamais

kibernetinio saugumo aspektais, būtent asmenimis. Kiekvienas gali atsitiktinai patekti į apsaugos sistemą. Mokymas vartotoją pašalinti įtartinus priedus iš el. laiško, neprisijungti prie anoniminių USB ir kitų svarbių problemų turėtų būti bet kurios įmonės saugumo plano dalis (Li, Liu, 2021).

Visų pirma, apibūdinant kibernetinio saugumo sampratą, pateikiamos šios bendrosios savybės ir nuorodos (Gavėnaitė – Sirvydienė, Miečinskienė, 2021):

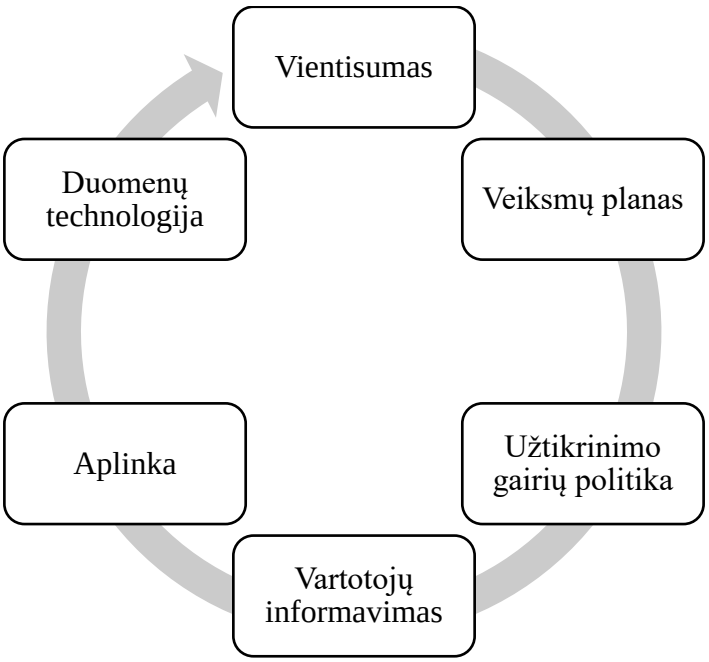
1. galimybė apsaugoti ar apginti aplinką nuo kibernetinių atakų;

2. vientisumo, informacijos konfidencialumo prieinamumo prevencija verslo aplinkoje;

3. visas priemones ir veiklą, kurios turėtų būti skirtos naudotojams ir kibernetinės erdvės apsaugai;

4. rizikos ir galimos žalos prevencija, siekiant apsaugoti ir prireikus atkurti informaciją, duomenis, internetinę saugyklą, elektroninių ryšių sistemas ir paslaugas.

Galima nurodyti, kad kibernetinio saugumo tikslai yra apsaugoti kibernetinę erdvę (įskaitant programinę ir techninę įrangą) nuo bet kokios kibernetinės grėsmės ar kibernetinės atakos. Požiūris ir veiksmai, susiję su kibernetinio saugumo valdymo veiksmais, kurių laikosi įmonės ir apskritys, siekdamos apsaugoti kibernetinėje erdvėje naudojamos programinės įrangos ir aparatinės įrangos konfidencialumą, vientisumą ir prieinamumą (Gavėnaitė – Sirvydienė, Miečinskienė, 2021). Koncepcija apima gaires, reikalavimus ir apsaugos priemonių rinkinius, technologijas, priemones ir darbuotojų mokymą, kad būtų užtikrinta geriausia įmonės kibernetinės erdvės ir jos vartotojų apsauga (žr. 3 pav.).



Šaltinis: sudaryta pagal Gavėnaitė – Sirvydienė, Miečinskienė, 2021

3 pav. Kibernetinio saugumo lygiai

3 paveiksle pateikiamos pagrindinės kibernetinio saugumo sąvokos, apimančios skirtingus aspektus: vientisumas/prieinamumas – reiškia, kaip svarbu ir būtina pasiekti bet kokius įrankius, informaciją ir duomenis; veiksmas/požiūris – atspindi protokolą ar strategiją dėl kibernetinio saugumo ir kibernetinės rizikos valdymo; užtikrinimas / gairės / politika – svarbios kibernetinio saugumo koncepcijos dalys, apimančios išsamią informaciją ir priemones šiai kibernetinei rizikai valdyti; vartotojas/organizacija – atstovauja šios koncepcijos žmogiškąjį kapitalą; aplinka – tai gali būti verslo aplinka; pramonės šaka, kurioje veikia įmonė, kibernetinio saugumo aplinka; turtas/duomenys/technologija – reiškia visą techninę ir programinę įrangą, kuri turėtų būti apsaugota nuo kibernetinės rizikos (Gavėnaitė – Sirvydienė, Miečinskienė, 2021).

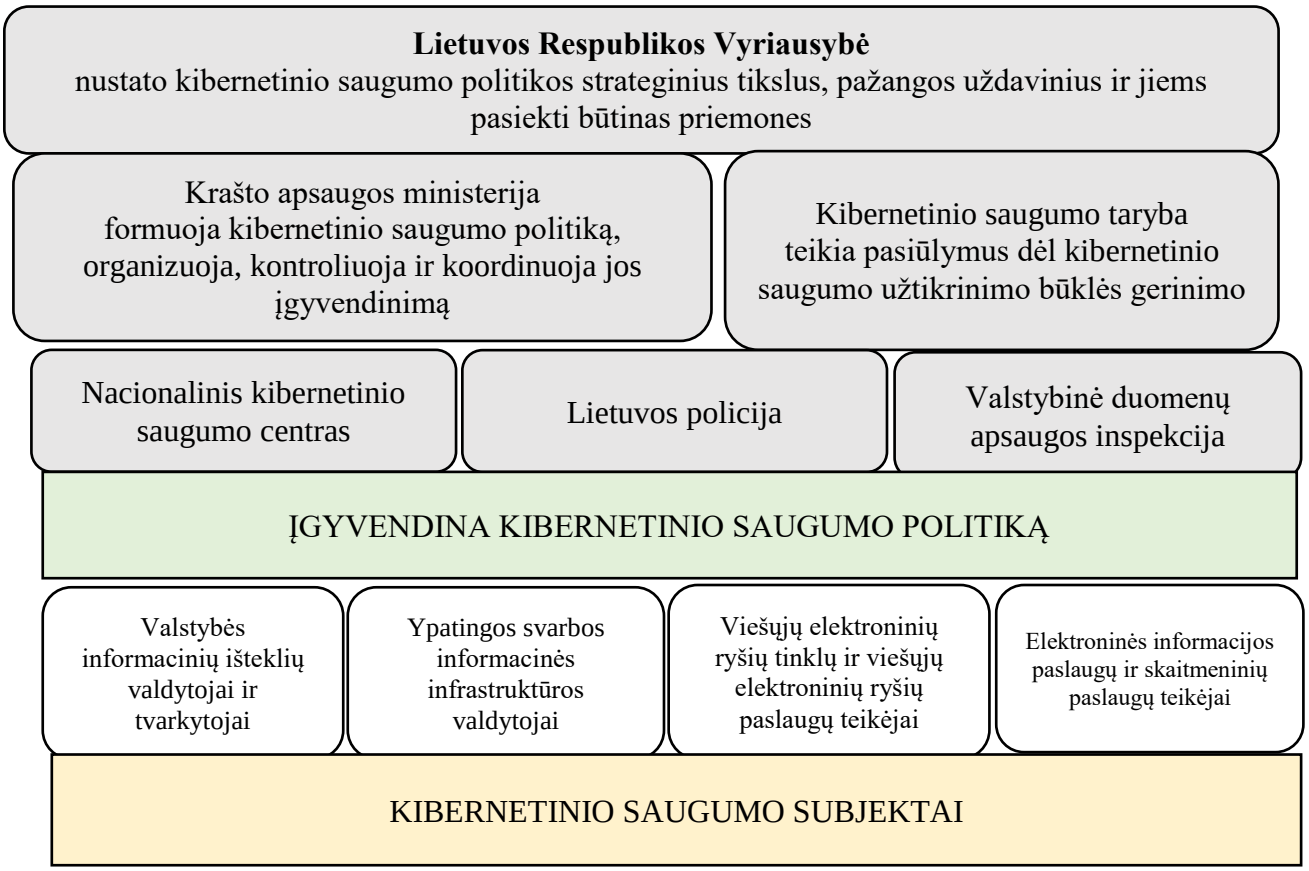
Kibernetinis saugumas reiškia ryšį tarp skirtingų rodiklių, tokių kaip rizikos įvertinimo priemonės, rizikos valdymo metodikos, įgūdžiai ir politika siekiant bendro tikslo – turto, jautrios informacijos ar duomenų saugumo gerinimo. Be to, svarbi dalis yra užtikrinti, kad grįžtamasis ryšys apie informacijos konfidencialumą, prieinamumą ir atitiktį būtų renkamas ir pateikiamas atsakingoms institucijoms (Cavelty, 2018). Veiksminga kibernetinio saugumo strategija reikalauja aukšto lygio visų atskaitingų organizacijos elementų įsitraukimo.

Lietuvos nacionalinėje kibernetinio saugumo strategijoje (toliau – Strategija) nustatytos pagrindinės nacionalinės kibernetinio saugumo politikos kryptys viešajame ir privačiame sektoriuose. Įgyvendinant strategiją siekiama stiprinti valstybės kibernetinį saugumą ir plėtoti kibernetinės gynybos pajėgumus, užtikrinti nusikalstamų veikų, padarytų naudojant kibernetinio saugumo objektus (toliau – nusikalstamos veikos kibernetinėje erdvėje), prevenciją ir tyrimą, skatinti kibernetinio saugumo kultūrą ir inovacijų plėtrą, stiprinti glaudų viešojo ir privataus sektorių bei tarptautinį bendradarbiavimą ir užtikrinti tarptautinių įsipareigojimų vykdymą kibernetinio saugumo srityje šalyje iki 2023 m.

Lietuvoje kibernetinio saugumo principus, kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijas, šių institucijų įgaliojimus, kibernetinio saugumo subjektų pareigas, tarpinstitucinį bendradarbiavimą, ryšių ir informacinių sistemų spragų paieškos, pranešimo apie jas ir kibernetinius incidentus pagrindus nuo 2015 m. reglamentuoja Kibernetinio saugumo įstatymas. Pagal šiame įstatyme įtvirtintą sampratą kibernetiniu saugumu yra laikoma visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, kuriomis siekiama išlaikyti atsparumą veiksniams, kibernetinėje erdvėje keliantiems grėsmę ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, ryšių ir informacinių sistemų netrikdomam veikimui, valdymui arba paslaugų šiomis sistemomis teikimui, taip pat kuriomis siekiama atkurti įprastinę ryšių ir informacinių sistemų veiklą.

Kibernetinio saugumo srities valdymą Lietuvoje atlieka Vyriausybė, srities politiką formuoja Krašto apsaugos ministerija, įgyvendina Nacionalinis kibernetinio saugumo centras, Lietuvos policija, Valstybinė duomenų apsaugos inspekcija ir kitos įgaliotos valstybės institucijos, kibernetinio saugumo

subjektai atsako už jų valdomų ryšių ir informacinių sistemų ar teikiamų paslaugų kibernetinį saugumą, užtikrina jų atitiktį nustatytiems kibernetinio saugumo reikalavimams (žr. 4 pav.).



Šaltinis: Valstybės kontrolė pagal Kibernetinio saugumo įstatymą

4 pav. Kibernetinio saugumo sistemos dalyviai

Pagal Tarptautinės telekomunikacijų sąjungos 2021 m. paskelbtus tarptautinio kibernetinio saugumo indekso rezultatus Lietuva priklauso stipriausiųjų kibernetinio saugumo srityje šalių dešimtukui: Lietuva tarp pasaulio valstybių užėmė 6, tarp Europos valstybių – 4 vietą. Tarptautinis kibernetinio saugumo indeksas parodo, kad šalyje galioja palyginti gera kibernetinio saugumo teisinė bazė, bet indekso skaičiavimo metodika neapima realios šio saugumo būklės vertinimo, t.y., kaip valstybės institucijos, ypatingos svarbos informacinės infrastruktūros valdytojai ir kitos organizacijos realiai yra pasirengusios atremti kibernetines atakas ir užtikrinti valdomos informacinės infrastruktūros ir tvarkomų informacinių išteklių saugumą.

Siekiant užtikrinti Nacionalinėje kibernetinio saugumo strategijoje, patvirtintoje Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Strategija), iškeltų tikslų ir uždavinių kibernetinio saugumo srityje įgyvendinimą, Vyriausybės 2019 m. liepos 3 d. nutarimu Nr. 709 patvirtintas 3 metų Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinis veiklos planas (toliau – TVP). TVP įgyvendina ne tik TVP koordinatorius – Lietuvos Respublikos krašto

apsaugos ministerija (toliau – KAM), bet ir jai pavaldūs KAM padaliniai, kitos valstybės institucijos ir įstaigos ir jiems pavaldūs padaliniai – Lietuvos Respublikos vidaus reikalų ministerija (toliau – VRM), Lietuvos Respublikos Vyriausybės kanceliarija (toliau – LRVK), Lietuvos Respublikos užsienio reikalų ministerija (toliau – URM), Lietuvos Respublikos ryšių reguliavimo tarnyba (toliau – RRT), Lietuvos Respublikos teisingumo ministerija (toliau – TM), Lietuvos Respublikos švietimo, mokslo ir sporto ministerija (toliau – ŠMSM).

Siekiant sutelkti valstybės institucijų ir įstaigų pastangas užtikrinti galimybę Lietuvos visuomenei saugiai naudotis informacinių ir ryšių technologijų teikiamomis galimybėmis, efektyviai ir laiku identifikuoti kibernetinius incidentus, užkirsti kelią jų atsiradimui ir plitimui, valdyti kibernetinių incidentų sukeltas pasekmes, TVP įgyvendinančių institucijų veikla buvo orientuota į 5 Strategijoje numatytus tikslus:

- stiprinti valstybės kibernetinį saugumą bei kibernetinių gynybos pajėgumų plėtrą;
- užtikrinti nusikalstamų veikų kibernetinėje erdvėje prevenciją, užkardymą ir tyrimą;
- skatinti kibernetinio saugumo kultūrą ir inovacijų plėtrą;
- stiprinti glaudų viešojo ir privataus sektorių bendradarbiavimą;
- stiprinti tarptautinį bendradarbiavimą ir užtikrinti tarptautinių įsipareigojimų kibernetinio saugumo srityje vykdymą.

2020 m. visame pasaulyje paplitęs COVID-19 virusas ir jo pasekmės sukėlė naujų iššūkių ir įtampą ne tik kibernetinio saugumo užtikrinimo srityje, bet taip pat turėjo įtakos suplanuotų TVP priemonių vykdymui. Nors 2020 m., įgyvendinant TVP 1 priede numatytas priemones, dalyvavo daugiau asignavimų valdytojų nei pernai – prie KAM, VRM, URM, LRVK ir RRT savo vykdomomis priemonėmis su nustatytais asignavimais prisidėjo TM ir ŠMSM, – tačiau dalis suplanuotų priemonių buvo neįvykdytos arba įvykdytos iš dalies ir tam iš dalies įtakos turėjo su COVID-19 viruso plitimo sustabdymu susiję visuomeninio gyvenimo suvaržymai.

2019–2021 m. užregistruota ypač daug kibernetinių atakų prieš Lietuvos valdžios institucijas, ypatingos svarbos informacinę infrastruktūrą, valstybės informacinius išteklius ir jų pagrindu veikiančias skaitmenines paslaugas. Nacionalinio kibernetinio saugumo centro duomenimis, 2019 m. buvo užfiksuotas 3 241 kibernetinis incidentas, 2020 m. – 4 330, 2021 m. – 4 088, iš viso 11 659 incidentai per tris metus.

Toliau šiame darbe analizuojamos kibernetinio saugumo užtikrinimo teisinės priemonės nacionaliniu bei tarptautiniu lygmeniu, aptariamos nacionalinės strategijos gairės bei reikšmė užtikrinant kibernetinį saugumą.

1.3.1. Kibernetinio saugumo teisinės priemonės

Pirmoji integruota ES kibernetinio saugumo strategija sukurta 2013 m. – ES kibernetinio saugumo strategija: atvira, saugi kibernetinė erdvė, kurioje nustatomos pagrindinės vertybės ir pagrindiniai Sąjungos prioritetai šioje srityje. Šiame dokumente ES atskleidžia, kad reikia priimti teisės aktus kibernetinio saugumo srityje, pabrėždama, kad visoje ES vis dar yra spragų, ypač nacionalinių pajėgumų, tarpvalstybinių incidentų koordinavimo ir privataus sektoriaus dalyvavimo bei pasirengimo srityse (ES kibernetinio saugumo strategija, 2013). 2016 m. Europos Parlamentas ir Europos Komisija paskelbė TIS direktyvą, kurioje nustatomos tam tikros priemonės, kurių reikia imtis siekiant aukšto bendro tinklų ir informacinių sistemų saugumo lygio Sąjungoje, siekiant pagerinti vidaus rinkos veikimą (Direktyva (ES) 2016/1148). Naujausias toks dokumentas, išleistas 2019 m., yra ES kibernetinio saugumo įstatymas, kuriame nustatyti nauji ENISA – ES kibernetinio saugumo agentūros – tikslai ir atsakomybė, taip pat „Europos kibernetinio saugumo sertifikavimo schemų kūrimo pagrindas, siekiant užtikrinti tinkamą lygį. IRT produktų, paslaugų ir procesų kibernetinio saugumo Sąjungoje siekiant „išvengti vidaus rinkos susiskaidymo“ dėl kibernetinio saugumo sertifikavimo. Taigi reikia išanalizuoti tris strateginius kibernetinio saugumo dokumentus, kurie skiriasi ir pagal tipą, ir pagal objektą: vieną rezoliuciją su bendromis nuostatomis ir gairėmis, vieną direktyvą, skirtą išskirtinai vienam kibernetinio saugumo komponentui – tinklų ir informacinių sistemų apsaugai, ir reglamentą dėl kibernetinio saugumo. Kitos dvi kryptys: viena vertus, stiprinti svarbią Europos kibernetinio saugumo instituciją ir, kita vertus, sukurti naują prevencinių priemonių rinkinį.

Europos Sąjungos kibernetinio saugumo strategija. Išdėstyti tikslai susiję su: pagrindinių ES vertybių išplėtimu į elektroninę erdvę; pagrindinių teisių, žodžio laisvės, asmens duomenų ir privatumo apsauga; visiems užtikrinti prieigą prie interneto; demokratinis ir veiksmingas valdymas, kad interneto ištekliai, protokolai ir standartai būtų gerai valdomi; ir bendra atsakomybė užtikrinti saugumą. Kitas strateginis prioritetas, į kurį turi atkreipti valstybės narės dėmesį, yra „Kibernetinės gynybos politikos ir pajėgumų, susijusių su Bendros saugumo ir gynybos politikos (BSGP) sistema, plėtra“, numatant keletą pagrindinių veiksmų, pavyzdžiui: „įvertinti operatyvinius ES kibernetinės gynybos reikalavimus ir skatinti ES kibernetinės gynybos pajėgumus ir technologijas“, „plėtoti ES kibernetinės gynybos politikos sistemą“, „skatinti dialogą ir koordinavimą tarp civilių ir karinių veikėjų ES“ ir „užtikrinti dialogą su tarptautiniais partneriais“. Be to, pagal prioritetą „Investicijų į mokslinius tyrimus ir plėtrą bei inovacijas skatinimas“ valstybės narės turėtų: „plėtoti gerą praktiką, kad būtų panaudota viešojo administravimo perkamoji galia“ ir „skatinti ankstyvą pramonės ir akademinės bendruomenės dalyvavimą kuriant ir koordinuojant sprendimus“. Dokumente nepateikiamas kibernetinio saugumo apibrėžimas, tačiau minima, kad jame dažniausiai nurodomos apsaugos priemonės ir veiksmai, kurie gali būti naudojami siekiant apsaugoti kibernetinį domeną tiek civilinėje, tiek karinėje srityse nuo tų grėsmių, kurios yra susijusios arba gali pakenkti jos tarpusavyje priklausomiems tinklams ir informacijos

infrastruktūrai, kad būtų išsaugotas tinklų ir infrastruktūros prieinamumas ir vientisumas bei juose esančios informacijos konfidencialumas.

Direktyva (ES) 2016/1148 dėl aukšto bendro tinklo ir informacinių sistemų saugumo lygio visoje Sąjungoje priemonių. Taikant visiškai kitokį požiūrį, daugiau dėmesio skiriant valstybių narių atsakomybei, TIS direktyvoje nustatytas priemonių rinkinys, kurio reikia imtis siekiant apsaugoti informacijos tinklus ir sistemas Europos Sąjungoje. Vykdydamos šią iniciatyvą, valstybės narės privalo priimti nacionalines tinklų ir informacinių sistemų saugumo strategijas, jos turėtų bendradarbiauti ir keistis informacija bei įsteigti nacionalines kompetentingas institucijas, atsakingas už tinklų ir informacinių sistemų saugumą. Siekiant padėti valstybėms priimti savo nacionalines TIS saugumo strategijas, direktyvoje pateikiamas klausimų, į kuriuos reikėtų atsižvelgti, rinkinys, pavyzdžiui: tikslai ir prioritetai; valdymo sistema, skirta vyriausybės organų ir kitų susijusių subjektų tikslams ir prioritetams, vaidmenims ir pareigoms pasiekti; į pasirengimą, reagavimą ir atkūrimą orientuotos priemonės, įskaitant viešojo ir privataus sektorių bendradarbiavimą; švietimo, informuotumo didinimo ir mokymo programos; tyrimų ir plėtros planai; rizikos vertinimo planas; ir atitinkamų subjektų, dalyvaujančių įgyvendinant strategiją, sąrašas. Kiekviena valstybė narė turi nustatyti nacionalinius esminių paslaugų teikėjus kiekvienam sektoriui ir padaliniams, todėl direktyvoje taip pateikiami kriterijai. Direktyvoje pateikiamas konkrečių terminų apibrėžimų rinkinys, nenurodant kibernetinio saugumo. Vietoj to yra terminas „tinklo ir informacinių sistemų saugumas“, kuris apibrėžiamas kaip „tinklo ir informacinių sistemų gebėjimas tam tikru pasitikėjimo lygiu atsispirti bet kokiems veiksmams, kurie kelia pavojų saugomų arba perduodamus ar tvarkomus duomenis arba susijusias paslaugas, kurias siūlo tie tinklai ir informacinės sistemos arba kurios per jas pasiekiamos.

Reglamentas (ES) 2019/881 dėl ENISA ir dėl informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo. Kibernetinio saugumo aktas, kurio taikymo sritis iš esmės tokia pati kaip ir kiti du pirmiau minėti dokumentai, pasiekti aukštą kibernetinio saugumo, kibernetinio atsparumo ir pasitikėjimo Sąjungoje lygį ir yra privalomas valstybėms narėms, susideda iš dviejų pagrindinių komponentų: ENISA stiprinimo (Europos Sąjungos kibernetinio saugumo agentūra), viena vertus, ir teikia paramą valstybėms narėms sprendžiant kibernetines grėsmes, sukuriant bendras Europos kibernetinio saugumo sertifikavimo sistemas IRT produktams, paslaugoms ir procesams. Remiantis šiuo dokumentu, ENISA yra nuolatinis, nepriklausomas, mokslinis ir techninis kibernetinio saugumo kompetencijos centras, padedantis ES institucijoms ir valstybėms narėms plėtoti ir įgyvendinti su kibernetiniu saugumu susijusią Sąjungos politiką ir skatinantis naudoti Europos kibernetinio saugumo sertifikatus. Europos kibernetinio saugumo sertifikavimas yra nauja Europos Sąjungos politika, kurią sudaro išsamus taisyklių, techninių reikalavimų, standartų ir procedūrų rinkinys, nustatytas Sąjungos lygiu ir taikomas konkrečių IRT produktų, IRT paslaugų ir IRT sertifikavimui arba atitikties vertinimui. Reglamente, be kitų terminų, taip pat pateikiamas kibernetinio saugumo apibrėžimas: veikla, reikalinga

tinklų ir informacinėms sistemoms, tokių sistemų naudotojams ir kitiems kibernetinių grėsmių paveiktiems asmenims apsaugoti (Jacuch, 2021).

ES kibernetinio saugumo formavimo procesas tęsiasi. 2020 m. gruodžio 16 d. ES pateikė tris pasiūlymus: ES skaitmeninio dešimtmečio kibernetinio saugumo strategiją, direktyvą dėl aukšto bendro kibernetinio saugumo lygio visoje Sąjungoje priemonių, vadinamą TIS2 direktyva (Europos Komisija 2020), ir direktyvą dėl ypatingos svarbos subjektų. 2021 m. birželio 10 d. Europos Parlamentas (EP) priėmė rezoliuciją dėl ES skaitmeninio dešimtmečio kibernetinio saugumo strategijos (Europos Parlamentas 2021), kuria siekiama, kad sujungti produktai ir susijusios paslaugos būtų saugios, atsparios kibernetiniams incidentams ir greitai pataisomos, jei būtų aptiktos pažeidžiamumo vietos (Pingen, 2021). Strategijos tikslas – užtikrinti globalų ir atvirą internetą su tvirtomis apsaugos priemonėmis. Remiantis ankstesne strategija padaryta pažanga, joje pateikiami pasiūlymai dėl trijų pagrindinių priemonių – reguliavimo, investicijų ir politikos iniciatyvų – naudojimo trijose srityse: atsparumas, technologinis suverenitetas ir lyderystė, „veiklinių gebėjimų prevencijai, atgrasymui kūrimas ir pasaulinės ir atviros kibernetinės erdvės pažanga stiprinant bendradarbiavimą (Europos Komisija 2020). Strategija parodo tvirtą ES įsipareigojimą nuolat plėtoti savo gynybinius kibernetinius pajėgumus ir intensyvinti bendradarbiavimą tarp savo narių ir su trečiosiomis šalimis, regiono nacionalinėmis ir tarptautinėmis organizacijomis, taip pat įvairiomis suinteresuotosiomis šalimis.

TIS2 direktyvoje nurodomi „esminiai subjektai“ ir „svarbūs subjektai“, pristatomas ES kibernetinių krizių ryšių organizacijų tinklas (CyCLONE), CSIRT tinklas ir bendradarbiavimo grupė, siekiant padėti valdyti didelio masto incidentus Europos Sąjungos lygmeniu. EU-CyCLONE atlieka papildomą funkciją – koordinuoti konkrečių subjektų pažeidžiamumų atskleidimą ES lygmeniu. NIS2 direktyva siekiama padidinti kibernetinio saugumo lygį ES. Bendradarbiavimas ES kibernetinio saugumo srityje apima teisinės bazės suderinimą. Iki 2030 m. planuojama sukurti patrauklias reguliavimo sąlygas duomenų potencialui didinti. Siekiama sukurti bendrą Europos duomenų erdvę – tikrą bendrąją duomenų rinką, atvirą duomenims iš viso pasaulio – kurioje asmeniniai ir neasmeniniai duomenys, įskaitant neskelbtinus verslo duomenis, būtų saugūs, o įmonės taip pat galėtų lengvai pasiekti beveik be galo daug aukštos kokybės pramonės duomenų, skatinančių augimą ir kuriant vertę, tuo pačiu sumažinant žmogaus anglies pėdsaką ir aplinką (Europos Komisija, 2020).

Apibendrinant galima teigti, kad Europos Sąjungos mastu kibernetinio saugumo užtikrinimui modernizuojama ir tobulinama teisinė bazė, atsižvelgiant į vykstančius pokyčius bei informacinių technologijų raidą ir saugumui keliamas grėsmes. Tačiau ES priimti teisės aktai bei reglamentai turi būti inkorporuojami į valstybių narių teisinę bazę, siekiat atitikti ES keliamus reikalavimus. Dauguma valstybių narių ES galiojančių teisės aktų pagrindu tobulina priimtus kibernetinio saugumo įstatymus bei atnaujina nacionalines kibernetinio saugumo strategijas.

1.3.2. Kibernetinio saugumo strategija ir politika

Terminas „politika“ vartojamas įvairiose su kibernetiniu saugumu susijusiose srityse ir reiškia informacijos platinimo taisykles ir reglamentus, privataus sektoriaus duomenų išsaugojimo tikslus, technologijų valdymo sistemos veikimo strategijas. Tačiau šios srities darbuose terminas kibernetinio saugumo politika vartojamas įvairiems tikslams. Kaip ir frazė „kibernetinė erdvė“, nėra fiksuoto kibernetinio saugumo politikos apibrėžimo (Tam ir kt., 2021). Kibernetinio saugumo politika yra priimta pagal galiojančią šalies reguliavimo sistemą ir oficialiai taikomas priemones atitinkamose reguliavimo institucijos srityse. Saugumo politikos komponentai skiriasi priklausomai nuo politikos spektro (Cheng ir kt., 2020). Pavyzdžiui, nacionalinė kibernetinio saugumo politika apima visus savo srityje dirbančius piliečius ir iš dalies užsienio verslininkus, tačiau įmonių kibernetinis saugumas taikomas tik tiems darbuotojams, kurie dirba arba turi teisinę sutartį ir turi reguliuoti savo elgesį įmonės atžvilgiu. Netgi negalima tikėtis, kad išteklių tiekėjai, kurie visiškai pasikliauja vienu klientu, laikysis klientų saugumo politikos, nebent būtų sudaryta oficiali sutartis (Alghamdi, 2021). Saugumo politikos turinį lemia atitinkamos reguliavimo institucijos tikslai. Nacionalinio saugumo tikslai labai skiriasi nuo įmonių saugumo tikslų. Politikos aiškinimo ir registravimo būdą nustato įgyvendinančios organizacijos, o jos patvirtinimą – reguliavimo taryba ir atitinkami komponentai. Valdžioje procesas, kurio metu tikslai tampa politika, ir procesas, kurio metu politika įtraukiama į teisę, skiriasi. Tačiau įmonėse įprasta turėti centralizuotą saugos padalinį, kuris yra atsakingas už kibernetinio saugumo politiką ir susijusius standartus bei sprendimus. Apsaugos padalinio standartai ir sprendimai įmonėse tampa taisyklių vadovu (Li, Liu, 2021).

Siekdamos prisitaikyti prie besiformuojančių skaitmeninių ekonomikų, vietos valdžios institucijos patiria panašius savo paslaugų, procesų, išteklių, organizacinės kultūros ir kompetencijų pokyčius, siekdamos (Polityka Cyfrowa Miasta Stołecznego Warszawy, 2020): (1) pagerinti prieinamumą ir viešųjų paslaugų kokybę, (2) racionalizuoti vietos valdžios funkciją, (3) remti strateginių ir operatyvinių sprendimų priėmimo procesus, (4) didinti vietos valdžios veiklos skaidrumą, (5) įtraukti gyventojus į vietos valdžios bendruomenės gyvenimą per IRT technologijas. Tokiomis pertvarkomis siekiama darnaus vystymosi tikslų.

Tiek telekomunikacijų infrastruktūros ir tinklų sukūrimas, tiek jų saugumo užtikrinimas visiems vartotojams reikalauja didelių finansinių išlaidų. Tai kelia problemų, nes, viena vertus, privatūs verslininkai ne visada suinteresuoti patirti tokias išlaidas, kita vertus, šių prekių ir paslaugų teikimas rinkos sąlygomis apribotų dalies visuomenės prieigą prie jų. Todėl šias užduotis turi perimti viešojo administravimo įstaigos, veikiančios viešąjį interesą, o jų tikslas – neutralizuoti vadinamąją skaitmeninę atskirtį. Tačiau vis labiau plintantis IRT technologijų naudojimas sukuria papildomą problemą, susijusią su IRT ar kibernetinio saugumo užtikrinimu ekonomikoje, įskaitant vietos valdžios padalinius. Kibernetinio saugumo incidentų ir kibernetinių atakų prieš viešojo administravimo įstaigas, apie kurias

pranešama, skaičius kasmet auga. Todėl šie subjektai privalo užtikrinti IRT tinklų ir sistemų saugumą (Chałubińska-Jentkiewicz, 2021). Būtina sukurti saugos programinę įrangą, apsaugančią nuo kibernetinių atakų, ir paskirti asmenis, atsakingus už kibernetinio saugumo politikos laikymosi stebėjimą (Chatfield & Reddick, 2019). Saugumas ir kibernetinis saugumas tampa pagrindinėmis problemomis ekstremaliomis situacijomis, tokiomis kaip pastaroji COVID-19 pandemija.

Siaurąja prasme kibernetinis saugumas yra duomenų ir informacijos (išteklių) apsaugos praktika. Kibernetinis saugumas šiuo metu laikomas vienu didžiausių socialinių ir technologinių iššūkių, su kuriais šiuo metu susiduria viešosios institucijos. Jis turi strateginę reikšmę ne tik tinkamam valstybės ir vietos valdžios funkcionavimui, bet ir privačioms įmonėms bei gyventojams, besinaudojantiems elektroninio administravimo paslaugomis (Karpiuk, 2021). Literatūroje, vyriausybiniuose dokumentuose, nepriklausomų institucijų rengiamose ataskaitose vis dažniau pabrėžiama būtinybė užtikrinti kibernetinį saugumą vykdant viešojo administravimo funkcijas, įskaitant vietos valdžios padalinius. Nepaisant to, realus tiek valdžios institucijų, tiek visuomenės supratimas apie grėsmes yra ribotas. Panašu, kad tai patvirtina ir faktas, kad vis dar yra palyginti mažai kibernetinių nusikaltimų ir kibernetinio saugumo tyrimų, ypač vietos valdžios lygmeniu. Didžiausias iššūkis tyrėjams yra oficialios statistikos apie vietos valdžios padaliniuose vykdomų kibernetinių atakų skaičių ir tipus bei centrinės ir vietos valdžios institucijų gebėjimą atremti tokias atakas. Dalis šios informacijos yra konfidenciali (Chodakovska, Kandula, 2022).

Apibendrinant galima teigti, kad formuojant kibernetinio saugumo politiką bei strategiją yra iškeliami atitinkami kibernetinio saugumo tikslai, apimantys viešąjį bei privatų sektorių, visuomenę, nacionalinį šalies saugumą. Tačiau moksliniuose tyrimuose pabrėžiama, kad kibernetinis saugumas sukelia viešajam sektoriui socialinių, technologinių bei ekonominių iššūkių, todėl strategijos įgyvendinimas turėtų apimti ir visuomenės švietimą kibernetinio saugumo tematika.

1.4. Kibernetinių atakų valdymo užsienio šalyse geroji patirtis

Nacionalinė kibernetinio saugumo strategija yra pagrindinis vyriausybės dokumentas, atspindintis interesus ir saugumo principus kibernetinėje erdvėje ir nustatantis būsimų teisės aktų, politikos krypčių, standartų ir kitų rekomendacijų, susijusių su saugumu ir kibernetiniu saugumu, pagrindą. Bet kurios ES narės strategija turi apimti visus kibernetinės erdvės aspektus, kad būtų užtikrintas visapusiškas požiūris į ateities kibernetines problemas. ENISA požiūris į kibernetinės erdvės poreikius prasideda nuo pagrindinių ES vertybių, tokių kaip demokratija ir žmogaus teisės aukščiausiame lygmenyje, o toliau – nuo pagrindinių piliečių poreikių.

Pagal Pasaulinį kibernetinio saugumo indeksą (GCI), Jungtinė Karalystė yra pirmoje sąrašo vietoje (ITU, 2019). Pasirinkimas iškelti JK į pirmą vietą rodo rimtą šalies įsipareigojimą investuoti į kibernetinio saugumo plėtrą. Vyriausybės išleistoje 2015 m. Nacionalinio saugumo strategijoje ir

Strateginėje gynybos ir saugumo apžvalgoje galima rasti dalį, skirtą ypatingai svarbiai nacionalinei infrastruktūrai (CNI) ir energetiniam saugumui. Strategijoje minimas įsipareigojimas užtikrinti CNI atsparumą būsimoms grėsmėms, tokioms kaip elektros energijos tiekimo sutrikimai ir pan. Be to, vyriausybė įkūrė Nacionalinės infrastruktūros apsaugos centrą, kurio tikslas – sumažinti nacionalinės infrastruktūros pažeidžiamumą, ypač CIP (CPNI, 2020), kartu su Nacionaliniu kibernetinio saugumo centru 2016 m. (Nacionalinis kibernetinio saugumo centras, 2020). Analizė, atlikta dėl JK požiūrio į ypatingos svarbos infrastruktūros objektų apsaugos valdymo aspektus, atskleidė savotišką situaciją. Pagrindiniai dokumentai, susiję su šia tema, buvo antrasis ir trečiasis Jungtinio komiteto dėl nacionalinio saugumo strategijos dėl kibernetinio saugumo įgūdžių ir JK kritinio nacionalinio komiteto ataskaitos. Dokumentai patvirtina, kad nors 2016 metais Vyriausybė paskelbė Nacionalinę kibernetinio saugumo strategiją 2016–2021 metams, yra detalizuojamos sisteminės kibernetinių įgūdžių trūkumo problemos. Užfiksuojamos problemos yra susijusios su išsilavinimo ir nusistovėjusių karjeros kibernetinio saugumo tema trūkumu, todėl nėra pakankamai Anglijos piliečių, kurie turi reikiamų įgūdžių ir gebėjimų dirbti ypatingos svarbos nacionalinės infrastruktūros sektoriuje. Trečiojoje ataskaitoje taip pat teigiama, kad Vyriausybės nustatytas ypatingos svarbos nacionalinės infrastruktūros objektų apibrėžimas yra per platus ir nepadeda nustatyti infrastruktūros tipų, kuriuos reikia labiausiai saugoti (Jungtinis Nacionalinio saugumo strategijos komitetas, 2018).

Antroji šalis pasaulyje pagal kibernetinio saugumo lygį, remiantis GCI 2018, yra Jungtinės Amerikos Valstijos. Tiesą sakant, JAV vyriausybė paskyrė Tėvynės saugumo departamentą kibernetiniam saugumui, Kibernetinio saugumo ir infrastruktūros saugumo agentūrą (CISA), kuri turi parengusi Nacionalinį infrastruktūros apsaugos planą (NIPP), kad sudarytų specialią ir išsamią CIP strategiją (CISA, 2018). Pirmiausia reikia pasakyti, kad yra daug dokumentų, visiškai skirtų ypatingos svarbos infrastruktūroms: svetainė siūlo plačią prieigą prie pagrindinių paslaugų ir galimybių. Iš išvardintų Valstybės saugumo departamentas pirmenybę teikia infrastruktūros ir bendruomenių vertinimams, padedantiems organizacijoms priimti sprendimus, teikti ir dalytis informacija tiek viešajam, tiek privačiam sektoriui (viešoji ir privati partnerystė laikoma gyvybiškai svarbia plėtrai). Kitas pagrindinių paslaugų dėmesys skiriamas mokymams ir pratyboms bendradarbiaujant valstybės, vietos ir valstijų lygmeniu ir organizuojant mokymus kritiniais infrastruktūros saugumo klausimais (CISA, 2018).

Hatcher ir kt. (2020) atlikta apklausa 168 valstybės tarnautojų, dirbančių skirtinguose JAV miestuose, grupė nustatė, kad dauguma miestų yra parengę dokumentą, kuriame išdėstyta saugumo politika, bet neregistruoja kibernetinių atakų. Miestų, išorės auditorių ir IT saugumo politikos specialistų bendradarbiavimo lygis taip pat toli gražu nėra patenkinamas. Viena iš galimų priežasčių yra nepakankamas finansavimas net tokiame dideliame mieste kaip Atlanta. Finansinės kliūtys taip pat trukdo vykdyti tinkamus kibernetinio saugumo mokymus. Minėtų tyrėjų išvados ir rekomendacijos

(kuriomis remiamės diskusijoje) patvirtina (Norris ir kt., 2019) pastebėjimus, nors atrodo, kad bendras JAV savivaldybių pasirengimo kovoti su kibernetinėmis priemonėmis vertinimas, atakos, išplaukiančios iš pirmosios šalies masto JAV savivaldybių kibernetinio saugumo būklės tyrimo, yra mažiau optimistiški.

2017 m. Lenkija priėmė savo kibernetinio saugumo strategiją 2017–2022 m. Joje kibernetinis saugumas apibrėžiamas kaip: „informacijos ir ryšių sistemų atsparumas tam tikru pasitikėjimo lygiu bet kokiai veiklai, kuri kelia pavojų saugomų, perduodamų ar tvarkomų duomenų prieinamumui, autentiškumui, vientisumui ar konfidencialumui, arba su šiais informaciniais tinklais ir sistemomis siūlomas arba per jas pasiekiamas susijusias paslaugas“ (Lenkijos Skaitmeninių reikalų ministerija 2017). 2018 m. Lenkija priėmė Nacionalinės kibernetinio saugumo sistemos įstatymą. Svarbūs įstatymo elementai buvo Vyriausybės įgaliotinio ir Valdybos veiklai koordinuoti ir įgyvendinti valstybės politiką kibernetinio saugumo srityje; atsakomybės paskirstymas tarp atskirų CSIR nacionaliniu lygiu ir kibernetinio saugumo srities priežiūros nustatymas skiriant kompetentingas institucijas ir įvedant finansines nuobaudas (Jacuch, 2021).

2019 m., laikydamasi ENISA reikalavimų, Lenkija priėmė patobulintą NCSS 2019–2024 m. kibernetinio saugumo strategiją, kurios tikslas padidinti atsparumo kibernetinėms grėsmėms lygį ir padidinti informacijos apsaugos lygį viešajame, kariniame ir privačiame sektoriuje ir skatinti žinias bei gerąją patirtį, leidžiančią piliečiams geriau apsaugoti savo informaciją (Skaitmeninių reikalų ministerija 2019 m.). Taip pat siekiama sukurti naujas arba esamas normas ir standartus paversti konkrečiomis rekomendacijomis kibernetinio saugumo srityje.

Lenkijos Respublikos kibernetinio saugumo strategija yra Ministrų Tarybos nutarimu priimtas dokumentas, nustatantis strateginius tikslus ir atitinkamas politines bei reguliavimo priemones, skirtas aukštam kibernetinio saugumo lygiui pasiekti ir palaikyti. Jis rengiamas penkerių metų laikotarpiui su galimais pakeitimais per visą jos galiojimo laiką (NSAĮ 68 straipsnis ir 69 straipsnio 1 dalis). Strategijos projektą rengia už kompiuterizavimą atsakingas ministras, bendradarbiaudamas su kitais ministrais, atsakingais centrinių įstaigų vadovais. Strategijos projekto rengimo darbe gali dalyvauti ir Lenkijos Respublikos Prezidento atstovas.

Strategijoje visų pirma nurodoma:

1) su kibernetiniu saugumu susiję tikslai ir prioritetai;

2) subjektai, dalyvaujantys įgyvendinant strategiją;

3) priemonės, nukreiptos į Strategijoje užsibrėžtų tikslų įgyvendinimą;

4) parengties, reagavimo ir atkūrimo priemonės, įskaitant viešojo ir privačiojo sektorių bendradarbiavimo principus;

5) rizikos vertinimo metodas;

6) veikla, susijusi su švietimo, informacinėmis ir mokymo programomis kibernetinio saugumo srityje;

7) veikla, susijusi su mokslinių tyrimų ir plėtros planais kibernetinio saugumo srityje.

Lenkijoje nacionalinio saugumo sistema suprantama kaip resursų, priemonių ir jėgų (subjektų), valstybės skiriamų saugumo srities užduotims vykdyti, visuma, organizuota (į posistemes ir komponentus), prižiūrima ir parengta taip, kad galėtų vykdant tokių užduočių atlikimo tikslą. Nacionalinio saugumo strategijos tikslas – atremti kylančias grėsmes tiek tautos, tiek valstybės išlikimui, teritoriniam vientisumui, politinei nepriklausomybei ir suverenitetui, efektyviam valstybės institucijų funkcionavimui, socialiniam ir ekonominiam vystymuisi. Ji apima tiek išorinio, tiek vidinio saugumo elementus, orientuotus į nacionalinio saugumo užtikrinimą kartu su socialine ir ekonomine šalies raida.

Nacionalinio saugumo sistemą sudaro visi įstatymų leidžiamąją, vykdomąją ir teisminę valdžią sudarantys organai ir institucijos, atsakingos už saugumo užtikrinimą pagal Lenkijos Respublikos Konstituciją ir kitus atitinkamus teisės aktus. Tai parlamentas, Lenkijos Respublikos Prezidentas, Ministrų Tarybos pirmininkas, Ministrų Taryba, centrinės valdžios administravimo institucijos ir kitos centrinės valstybės įstaigos bei viešosios institucijos. Ginkluotosios pajėgos, taip pat vyriausybės tarnybos ir institucijos taip pat sudaro esminius nacionalinio saugumo sistemos elementus. Jie yra įpareigoti užkirsti kelią išorinėms grėsmėms ir jas atremti, užtikrinti visuomenės saugumą, vykdyti gelbėjimo darbus, saugoti žmones ir turtą ypatingose situacijose. Be to, sistema apima vietos valdžios institucijas ir kitus juridinius asmenis, įskaitant verslininkus, formuojančius pramoninės gynybos potencialą ir vykdančius pareigas krašto apsaugos srityje.

Nacionalinio saugumo sistemą sudaro nacionalinio saugumo kontrolės posistemis ir keli vykdomieji posistemiai. Kontrolės posistemį sudaro valstybės institucijos ir su nacionaliniu saugumu susijusias pareigas vykdančių organizacinių padalinių vadovai bei Lenkijos Respublikos ginkluotųjų pajėgų valdymo institucijos. Vykdomieji posistemiai yra priemonės ir pajėgos, skirtos ministrams, vadovaujantiems vyriausybės administracijos departamentams, centrinės vyriausybės administracijos institucijoms, provincijų valdytojams (vaivadoms), vietos valdžios institucijoms ir kitoms viešosioms institucijoms bei subjektams, atsakingiems už kylančių pareigų nacionalinio saugumo srityje įgyvendinimą.

Estijos Kibernetinio saugumo strategijoje išdėstyti trys pagrindiniai tikslai. Pirmasis tikslas – užtikrinti, kad Estija būtų tvari skaitmeninė visuomenė, pasižyminti stipriu technologiniu atsparumu ir pasirengusia įveikti krizes. Tai, be kita ko, apima laikymąsi informacijos saugumo ir duomenų apsaugos principų, platų Estijos ISKE bazinių saugumo reikalavimų įgyvendinimą ir sistemingą rizikos, susijusios su naujos kartos technologijomis, įvertinimą ir administravimą tokiose srityse kaip kriptografija, blokų grandinės technologija, dirbtinis intelektas (AI) ir saugus tapatybės valdymas. Šio tikslo veiklos rodiklis

yra bendro visiems interneto vartotojams prieinamų atvirų paslaugų skaičiaus valstybiniame tinkle ir Estijos kibernetinėje erdvėje sumažinimas iki maždaug trečdalio pradinio lygio.

Antrasis tikslas – pasauliniu mastu konkurencinga, tyrimais pagrįsta kibernetinio saugumo pramonė – matuojamas pagal sektoriaus eksporto apimtis. Juo siekiama apytikriai padvigubinti toje srityje pradedančių įmonių skaičių ir padidinti suteikiamų doktorantų skaičių. Estijos informacijos saugumo asociacija (EISA) yra kibernetinio saugumo klasteris, remiantis universitetų, įmonių ir vyriausybės bendradarbiavimą. Juo siekiama sukurti administracinės paramos mechanizmą vieningam tarpsektoriniam dalyvavimui konkursuose. Estijos IRT plėtros programa ir IT akademijos programa yra dabartinės priemonės, susijusios su mokslinių tyrimų ir plėtros skatinimu. Tačiau jie nėra visiškai orientuoti į kibernetinį saugumą, o rengiamas visos šalies kibernetinio saugumo MTEP planas, apibrėžiantis prioritetines fokusavimo sritis. Galiausiai „Startup Estonia“ ir Gynybos ministerija bendradarbiauja. Estija taip pat plėtoja Open Cyber Range platformą, siūlančią sprendimus sektorinėms (start-up) įmonėms ir universitetams MTEP veiklai vykdyti, testavimui, mokymams.

Trečiasis tikslas – kad Estija būtų patikima ir stipri partnerė tarptautinėje arenoje – sunkiausia kiekybiškai įvertinti. Jis vertinamas remiantis kasmetiniu ekspertų vertinimu. Šioje srityje siekiama, kad Estija būtų pakankamai atstovaujama ir turi kompetenciją kibernetinių temų klausimais savo atstovybėse ES, JT ir NATO. Ji prisideda prie tarptautinės teisės formavimo procesų, plėtoja dvišalio bendradarbiavimo formatus su pagrindiniais partneriais, reguliariai rengia bendras pratybas. Be to, ji aktyviai stengiasi stiprinti ES ir NATO atgrasymo pozicijas. Tai taip pat sustiprina aktyvų Estijos vaidmenį didelio masto pratybose, tokiose kaip „Locked Shields“ ir „Cyber Coalition“. Galiausiai Estija siekia dalyvauti kuriant ES kibernetinės pagalbos tinklą ir plėtoti konkurencingą ir tvarų kibernetinės pagalbos teikimo pajėgumą.

Paskutinis tikslas – kad Estija būtų kiberraštinga visuomenė, kuri ateityje garantuotų specialistų pasiūlą. Šio tikslo veiklos rodikliai apima 16–74 metų amžiaus interneto vartotojų, kurie per vienerius metus patyrė vieną nuostolį dėl saugumo spragų internete, dalį. Estija siekia sumažinti šį rodiklį nuo 27,7 proc. 2015 m. iki mažiau nei 20 proc. 2020 m. Ji taip pat siekia padidinti įmonių, taikančių IRT saugumo politiką, dalį nuo 16,9 iki daugiau nei 25 proc., taip pat vyriausybės darbuotojų dalį, kurie patenkinamai atlieka naujai reikalaujamą praktinių įgūdžių patikrinimą iki daugiau nei 75 proc.

Užsienio politikos plėtros planas 2030 yra pirmoji ilgalaikė Estijos užsienio politikos strategija su numatomais vidurio laikotarpio ir ex-post vertinimais. Strategijoje pažymima, kad mažos šalies saugumas, įtaka ir dalyvavimas tarptautiniuose reikaluose labiau priklauso nuo jos reputacijos, palyginti su didelėmis šalimis. Taigi Estijos stipriosios pusės ir reputacija, skaitmeninės tapatybės, e. paslaugų ir kibernetinio saugumo srityse yra jos įtaka (Užsienio reikalų ministerija, 2019, p. 12). Estija siekia būti tarptautinio kibernetinio saugumo advokate. Ji plėtoja ir stiprina kibernetinį saugumą ES, NATO, JT, Europos saugumo ir bendradarbiavimo organizacijoje (ESBO), kitose tarptautinėse organizacijose. Tai

apima Europos išorės veiksmų tarnybos gebėjimų kovojant su kibernetinėmis grėsmėmis stiprinimą, taip pat bendradarbiavimą su panašiai mąstančiomis šalimis visame pasaulyje, skatinant atsakingą elgesį kibernetinėje erdvėje. Estija toliau planuoja plėtoti visapusį ir nuodugnų bendradarbiavimą su Jungtinėmis Valstijomis, kaip prioritetą, įskaitant bendradarbiavimą kibernetinio saugumo srityje. Šiaurės ir Baltijos šalių regione kviečia prisijungti prie X-kelio saugaus keitimosi duomenimis sluoksnio (Užsienio reikalų ministerija, 2019, p. 16).

Apibendrinant galima teigti, kad analizuotose užsienio šalyse kibernetinio saugumo strategijose identifikuojami pagrindiniai tikslai bei įgyvendinimo priemonės. Lietuva analizuotų šalių kontekste užima aukštą vietą vertinant pagal kibernetinio saugumo indeksavimo sistemą. Tačiau norėtųsi atkreipti dėmesį į Estijoje taikomą kibernetinio saugumo strategiją, kurioje daug dėmesio skiriama tarptautiniam bendradarbiavimui, tarpinstituciniam nacionalinių įstaigų bei struktūrų darbui, visuomenės švietimo iniciatyvoms. Taip pat atliekamas periodinis strategijos vertinimas ir papildymas, atsižvelgiant į šalyje ir pasaulyje vykstančias tendencijas.

2. KIBERNETINIŲ ATAKŲ VIEŠOJO VALDYMO ĮSTAIGŲ INFORMACINĖSE SISTEMOSE METODOLOGIJA

Tyrimo tikslas – nustatyti savivaldybės atstovų požiūrį į kibernetinio saugumo valdymo situaciją viešojo valdymo įstaigų informacinėse sistemose.

Tyrimo uždaviniai:

1. Įvertinti kibernetinio saugumo problemas ir grėsmes savivaldybėje.
2. Ištirti kokias kibernetinio saugumo užtikrinimo priemones taiko savivaldybės.
3. Įvertinti kokias kibernetinio saugumo gerinimo priemones respondentai rekomenduoja taikyti savivaldybėse.
4. Pateikti kibernetinio saugumo užtikrinimo modelį.

Tyrimo metodas. Siekiant atskleisti tyrimo dalyvių apibrėžiamą požiūrį į tiriamą fenomeną, remiantis informantų patirtimi ir suvokimu pasak Žydžiūnaitės (2017) tinkamiausias yra kokybinis tyrimas. Kardelis (2007) kokybinį tyrimą apibūdina kaip „sistemingą, nestruktūrizuotą atvejo, situacijos tyrimą natūralioje aplinkoje, siekiant suprasti tiriamuosius reiškinius bei pateikti interpretacinį, holistinį jų paaiškinimą“. Tokiu būdu, pasitelkus kokybinį tyrimą, atrandamas reikšmių ir patirčių turinys: kaip vyko koks nors procesas, kokia jo reikšmė (prasmė) tyrimo dalyviams, kokie galimi šios patirties skirtumai ir savitumai (Gaižauskaitė, Valavičienė 2016). Taigi šiame baigiamajame darbe kokybinio tyrimo prieigos pasirinkimą sąlygojo šios prielaidos: kadangi tyrimas atliekamas viešojo valdymo institucijose - savivaldybėse, todėl pasirenkami tyrimo dalyviai yra asmenys atsakingi už kibernetinio saugumo sistemos priežiūrą bei valdymą.

Taikytas tyrimo metodas – interviu raštu. Remiantis Prakapu, Butvilu (2011) interviu apibrėžiamas kaip nuoširdus, atviras pokalbis nagrinėjama tema. Pagrindinis elementas yra klausimas. Jis gali būti atviras (dažniausiai) arba struktūruotas. Kaip nurodo Gaižauskaitė, Valavičienė (2016) interviu yra bendravimo tarp tyrėjo ir tyrimo dalyvio forma, o pokalbis vyksta užduodant klausimus ir į juos atsakant.

Ekspertų atranka: tyrimui atlikti naudota neatsitiktinė respondentų atranka, taikant patogumo metodą. Vykdant neatsitiktinę, t.y. tikslinę, atranką buvo apklausiami tie respondentai, kurie galėjo suteikti prasmingos informacijos apie tiriamąjį dalyką. Patogumo metodas leido parinkti respondentus, kuriuos galima rasti savivaldybių viešai skelbiamuose kontaktuose. Neatsitiktinės atrankos privalumai – sugaištama mažiau laiko, profesionaliai atrinkus visumos elementus galima gauti pakankamai reprezentatyvią imtį. Trūkumai – negalima apskaičiuoti atrankos paklaidos, ne visada aišku, kaip atrinkta imtis atspindi tiriamąją visumą (Kardelis, 2016, p. 115). Tyrime dalyvavusių savivaldybių ekspertų duomenys pateikiami 1 lentelėje.

1 lentelė. Tyrimo dalyvių charakteristika

Ekspertas	Užimamos pareigos	Darbo stažas savivaldybėje
E1	Informacinių sistemų specialistas	9 m.
E2	Vyresnioji specialistė informatikai	12 m.
E3	Vyriausiasis specialistas informatika	5 m.
E4	Veiklos duomenų apdorojimo inžinierius	15 m.
E5	Tarybos narė	9 m.
E6	Skyriaus vadovas	20 m.

Tyrimo instrumentarijaus sudarymas: ekspertinio tyrimo interviu klausimai apima analizuotus kibernetinio saugumo problematikos, kibernetinio saugumo užtikrinimo priemones bei tobulinimo sprendimus. Interviu klausimų teorinis pagrindimas pateikiamas 2 lentelėje.

2 lentelė. Tyrimo instrumento teorinis pagrindimas

Klausimų grupės	Tikslas	Autoriai
1. Apibūdinkite su kokiomis kibernetinio saugumo grėsmėmis jums teko susidurti per pastaruosius dvejus metus savivaldybėje. 2. Kokį poveikį kibernetinės atakos turi/turėjo jūsų savivaldybei. Pateikite kibernetinių atakų pavyzdžių bei apibūdinkite sukeliamą riziką.	Nustatyti su kokiomis kibernetinio saugumo grėsmėmis dažniausiai susiduria savivaldybės, kokios kibernetinės atakos įvyko per pastaruosius metus.	Jacuch, 2021 Li, Liu, 2021 Nikolova, 2017 Wirtz, 2017
3. Kokios kibernetinio saugumo priemonės yra taikomos Jūsų savivaldybėje? Kaip vertinate taikomų priemonių efektyvumą užtikrinant kibernetinį saugumą? 4. Kokias priemones jūs asmeniškai taikote savo darbe siekdamas užtikrinti kibernetinį saugumą? 5. Papasakokite kaip elgiatės ar kokių veiksmų imatės jeigu pastebite kibernetinių atakų riziką?	Įvertinsime kokias priemones savivaldybės taiko kibernetiniam saugumui užtikrinti, kaip yra vertinamas priemonių efektyvumas, taip pat kokių veiksmų savivaldybės imasi pastebėjus kibernetinių atakų riziką.	Al-Ghamdi, 2021 Cavelty, 2018 Enescu, 2020 Karpiuk, 2021 Norris, Mateczun, 2022
6. Kaip vertinate kibernetinio saugumo politiką bei teisinį	Nustatysime ekspertų nuomonę apie kibernetinio saugumo	Attatfa, 2020 Backhaus, 2020

reguliavimą Lietuvoje ir Jūsų savivaldybėje? Kokios teisinės priemonės yra taikomos savivaldybėje? Kokius dokumentus, procedūras ar strategijas esate parengę?	politiką Lietuvoje bei savivaldybėje, teisines priemones.	Chodakowska, 2022
7. Kokie darbuotojų mokymai yra organizuojami savivaldybėje, siekiant užtikrinti kibernetinį saugumą? Kaip dalijamasi patirtimi susijusia su kibernetinio saugumo užtikrinimu? 8. Kokius sprendimus reiktų priimti ir kokias priemones taikyti, siekiant efektyvinti kibernetinių atakų bei grėsmių valdymą savivaldybėje? Lietuvos mastu? 9. Kokius kibernetinio saugumo užtikrinimo bei gerinimo pasiūlymus galite pateikti savivaldybėje?	Įvertinsime kokie mokymo būdai taikomi savivaldybėse, kokius kibernetinio saugumo sprendimus priima savivaldybės bei kokiomis priemonėmis reikia gerinti kibernetinio saugumo užtikrinimą.	Bullock, Haddow, 2021 Nikolova, 2018 Norris, 2022

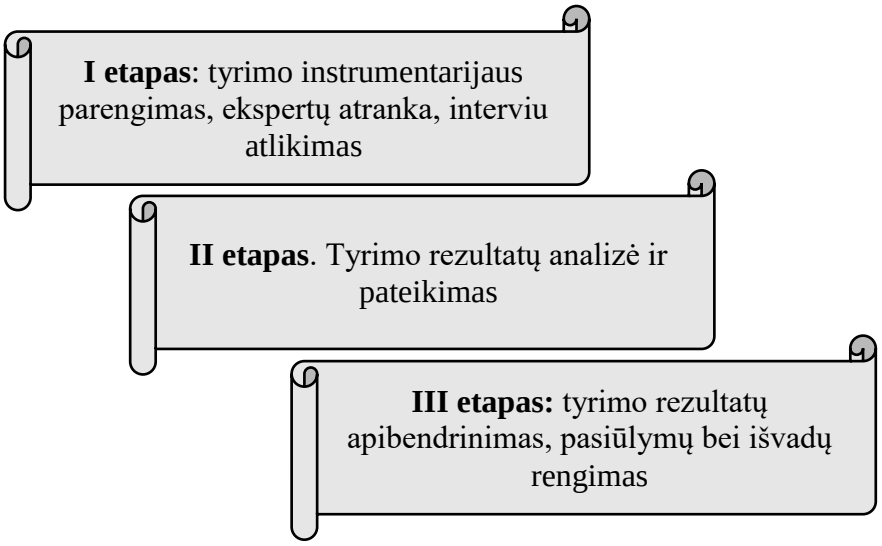
Remiantis lentelėje pateikta informacija matome, kad tyrimo metu ekspertai įvertino kibernetinio saugumo situaciją šiose srityse:

- Kibernetinio saugumo grėsmės, kibernetinių atakų poveikis savivaldybės veiklos organizavimui;
- Kibernetinio saugumo priemonės ir jų taikymas;
- Veiksmai pastebėjus kibernetinių atakų grėsmę;
- Kibernetinio saugumo teisinio reguliavimo, savivaldybės strateginių dokumentų vertinimas
- Kibernetinio saugumo užtikrinimo tobulinimo pasiūlymai.

Tyrimo duomenų analizė. Analizuojant duomenis buvo remiamasi autentiškomis citatomis. Taip pat analizuojant duomenis įterpti darbo autoriaus pasisakymai ir interpretacijos, remiantis tyrimo dalyvių pasisakymais. Tyrimui išanalizuoti pasirinkta kokybinės turinio analizės strategija (angl. Qualitative content analysis). „Kokybinė turinio analizė yra metodas, kuriuo gilinamasi į objektą ir kontekstą, domintis panašumais bei skirtumais tarp kategorijų ar kodų“ (Gaižauskaitė ir Valavičienė, 2016, p. 144). Interviu duomenys analizuojami pateikiant kategorijas, šios dar suskaidomos į subkategorijas; išskiriami semantiniai teksto vienetai. Turinio analizėje didesnis dėmesys buvo skiriamas subkategorijos išskyrimui bei informantų pagrindžiančių teiginių pateikimui.

Tyrimo atlikimo laikas: tyrimas buvo atliktas 2023 m. kovo – balandžio mėnesiais.

Tyrimo eiga ir etapai. Baigiamajame darbe tyrimas atliekamas laikantis tam tikrų etapų eiliškumo. Tyrimo loginė schema pateikiama 5 paveiksle.



5 pav. Tyrimo etapų loginė seka

Tyrimo etika. Vykdant tyrimą, laikytasi pagrindinių etikos principų: savanoriškumo ir geranoriškumo (Kardelis, 2007, Bitinas, Rupšienė, Žydžiūnaitė, 2008). Žydžiūnaitė, Sabaliauskas (2017) išskiria šiuos mokslinio tyrimo etikos principus: pagarbos asmens privatumui principas; konfidencialumo ir anonimiškumo principas; geranoriškumo ir nusiteikimo nekenkti tiriamam asmeniui principas ir teisingumo principas.

Respondentams buvo atskleista tyrimo esmė, tikslai ir uždaviniai, paaiškinti etiniai principai, asmens duomenų apsauga, konfidencialumo užtikrinimas, taip pat nurodoma, jog asmeniniai duomenys nebus skelbiami.

Pagrindiniai nurodytų etikos principų elementai:

- Tyrime ekspertai dalyvavo tik laisvai apsisprendę – niekas negalėjo daryti jokio spaudimo.
- Ekspertams buvo pateikiama išsami ir tiksli informacija apie tyrimo tikslus, savanoriškumą.
- Atliktas tyrimo metu surinktų duomenų nuasmeninimas ir kodavimas.
- Respondentams bus suteikiama galimybė susipažinti su tyrimo duomenų rezultatais.

Tyrimo ribotumai: menkas savivaldybių suinteresuotumas dalyvauti apklausoje, ekspertinio vertinimo atranka užtruko labai ilgai, buvo susiduriama su priešiškomis tiriamųjų nuostatomis. Taip pat pateikiant interviu metu surinktą informaciją neišvengiama tiriamųjų subjektyvumo.

3. KIBERNETINIŲ ATAKŲ VIEŠOJO VALDYMO ĮSTAIGŲ INFORMACINĖSE SISTEMOSE TYRIMO REZULTATAI

3.1.Kibernetinio saugumo statistika Lietuvoje

2021 m. birželio 29 d. ITU paskelbė tarptautinio kibernetinio saugumo indekso (toliau – KSI) rezultatus, pagal kuriuos Lietuva, surinkusi 97,3 balo, tarp pasaulio valstybių užėmė šeštą, o Europos valstybių sąraše – ketvirtą vietą. Aukščiausių įvertinimų Lietuva sulaukė teisinio reglamentavimo ir kibernetinio saugumo pajėgumų plėtojimo srityse. Ir toliau bus siekiama išlaikyti aukštą KSI, didinant kibernetinio saugumo technologinių ir organizacinių priemonių efektyvumą.

CERT-LT 2021 m. iš viso fiksavo 4 088 kibernetinius incidentus ir tai yra 5 proc. mažiau negu 2020 m., kai buvo fiksuota 4 330 kibernetinių incidentų. Pažymėtina, kad 93 iš 4 088 fiksuotų kibernetinių incidentų 2021 m. buvo vidutinės reikšmės ir tai yra beveik trečdaliu daugiau negu 2020 m., kai buvo fiksuoti 67 tokio poveikio incidentai. Ryškesni vidutinės kategorijos incidentai buvo Vilniaus kolegijos studentų duomenų bazės nutekėjimas, įsilaužimas ir melagienų platinimas Prienų savivaldybės interneto svetainėje.

Iš visų pagal subjektų veiklos sritis vertintų 2021 m. incidentų daugiau nei pusė (53 proc.) CERT-LT fiksuotų kibernetinių incidentų buvo susiję su Lietuvos interneto prieglobos teikėjų infrastruktūra, kurią, pvz., galima naudoti svetainėms, virtualioms darbo vietoms kurti, el. pašto paslaugoms ir pan. Toks didelis incidentų skaičius siejamas su aktyvia internetinių sukčių veikla, pvz., turėdami galimybę už prieglobos paslaugas anonimiškai atsiskaityti kriptovaliutomis, šias paslaugas sukčiai išnaudojo kibernetinėms atakoms Lietuvoje ir kitose šalyse vykdyti. Vertinant visus interneto prieglobos tiekėjus matyti, kad daugiausia kenkimo veiklos 2021 m. buvo fiksuota UAB „Interneto vizija" (15 proc.) , UAB „Host Baltic" (10 proc.), „Hostinger International Limited" (7 proc.).

2022 m. pirmą ketvirtį kibernetinių incidentų intensyvumas išliko aukštas. Per pirmus tris 2022 m. mėnesius NKSC fiksavo 1 020 kibernetinių incidentų. Jų skaičius kiek didesnis nei prieš metus per tą patį laikotarpį, kai fiksuotas 981 incidentas. Taip pat pastebėta, jog trečdaliu daugiau incidentų buvo fiksuota aštuntą 2022 m. savaitę, kai prasidėjo karas Ukrainoje. Šis momentinis šuolis siejamas su padidėjusiu įstaigų ir asmenų dėmesiu kibernetiniam saugumui.

2021 m., kaip ir ankstesniais metais, daugiausia kibernetinių incidentų buvo susiję su kenkimo programinės įrangos (toliau – PĮ) platinimu. Šio tipo kibernetiniai incidentai, kartu su informacijos rinkimo atakomis (angl. *phishing*), išlieka pagrindinė kibernetinių incidentų grėsmė Lietuvoje. 2021 m. augo tiek mėginimų įsilaužti į ryšių ir informacines sistemas (fiksuoti 278 incidentai), tiek ir sėkmingų

įsilaužimų (fiksuoti 125 incidentai) skaičiaus. Viena iš pagrindinių priežasčių, kodėl 2021 m. daugėjo pranešimų apie sėkmingus įsilaužimus, – tai „Microsoft Exchange“ elektroninio pašto paslaugos „nulinės dienos“ (angl. *zero-day*) spraga, kuri kai kurių naudotojų laiku nebuvo pašalinta.

Ypatingos svarbos informacinė infrastruktūra, valstybės informacinių išteklių elektroninė informacija ir jų pagrindu veikiančios sistemos ir paslaugos yra gyvybiškai svarbios Lietuvos Respublikai. Dėl didėjančio paslaugų ir procesų skaitmenizavimo, COVID-19 pandemijos, geopolitinių iššūkių ir įtampų auga kibernetinių ir hibridinių atakų grėsmė, didėja jų socialinis ir ekonominis poveikis. Nacionalinio kibernetinio saugumo centro duomenimis1, per 3 pastaruosius metus užregistruota 11 659 kibernetinių incidentų: 2019 m. – 3 241, 2020 m. – 4 330, 2021 m. – 4 088. Dėl didelio kibernetinių incidentų skaičiaus, jų modernėjimo, galimos rizikos patirti reikšmingus kibernetinių atakų ir incidentų padarinius, vis svarbiau užtikrinti kibernetinį saugumą nacionaliniu lygmeniu.

Kibernetinio saugumo užtikrinimas grindžiamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos ypatingos svarbos informacinės infrastruktūros, ryšių ir informacinių sistemų saugumui, rizikos vertinimu. Rizikos valdymas sudaro pagrindą veiksmingos saugumo reikalavimų valdymo sistemos sukūrimui, diegimui, palaikymui ir tobulinimui. Saugumo valdymo sistema apima institucijų, organizacijų tinklų ir informacinių sistemų saugumo reikalavimų (priemonių, taisyklių ir procedūrų) nustatymą ir vykdymą, stebėseną ir peržiūrą (atitikties vertinimą), kibernetinių incidentų prevenciją, aptikimą, reagavimą į juos, atsigavimą, atsako į kibernetinius incidentus galimybių, jų išvengimo priemonių vertinimą, saugumo technologijų valdymą, darbuotojų mokymą, informuotumo programas.

Valstybės kontrolės audito ataskaitoje (2022) nurodoma kad 2019–2021 m. beveik pusė (45 proc., 80 iš 176) valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų nė karto neatliko informacinių technologijų saugos atitikties vertinimo ir taip neįsitikino savo informacijos saugumo valdymo sistemos būkle, kad, prireikus, laiku galėtų imtis veiksmų ją tobulinti. Kasmet informacinių technologijų saugos atitikties vertinimų skaičius auga, tačiau 2021 m. nepateikta net 81 proc. valstybės informacinių išteklių informacinių technologijų saugos atitikties vertinimo ataskaitų. Didelė dalis (41 proc., 39 iš 96) informacinių technologijų saugos atitikties vertinimus atlikusių valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų duomenų Valstybės informacinių išteklių atitikties informacijos saugos reikalavimams stebėsenos sistemai neteikė. Tai mažina galimybes centralizuotai valdyti informaciją apie informacinių technologijų saugos neatitiktis ir nacionaliniu lygiu užtikrinti reikalavimų laikymosi priežiūrą. Valstybės kontrolė 2018 m. nustatė trūkumų5, nors rekomendacijos priemonė turėjo būti įgyvendinta iki 2019-06-01, tačiau problemos iki šios dienos nėra išspręstos, nes pagal esamą programinį kodą nėra galimybės atlikti Valstybės informacinių išteklių atitikties informacijos saugos reikalavimams stebėsenos sistemos funkcinio praplėtimo, todėl ilgus metus problemos, kurių nepavyksta išspręsti, neigiamai veikia šį tvarumą, sudaro sąlygas pažeidžiamumams atsirasti.

3.2.Savivaldybių atstovų interviu rezultatai

Šiame darbo skyriuje analizuojami savivaldybių atstovų – ekspertų interviu rezultatai, išskiriamos kategorijos bei subkategorijos, pateikiami patvirtinantys teiginiai bei apibendrinta interviu rezultatų interpretacija. Pirmu interviu klausimų ekspertų buvo prašoma apibūdinti su kokiomis kibernetinėmis atakomis bei saugumo grėsmėmis teko susidurti per pastaruosius dvejus metus (žr. 3 lentelę).

3 lentelė. Ekspertų nuomonė apie kibernetinio saugumo grėsmes

KATEGORIJA	SUBKATEGORIJOS	PATVIRTINANTYS TEIGINIAI
Kibernetinio saugumo grėsmės	Kenkėjiški laiškai	„dažniausiai gauname kenkėjiškus laiškus, su įvairiomis klaidinančiomis nuorodomis bei informacija“ (E2) „laiškai su užkrėstomis bylomis, suzipuoti failai ar kitaip pateikiama informacija“ (E4) „ypač pagausėjo visokių kenkėjiškų laiškų, su įvairiomis melagingomis nuorodomis, klaidinga informacija“ (E6)
	Virusinės atakos	„phishing“ atakos, siunčiama informacija su fiktyviomis nuorodomis, bandoma išvilioti jautrius duomenis“ (E1) „bandoma įsilaužti į vidinį tinklą, DDoS atakos“ (E3) „per pandemiją yra buvusi situacija kai per nuotolinio darbo stotį pasigautas virusas“ (E5)
	Dezinformacija, melagingos naujienos	„įvairių klaidingų naujienų, dezinformacijos sklaida“ (E3) „melagingi prašymai ar kreipimasis pervesti lėšas, suteikti paramą“ (E4)

Remiantis pateikta informacija galima teigti, kad kibernetinio saugumo grėsmių kategorijoje yra išskiriamos trys subkategorijos: kenkėjiški laiškai, virusinės atakos, dezinformacija bei melagingos naujienos. Ekspertų nuomone dažniausiai savivaldybėse tenka susidurti su įvairiais kenkėjiškais laiškais, kurie siunčiami su užkrėstais prisegtukais, klaidinančiomis nuorodomis, melagienomis, pinigų pervedimo užklausomis. Taip pat ekspertai atkreipia dėmesį, kad pandemijos laikotarpiu buvo ir tokių kibernetinių atakų incidentų, kai virusą pasigaudavo nuotolinio darbo stotis per užkrėstą asmeninę kompaktinę plokštelę, nustatyti ir tokie atvejai, kai bandoma įsilaužti į vidinį tinklą arba atakuojama interneto svetainė (DDoS). Interviu rezultatų analizė atskleidė, kad savivaldybėse neišvengiamai yra

susiduriama su kenkėjiškais laiškais, visuomenėje pastebima, kad ne tik savivaldybėse, bet ir verslo įmonėse dažniau pastebimas įvairių laiškų siuntimo pagausėjimas, kuriuose skleidžiami įvairūs virusai, bandymu įsilaužti į interneto svetaines, išvilioti jautrius ar net konfidencialius duomenis. Apibendrinant galima teigti, kad savivaldybės dažniausiai susiduria su įvairių virusų sklaida bei nepageidaujamais laiškais, melagienomis, siekimu įsibrauti į savivaldybės sistemas. Kitu interviu klausimu ekspertų buvo prašoma nurodyti kokį poveikį kibernetinės atakos turi savivaldybei bei kokią riziką sukelia (žr. 4 lentelę).

4 lentelė. Ekspertų nuomonė apie kibernetinių atakų riziką

KATEGORIJA	SUBKATEGORIJOS	PATVIRTINANTYS TEIGINIAI
Kibernetinių atakų rizika	Darbuotojų sąmoningumo trūkumas	„visgi pasigendama mūsų darbuotojų sąmoningumo, vis kas nors paspaudžia atsiųstas nuorodas“ (E1) „bet kokią ataką pastebėjus būtina laiku informuoti atitinkamus skyrius bei atsakingus asmenis“ (E2) „svarbiausia visiems išlikti budriems ir sąmoningiems, gebėti atskirti kas tikra, o kuri informacija yra klaidinanti“ (E5)
	Techninės problemos	„ne visa turima programinė įranga pastebi kibernetinio įsilaužimo žymes“ (E2) „mes pakankamai daug dėmesio skiriame tinkamai antivirusinei įrangai įsigyti, nuolat ją atnaujiname“ (E5) „įvedama grupinė politika, uždrausti USB raktai, todėl sumažėjo ir grėsmių tikimybė“ (E6)
	Kibernetinio saugumo įrangos kaina	“kai kuri įranga yra labai brangi ir ne visoms savivaldybėms prieinama” (E3) “gerai kad rimtų grėsmių ir kibernetinių atakų pasitaiko retai, todėl nereikia pirkti itin brangios įrangos” (E5)

Įvertinus ekspertų nuomonę apie kibernetinių atakų keliamą riziką ir grėsmę nustatyta, kad kibernetinės atakos grėsmės yra susijusios su savivaldybės darbuotojų sąmoningumu, techninėmis priemonėmis bei tinkama programine įranga. Ekspertų nuomone didelė problema yra darbuotojų sąmoningumas, nes nors ir darbuotojai yra informuojami apie kenkėjiškus laiškus, virusų sklaidą, tačiau pasitaiko atvejų kai nurodymų yra nesilaikoma ir atidaroma kenkėjiška nuoroda. Savivaldybėse yra taikomos įvairios techninės priemonės, kurios automatiškai pastebi ir fiksuoja kenkėjiškus laiškus, tačiau

būna ir tokių atvejų, kai laiškai nėra atpažįstami ir pasiekia adresatus. Ekspertai atkreipia dėmesį, kad kibernetinės grėsmės dažnai kildavo kai buvo naudojamos USB atmintinės, nes neįmanoma sukontroliuoti kokias atmintines darbuotojai naudoja. Tačiau ši problema buvo išspręsta per grupinę politiką (angl. *group policy*) uždraudus visuose įrenginiuose USB lizdus. Kiti ekspertai pritaria, kad dažniausiai bandoma siuntinėti įvairius laiškus savivaldybės darbuotojams, kadangi adresai yra viešai prieinami. Tačiau pašto serveriai yra apsaugoti nuo užkrėstų bylų gavimo, pagrindinė problema yra laiškai su apgaulingomis nuorodomis, todėl čia galioja tik darbuotojų pastabumas. Yra buvęs atvejis, kai darbuotojas, norėdamas atsiimti kažkokį prizą, sumąstė prisiregistruoti atsiųstoje svetainėje su tarnybiniu paštu, tarnybinį kompiuterį teko perinstaliuoti, kadangi jis buvo užtvindytas šlamšto (angl. *spam*) laiškais. Daugiau problemų ir grėsmių sukelia DDoS ataka, tai irgi opi problema, kadangi apsaugos įranga yra per brangi įsigyti, tačiau tokios atakos yra gan retas reiškinys ir trunka ne ilgai. Vienintelė apsauga nuo tokių atvejų, nuolatinis tinklo monitoringas ir informavimas valstybinių institucijų, tokių kaip nacionalinis kibernetinio saugumo centras. Ekspertai nurodė, kad pasitaiko ir atvejų, kai bandoma įsibrauti į savivaldybės interneto svetainę. Didelės materialinės žalos nepatirta, klausimas išspręstas greitai, praradome nebent kelis dokumentus, kurie buvo sugadinti, tačiau sistema buvo skubiai atstatyta. Toks įvykis aišku privertė susimąstyti ir rimčiau žiūrėti į saugumą. Apibendrinant galima teigti, kad bet kokia kibernetinė ataka gali turėti pasekmių tiek darbuotojui, tiek pačiai savivaldybei, todėl svarbu išlaikyti budrumą, pastabumą, įvertinti siunčiamos informacijos turinį. Kibernetinių atakų grėsmių valdymui yra naudojamos įvairios techninės priemonės, programinė įranga, kurios padeda laiku atpažinti kenkėjiškus laiškus, melagingą informaciją bei kibernetinę ataką. Tyrimo metu ekspertai įvertino kokios kibernetinio saugumo priemonės yra taikomos savivaldybėse bei kaip yra vertinamas taikomų priemonių efektyvumas, užtikrinant kibernetinį saugumą savivaldybėje (žr. 5 lentelę).

5 lentelė. Ekspertų nuomonė apie taikomas kibernetinio saugumo priemones

KATEGORIJA	SUBKATEGORIJOS	PATVIRTINANTYS TEIGINIAI
Kibernetinio saugumo priemonės	Techninės priemonės	„turbūt kaip ir bet kuri organizacija taikomos įvairios ant virusinės programos“ (E1) „ugniasienės, potinklių atskyrimai, antivirusinės programos, tai standartiniai saugumo paketai“ (E3) „atsarginių kopijų darymas, saugus duomenų perdavimo tinklas, duomenų atstatymas po incidento“ (E6)
	Su vartotoju susijusios priemonės	„sukurtos įvairios apsaugos priemonės, vartotojų slaptažodžiai,

		teisių bei prieigų suteikimo kontrolė“ (E5) „vartotojų slaptažodžiai, taip pat vartotojų kontrolė ir monitoringas, tam tikrų tinklapių blokavimas“ (E2)
	Papildomos priemonės	„parengtos įvairios papildomos tvarkos ir nuostatai, pavyzdžiui incidentų pranešimo tvarka, reakcija į incidentus“ (E2) „asmens duomenų apsaugos reglamento taikymo tvarka“ (E3) „organizuojami darbuotojų mokymai, kompiuterinio raštingumo bei sąmoningumo ugdymas“ (E4) „informaciniai pranešimai darbuotojams kaip atpažinti kibernetines atakas ir grėsmes ir kaip elgtis joms įvykus“ (E6)

Apibendrinant pateiktus ekspertų interviu rezultatus galima teigti, kad dažniausiai savivaldybėse kibernetinių grėsmių valdymui yra naudojamos ugniasienės, potinklių atskyrimai, antivirusinės programos, vartotojų kontrolė (teisės, slaptažodžiai, administratoriai), sistemų rezervinių kopijų darymas, fizinė apsauga, taip pat naudojamas saugus duomenų perdavimo tinklas (SVDPT). Tyrimo metu ekspertai taip pat nurodė, kad pagrindinės priemonės paimtos iš KS įstatymo reikalavimų valstybinėms institucijoms, jų pagrindu yra parengiamos informacinių sistemų saugumo reikalavimų tvarkos, kurios apima:

- Kompiuterių administravimo/administratorių slaptažodžiai;
- Vartotojų slaptažodžių administravimo tvarka;
- Vartotojų kontrolė, monitoringas;
- VPN naudojimas;
- Duomenų apsauga (atsarginės kopijos, jų saugojimas, duomenų atstatymo po incidentų tvarka);
- Įsilaužimų detektavimas/prevencija;
- Incidentų raportavimo, reakcijos į incidentus tvarka;
- Fizinė prieigos kontrolė;
- Asmens duomenų apsaugos reglamento (BDAR) taikymo tvarka.

Papildomai yra taikomos ir darbuotojų ugdymo priemonės, yra organizuojami vidiniai specialistų mokymai, darbuotojų mokymai apie grėsmes ir kaip jų išvengti, organizuojamos pratybos. IT skyrius siunčia atmintines kaip atpažinti kilusią riziką, kokių priemonių imtis bei kur kreiptis. Ekspertų nuomone visos pateiktos bei išvardintos priemonės užtikrina vidutinį saugumo lygmenį savivaldybėje, siekiant aukštesnio kibernetinio saugumo lygio yra būtinas personalo švietimas, tinkamos programinės įrangos įsigijimas bei kvalifikuotų specialistų informacinio saugumo srityje įdarbinimas.

Kitu klausimu nustatyta ekspertų nuomonė apie tai kokias priemones taiko savo darbe siekiant užtikrinti kibernetinį saugumą (žr. 6 lentelę).

6 lentelė. Ekspertų nuomonė apie taikomas asmenines saugumo priemones

KATEGORIJA	SUBKATEGORIJOS	PATVIRTINANTYS TEIGINIAI
Asmeninis elgesys laikantis kibernetinio saugumo	Vidaus tvarkos taisyklių laikymasis	„visada naudoju tas priemones, kurias yra savivaldybė nupirkusi ir įdiegusi“ (E1) „laikausi numatytų vidaus tvarkos taisyklių“ (E3) „stengiuosi laikyti vidaus tvarkos taisyklių, informuoti atsakingus asmenis apie įvykusius incidentus ar galimas grėsmes“ (E6)
	Darbo vietos higiena	„svarbu laikytis darbo vietos dar kitaip vadinamos skaitmeninės higienos“ (E5) „kaip ir visi vartotojai turi užtikrinti darbo vietos tvarką ir tokiu būdu vengti bet kokių kylančių grėsmių“ (E2)
	Savišvieta	„interneto platybėse galima rasti daug naudingos ir reikiamos informacijos“ (E2) „daug dėmesio skiriu savišvietai, domiuosi naujovėmis, taip pat kibernetinių atakų pobūdžiu“ (E3) „renkuosi ir skaitau įvairią literatūrą, diskutuojame su kolegomis įvairiais klausimais“ (E6)

Tyrimo metu nustatyta kokiomis priemonėmis ekspertai siekia užtikrinti kibernetinį saugumą savivaldybėje. Ekspertų nuomone visada yra naudojamos tos programos, kurias savivaldybė įsigyja ir kurios yra prieinamos visiems vartotojams. Taip pat ekspertai nurodė, kad visada laikosi vidaus tvarkos taisyklių, stengiasi šviestis savarankiškai. Taip pat pabrėžia, kad pati savivaldybė turėtų būti labiau linkusi investuoti personalo mokymus.

Kitų ekspertų nuomone svarbi yra ir darbo vietos higiena (vadinama skaitmeninė higiena). Taip pat domėjimasis kibernetinio saugumo naujienomis. Organizuoju paskaitas kibernetinio saugumo temomis, ypač apie dažniausiai pasitaikančias vartotojų klaidas. Visų pirma interneto platybėse yra daug prieinama informacijos, todėl dažniausiai ekspertai renkasi literatūrą, diskutuoja ir analizuoja situaciją su kolegomis, o jeigu iškyla rimtesnių klausimų IT skyrius visada yra pasirengęs atsakyti į rūpimus klausimus. Taip pat ekspertai atkreipia dėmesį, kad IT skyrius kartais organizuoja ir siunčia informacinius pranešimus, atnaujinimus. Bet viskas priklauso nuo asmens nusiteikimo ir noro, nes jeigu

neaktualu nepadės niekas. Kitu klausimu nustatyta kaip ekspertai elgiasi ir kokių veiksmų imasi jeigu pastebi kibernetinių atakų riziką (žr. 7 lentelę).

7 lentelė. Ekspertų nuomonė apie reagavimą į kibernetines grėsmes

KATEGORIJA	SUBKATEGORIJOS	PATVIRTINANTYS TEIGINIAI
Reagavimas į kibernetines grėsmes	Numatytų procedūrų ir taisyklių laikymasis	„svarbiausia įvykus kibernetiniam incidentui laiku informuoti atsakingus darbuotojus“ (E2) „daugiau dėmesio reikia skirti darbuotojų supažindinimui su vidinėmis taisyklėmis, galiojančia tvarka“ (E3) „visada informuoju atsakingus darbuotojus, vos tik pastebėjus galimą riziką ar grėsmę“ (E5)
	Darbuotojų savalaikis informavimas	„svarbu kad darbuotojams būtų prieinama naujausia informacija tiek apie incidentus, tiek apie pasikeitusią valdymo tvarką“ (E1) „reikia mokyti darbuotojus atpažinti galimas grėsmes, nes tik tada informacija bus pateikiama laiku“ (E6)
	Papildomos pastangos ir reakcijos	„pasikeitus grėsmių pobūdžiui, peržiūrime ir taikomų priemonių pobūdį bei diegiame naujas priemones“ (E3) „gavus pranešimus iš NKSC atitinkamai reaguojame ir informuojame savivaldybės darbuotojus“ (E4) „pasikeitusios grėsmės skatina peržiūrėti ir atnaujinti turimas priemones, tam tikrais atvejais ir įsigyti naujų programų ar tinkamų kibernetinio saugumo priemonių“ (E5)

Remiantis pateiktais tyrimo rezultatais galima teigti, kad pagrindiniai veiksmai yra aprašyti vidaus tvarkos taisyklėse, reakcija į incidentus, pranešimo apie galimas grėsmes bei pastebėtus kibernetinius incidentus tvarka. Žinoma aprašyti visų priemonių neįmanoma, todėl parengtos tvarkos yra kasmet arba įvykus incidentui peržiūrimos bei atnaujinamos. Tačiau ekspertai atkreipia dėmesį, kad savivaldybės būdamos biudžetinėmis įstaigomis neturi pakankamai lėšų prevencijos programų įgyvendinimui, ne visada gali leisti prabangių ir modernių sprendimų diegimą, bet bazinius reikalavimus apibrėžtus įstatymuose užtikrina. Ekspertai atkreipia dėmesį, kad programinė įranga bei techninės

priemonės yra tik viena kibernetinio saugumo sistemos dalis, svarbus vaidmuo tenka ir žmogiškiesiems ištekliams, visada atsiranda kažkas, kas pabandys paspausti ant neaiškios nuorodos arba pabandys atidaryti neaiškų failą. Ekspertai nurodė, kad turi parengę reakcijos į kibernetinius incidentus atmintinę. Jeigu gauna įspėjimų iš NKSC apie suaktyvėjusią įsilaužėlių veiklą Lietuvoje (dažnai sąlygojamą pasaulinių įvykių), tai dedama daugiau pastangų į anomalijų savivaldybės tinkle stebėseną, labai praverčia tinklo monitoringo programinė įranga (aišku, norėtųsi turėti kažką galingesnio, tačiau metinės tokios įrangos prenumeratos yra ne visada finansiškai prieinamos savivaldybei). Taip pat visus incidentus, pagal tvarką, pranešame NKSC. Taigi standartinė procedūra įvykus kibernetinei atakai yra susijusi su visų pirma informavimu atsakingą skyrių bei darbuotojus, taip pat artimuosius, kolegas, svarbu kad apie grėsmę pirmiausia sužinotų atsakingas skyrius, kuris gali imtis reikalingų priemonių bei užtikrinti efektyvų situacijos valdymą. Po kibernetinės atakos mūsų IT skyrius visada parengia trumpą situacijos aprašymą bei atmintinę darbuotojams. Kitu klausimu nustatyta kaip ekspertai vertina kibernetinio saugumo politikos teisinį reguliavimą (žr. 8 lentelę).

8 lentelė. Kibernetinio saugumo teisinio reguliavimo vertinimas

KATEGORIJA	SUBKATEGORIJOS	PATVIRTINANTYS TEIGINIAI
Kibernetinio saugumo teisinis reguliavimas	Teisinis reguliavimas Lietuvoje	„vertinu gana teigiamai, nes parengti KS įstatymai, nuolat tobulinami ir atnaujinami“ (E2) „įstatymai nors ir parengti, tačiau labai neapibrėžti, trūksta aiškumo ir paprastumo“ (E4) „ne visi nurodyti įstatymuose punktai gali būti įgyvendinami ir pasieki savivaldybėse“ (E6)
	Savivaldybėje taikomos programos ir strategijos	„laikomės teisės aktuose nurodytų nuostatų, jas adaptuojame ir perkeliame į vidinius savivaldybės dokumentus“ (E1) „rengiamos savivaldybės strategijos, projektai, atmintinės ir įvairios tvarkos“ (E3) „parengtos bei atnaujinamos informacinių sistemų duomenų apsaugos nuostatos, taip pat remiamasi naujausiais BDAR pateiktais reikalavimais bei rekomendacijomis“ (E5)

Ekspertų nuomone įvertinus teisinį reguliavimą nustatyta, kad teisiškai sistema atrodo neblogai, KS įstatymai tobulinami, pateikiami savivaldybėms įgyvendinti. Kita vertus, jie labai sausi, trūksta konkretumo, gal netgi paprastumo. Galėtų būti kažkoks supaprastintas šablonas, kas turi būti įgyvendinta, pašalinant tai, kas viešajam sektoriui yra nepasiekiama (ar tai dėl finansinių ar žmogiškųjų

resursų stokos). Nes dažnai tai, kas yra „ant popieriaus“ prasilenkia su realybe. Teisinis reguliavimas padeda apsibrėžti vidines tvarkas savivaldybėje. Tačiau ekspertų nuomone yra abejojama ar visi perskaito visas nuorodas į visas įstatymų nuostatas. Ekspertų nuomone reiktų apsilankyti ir NKSC informacinėje svetainėje, kurioje informacija pateikiama pakankamai detaliai, pateikiama ne tik informacija, bet ir naudingos informacinės nuorodos, kurios gali būti sėkmingai pritaikytos savivaldybėje rengiant paskaitas darbuotojams arba ruošiant atmintines kibernetinio saugumo tematika.

Ekspertai nurodė, kad savivaldybės turi parengusios nemažą skaičių vidinių tvarkų savivaldybėje, remiantis saugumo politikos Lietuvoje įstatymais. Savivaldybės atveju yra parengtos procedūros, kibernetinis saugumas yra įtraukiamas į strateginius planus, pavyzdžiui kompiuterinio raštingumo ugdymas, kai kurie dokumentai yra naudojami tik savivaldybės lygmeniu ir neskleidžiami plačiajai visuomenei, tačiau strateginius planus, savivaldybės tikslus bei biudžeto paskirstymą gali peržiūrėti bet kuris visuomenės atstovas. Lietuvoje kibernetiniams saugumui manau yra skiriama daug dėmesio, dėl teisinio reguliavimo manau vertinimą turėtų atlikti teisininkai ir strategijas rengiantys atsakingi asmenys, bet mano nuomone teisinis reguliavimas yra pakankamas, o svarbiausia yra ne tik teisės aktų išleidimas, bet tinkamas nuostatų laikymasis ir teisės aktų įgyvendinimas. Čia būtinas visos visuomenės indėlis. Kadangi savivaldybės darbuotojų sąmoningumas lemia ir teisės aktų reikalavimų, programų įgyvendinimo sėkmę ekspertai įvertino kokie mokymai yra organizuojami darbuotojams (žr. 9 lentelę).

9 lentelė. Ekspertų nuomonė apie darbuotojų švietimą

KATEGORIJA	SUBKATEGORIJOS	PATVIRTINANTYS TEIGINIAI
Darbuotojų švietimas kibernetinio saugumo klausimais	Bendras švietimas, instruktažai	„visi savivaldybės darbuotojai bent kartą pusmetyje turi periodinį instruktažą kibernetinio saugumo klausimais“ (E1) „kartais atliekami budrumo ir savivaldybės darbuotojų sąmoningumo patikrinimai“ (E3) „įvykus kibernetinei atakai visada arba bent jau dažnai organizuojami pasitarimai, situacijos vertinimas, diskusija“ (E5)
	Vidiniai mokymai	„IT skyrius dažnai parengia įvairius pristatymus, organizuoja personalo mokymus“ (E2) „visi darbuotojai periodiškai gauna atnaujintas atmintines“ (E4) „skatinama informacijos ir patirties pasidalijimo praktika“ (E6)
	Išoriniai mokymai	„esant poreikiui pasitelkiame ir išorinius mokymus, lektorius“ (E3) „dalyvaujame NKSC rengiamuose mokymuose bei dalijamės

		informacija su kitomis savivaldybėmis“ (E5)

Ekspertų nuomone kibernetinio saugumo užtikrinimui savivaldybėje yra nuolat vykdomas bendras švietimas, kas pusmetiniai instruktažai. Ypač propaguoja informacinius aptarimus po kažkokių patirtų incidentų. Kartais atliekami tokie budrumo patikrinimai, kai savivaldybės personalui išsiuntinėjama kompromituojančius laiškus ir fiksuojame, kiek vartotojų susigundo paspausti klastingas nuorodas. Ekspertai nurodė, jog nuolat dalyvauja NKSC rengiamuose mokymuose, dalijasi incidentų informacija ar naujienomis su kaimyninių savivaldybių kolegomis. Ekspertų nuomone taip pat teigiamai vertinami NKSC su KAM rengiamus kas metinius kibernetinio saugumo mokymus savivaldybėms. Norėtume sudalyvauti ir įvairiuose hakatonuose, tačiau neturime pakankamai personalo, kad galėtume sau leisti kelioms dienoms apleisti savo darbinius postus. Galima išskirti vidinius ir išorinius mokymus. Vidiniai mokymai dažnai organizuojami savivaldybės iniciatyva, išorinius mokymus savivaldybė užsako pagal poreikį. Taip pat mūsų savivaldybėje visada skatinama iniciatyva pasiūlyti aktualius mokymus, kibernetinio saugumo taip pat. Todėl visada kolegoms rekomenduoju dalintis idėjomis, nes galbūt mes nepamatėme aktualių mokymų. Po bet kurių mokymų pasidalijame patirtimi su kitais kolegomis. Tačiau dar kartą pabrėšiu, nepakanka tik sudalyvauti mokymuose, reikia tas žinias dar pritaikyti ir praktikoje.

Tyrimo metu nustatyta ekspertų nuomonė apie tai kokius sprendimus reiktų priimti ir kokias priemones taikyti, siekiant efektyvinti kibernetinių atakų bei grėsmių valdymą savivaldybėje? Lietuvos mastu? (žr. 10 lentelę).

10 lentelė. Kibernetinio saugumo sprendimai

KATEGORIJA	SUBKATEGORIJOS	PATVIRTINANTYS TEIGINIAI
Kibernetinio saugumo sprendimai	Darbuotojų švietimas	„darbuotojai privalo turėti bent elementarių žinių ir informacijos apie kibernetinį saugumą ir grėsmes“ (E1) „švietimas ir dar kartą švietimas, nes dauguma klaidų įvyksta būtent dėl žmogiškojo faktoriaus neteisingų veiksmų“ (E3) „visuomenės švietimas yra būtinas kibernetinio saugumo sistemos elementas, padedantis įgyvendinti teisinius reikalavimus bei programose užsibrėžtus tikslus“ (E6)
	Infrastruktūros gerinimas	„reikia nepamiršti, kad įranga savaime neatsinaujina, todėl būtina daugiau dėmesio skirti programinės

		įrangos ir techninių priemonių atitikties vertinimui“ (E5) „nereikia pamiršti ir programinės įrangos bei nuolatinio infrastruktūros gerinimo“ (E2)
	Kvalifikuoto personalo pritraukimas	„labai stinga kvalifikuotų darbuotojų, ypač IT personalo, nes tik personalo dėka galima užtikrinti numatytų priemonių įgyvendinimą“ (E2) „ypač jaučiamas IT specialistų trūkumas, ypač mažuose miesteliuose“ (E3) „galima apgalvoti papildomų lėšų skyrimą kvalifikuoto personalo ugdymui bei specialistų pritraukimui“ (E6)

Ekspertų nuomone kibernetinio saugumo užtikrinimui, svarbiausia yra švietimas. Savivaldybės ir Lietuvos gyventojų skaitmeninis raštingumas yra gana žemas. Tai ypač matosi, kai IT specialistą užklausia darbuotojai patyrę kažkokį incidentą asmeniškai (dažniausiai savo mobiliame telefone) ir tada prašo pagalbos „čia pas mane kažkas dingo arba užsiblokavo arba nustojo veikti“ ir tu suvoki, kad viso to galima buvo išvengti, jei jie turėtų bent kažkokius žinių apie kibernetinės grėsmes pagrindus. Bet netgi nekalbant apie visokias grėsmes, žmonės (ypač mažesniuose miesteliuose) nemoka naudotis elektroniniu parašu, nemoka užsipildyti deklaracijų, užsiregistruoti pas specialistus ir pan. Gyventojus reikia šviesti ir pradėti jau reikia nuo pačių mažiausių vaikų. Taigi švietimas turėtų visų pirma apimti ne tik savivaldybės darbuotojus, bet ir bendrai daugiau dėmesio reikia skirti visuomenės švietimui ir ugdymui. Be abejo, reikėtų nepamiršti ir investavimo į infrastruktūrą, užtikrinančią kibernetinį saugumą. Ir galiausiai, viešajame sektoriuje ypač aktualu yra IT specialistų pritraukimas keliant jiems atlyginimus, savivaldybės nesugeba konkuruoti su privačiu sektoriumi. Ekspertai taip pat nurodė, kad galėtų būti vertinama ir apgalvojama apie viešojo sektoriaus subjektų valdymo centralizavimą, kaip tai daro Krašto apsaugos sistema. Pvz.: priskirti NKSC arba įkurti atskirą centrą, kuris teiktų prieglobos funkciją visų savivaldybių IS, tai padėtų kontroliuoti saugumą ir sumažintų išlaidas įrangai ir jos priežiūrai. Taip pat galėtų būti įvesti kažkokie nacionaliniai savivaldybių IT specialistų kibernetinio saugumo sertifikavimo reikalavimai, kas priverstų savivaldybes planuotis papildomas lėšas tų specialistų kvalifikacijos kėlimui.

Tiek savivaldybėje, tiek pačioje Lietuvoje turbūt pasigendama išsamesnių tyrimų ar informacijos sklaidos visuomenei suprantama kalba. Jeigu paimti ir paanalizuoti statistiką, tai joje faktai pateikiami sunkiai paprastam asmeniui suprantama kalba. Todėl turbūt būtų aktualu parengti informacinį vadovą ar kokią brošiūrą kurioje informacija būtų išdėstoma ir struktūruota: kas yra kibernetinė ataka, kodėl ji aktuali, kodėl reikia spręsti kibernetinio saugumo klausimus ir svarbiausia kaip atpažinti kibernetinius

įsilaužimus ir kaip į juos reaguoti. Paskutiniu klausimu ekspertai pateikė pasiūlymus kibernetinio saugumo gerinimui savivaldybėje užtikrinti (žr. 11 lentelę).

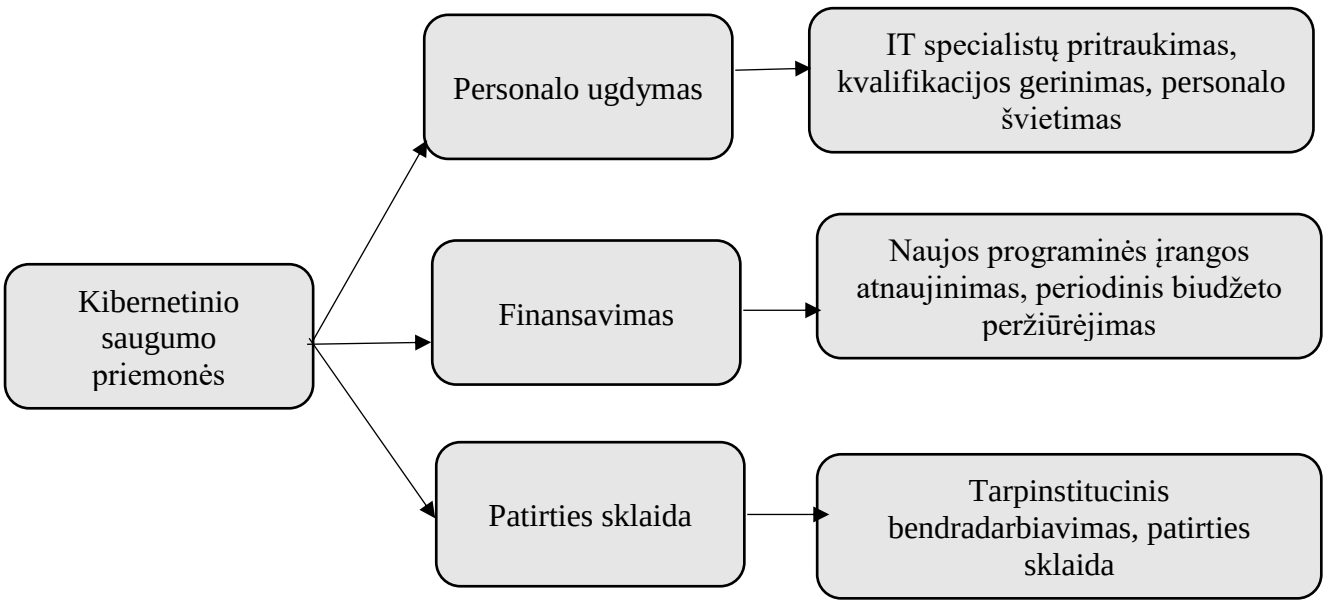
11 lentelė. Kibernetinio saugumo užtikrinimo priemonės

KATEGORIJA	SUBKATEGORIJOS	PATVIRTINANTYS TEIGINIAI
Kibernetinio saugumo gerinimo priemonės	Su personalu susiję sprendimai	„įvertinti ir daugiau dėmesio skirti personalo kompetencijos didinimui, IT specialistų pritraukimui“ (E1) „visuomenės sąmoningumo ir raštingumo lygio gerinimas“ (E3) „švietimas, įvairių programų rengimas tiek kibernetinio saugumo, tiek bendro kompiuterinio raštingumo klausimais“ (E6)
	Su savivaldybe susiję sprendimai	„perplanuoti metinės lėšas, daugiau dėmesio skiriant techninių sprendimų įgyvendinimui“ (E5) „tvarkas bei parengtas nuostatas kibernetinio saugumo klausimais peržiūrėti bent kartą metuose“ (E2)
	Lietuvos mastu susiję sprendimai	„finansavimo savivaldybėms didinimas, siekiant užtikrinti kibernetinio saugumo grėsmių valdymą ne tik savivaldybėse bet ir Lietuvos mastu“ (E2) „atlikti periodinius tyrimus, kurių metu būtų atskleidžiama visuomenės sąmoningumo bei susipažinimo su kibernetiniu saugumu situacija, skirti papildomai lėšų visuomenės švietimui“ (E6)

Ekspertų nuomone siekiant užtikrinti geresnį bei efektyvesnį kibernetinių atakų bei kibernetinio saugumo grėsmių valdymo lygmenį yra rekomenduojama didinti IT personalo etatų skaičių. Planuojant metines lėšas nenuvertinti tinklo įrangos atnaujinimo ir kitų saugumo priemonių įsigijimo svarbos. Nesikartojant apie švietimą, visiems reikėtų nustoti galvoti, kad kibernetinio saugumo problemos liečia tik IT padalinius ir tik jie už tai atsakingi. Kitas svarbus momentas yra kibernetinio saugumo priemonių finansavimas, būtina skirti dalį lėšų tinklo įrangos atnaujinimams ir saugumo programinės įrangos prenumeratoms ar kitiems įsigijimams. Pagrindiniai kibernetinio saugumo gerinimo sprendimai: organizuoti reguliarius kibernetinio saugumo mokymus savivaldybės darbuotojams, kad jie žinotų apie galimus pavojus. Papildomas – bendradarbiauti su kitomis savivaldybėmis, valstybinėmis institucijomis ir privačiomis įmonėmis, dalintis gerosiomis praktikomis bei rengti bendrus renginius, seminarus bei pasidalijimą patirtimi.

3.3.Kibernetinio saugumo savivaldybėje gerinimo sprendimai

Remiantis atlikto tyrimo rezultatais kibernetinio saugumo gerinimo sprendimai gali apimti tokias sritis: savivaldybės darbuotojų ir gyventojų kompiuterinio raštingumo didinimas, švietimas, savivaldybės rengiamų dokumentų periodinė peržiūra, bendradarbiavimo skatinimas ir kvalifikuoto personalo pritraukimas (žr. 6 pav.).



6 pav. Kibernetinio saugumo gerinimas savivaldybėje

Kovoti su kibernetinėmis atakomis yra įvairių metodų. Viena iš žinomiausių metodikų yra sukurta Jungtinių Tautų tarptautinė telekomunikacijų sąjunga (ITU). Joje numatyta, kas turi būti įgyvendinta valstybėje, kad ji būtų atspari. Pagal ITU skelbiamą atsparumo indeksą, Lietuva šiais metais pakilo net į ketvirtą vietą pralenkdama Estiją (NKSC, 2021). Kita dažnai sutinkama metodologija yra vadinamasis Oksfordo modelis, sukurtas Oksfordo universitete. Svarbiausias šio modelio privalumas tas, kad ne tik surenkami faktai apie teisės aktų ar institucijų egzistavimą, bet ir vertinamas jų realus poveikis (Giniotienė, 2019). Į kibernetinio saugumo sistemą žiūrima per penkias dimensijas (Giniotienė, 2019): kibernetinio saugumo politikos planavimo, teisinio reguliavimo, kibernetinės kultūros lygio, švietimo mokykloje, universitetuose ir profesinio ugdymo įstaigose bei kibernetinio saugumo geruųjų praktikų taikymo valstybiniame ir privačiame sektoriuje.

Remiantis paveiksle pateikta informacija savivaldybės įstaigoms yra rekomenduojama adaptuoti Oksfordo modelį bei pritaikyti atsižvelgiant į tris pagrindines kibernetinio saugumo modelio dimensijas:

- Visuomenės ir savivaldybės darbuotojų švietimas, kompiuterinio raštingumo lygio gerinimas, informacijos sklaida. Šiuo metu pasigendama organizuojamų mokymų visuomenei, kurių metu būtų suteikiama išsami informacija apie grėsmių valdymą,

kibernetinių atakų atpažinimą, galimas valdymo priemones. Tačiau mokymų metu įgytos žinios turėtų būti pritaikomos praktikoje;

- Finansavimo didinimas. Tyrimo rezultatai atskleidė, kad savivaldybėms ne visada pakanka lėšų įsigyti reikiamą programinę įrangą arba ją atnaujinti, tokią situaciją lemia netinkamas lėšų planavimas. Kita problema susijusi su finansavimu yra kvalifikuotų specialistų pritraukimas bei mokymas.
- Tarpinstitucinio bendradarbiavimo skatinimas yra būtina kibernetinio saugumo užtikrinimo bei gerinimo programos dalis, kurios metu pasidalijama patirtimi su kitomis institucijomis, savivaldybėmis, tarptautinėmis organizacijomis. Savivaldybėms rekomenduojama analizuoti ir kitų šalių savivaldybių taikomą praktiką.

IŠVADOS

- Moksliniuose tyrimuose nėra pateikiama vieninga kibernetinių atakų samprata, dažnai naudojamos sąvokos, tokios kaip kibernetinis pavojus, kibernetinė rizika, išpuolis ar kibernetinė grėsmė yra kibernetinių atakų sąvokos sinonimai. Išanalizavus įvairius apibrėžimus galima teigti, kad kibernetinės atakos yra veiksmai, kurių šalys imasi siekdamos prasiskverbti į šalies ar kitų šalių kompiuterius ar kompiuterinius tinklus, kad pakenktų ar sutrikdytų įprastinę veiklą, kibernetinės atakos tai kibernetinės operacijos, kurios skirtos užpulti arba apsiginti, dėl kurių pagrįstai galima tikėtis žmonių sužalojimo ar mirties, objektų sugadinimo ar sunaikinimo.
- Europos Sąjungos mastu kibernetinio saugumo užtikrinimui modernizuojama ir tobulinama teisinė bazė, atsižvelgiant į vykstančius pokyčius bei informacinių technologijų raidą ir saugumui keliamas grėsmes. Tačiau ES priimti teisės aktai bei reglamentai turi būti inkorporuojami į valstybių narių teisinę bazę, siekiat atitikti ES keliamus reikalavimus. Dauguma valstybių narių ES galiojančių teisės aktų pagrindu tobulina priimtus kibernetinio saugumo įstatymus bei atnaujina nacionalines kibernetinio saugumo strategijas.
- Analizuotose užsienio šalyse kibernetinio saugumo strategijose identifikuojami pagrindiniai tikslai bei įgyvendinimo priemonės. Lietuva analizuotų šalių kontekste užima aukštą vietą vertinant pagal kibernetinio saugumo indeksavimo sistemą. Tačiau norėtųsi atkreipti dėmesį į Estijoje taikomą kibernetinio saugumo strategiją, kurioje daug dėmesio skiriama tarptautiniam bendradarbiavimui, tarpinstituciniam nacionalinių įstaigų bei struktūrų darbui, visuomenės švietimo iniciatyvoms.
- Atlikus tyrimą nustatyta, kad dažniausiai pasitaikančios grėsmės savivaldybėje yra susijusios su bandymais užkrėsti arba „Phishing“ tipo elektroniniai laiškai ir mėginimai įsilaužti į naudojamas sistemas. Savivaldybės susiduria ir su dezinformacijos, melagingų elektroninių laiškų grėsmėmis. Savivaldybių taikomi kibernetinio saugumo reikalavimai. Informacinių sistemų tarnybinių stočių apsauga nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėti, nepageidaujamo elektroninio pašto ir pan.) užtikrinama programinėmis priemonėmis: antivirusinėmis programomis, ugniasienėmis (techninė ir programinė). Pagrindinis situacijos gerinimo būdas – organizuoti reguliarius kibernetinio saugumo mokymus savivaldybės darbuotojams, kad jie žinotų apie galimus pavojus. Papildomas – bendradarbiauti su kitomis savivaldybėmis, valstybinėmis institucijomis ir privačiomis įmonėmis, dalintis gerosiomis praktikomis bei rengti bendrus seminarus.
- Bet kokia kibernetinė ataka gali turėti pasekmių tiek darbuotojui, tiek pačiai savivaldybei, todėl svarbu išlaikyti budrumą, pastabumą, įvertinti siunčiamos informacijos turinį. Kibernetinių atakų grėsmių valdymui yra naudojamos įvairios techninės priemonės, programinė įranga, kurios

padeda laiku atpažinti kenkėjiškus laiškus, melagingą informaciją bei kibernetinę ataką. Ekspertų nuomone visos pateiktos bei išvardintos priemonės užtikrina vidutinį saugumo lygmenį savivaldybėje, siekiant aukštesnio kibernetinio saugumo lygio yra būtinas personalo švietimas, tinkamos programinės įrangos įsigijimas bei kvalifikuotų specialistų kibernetinio saugumo srityje įdarbinimas.

- Vidiniai mokymai dažnai organizuojami savivaldybės iniciatyva, išorinius mokymus savivaldybė užsako pagal poreikį. Taip pat savivaldybėse visada skatinama iniciatyva pasiūlyti aktualius mokymus, kibernetinio saugumo taip pat. Po bet kurių mokymų pasidalijama patirtimi su kitais kolegomis. Tačiau svarbu užtikrinti, kad įgytos žinios būtų pritaikomos praktikoje.

REKOMENDACIJOS

Remiantis atlikto tyrimo rezultatais savivaldybėms yra rekomenduojama:

- Gerinti darbuotojų sąmoningumą užtikrinant periodinį žinių atnaujinimą, informacijos apie kibernetinio saugumo grėsmių keliamą žalą naudą, kibernetinių grėsmių atpažinimo priemones;
- Skatinti bendradarbiavimą ir patirties pasidalijimą su kitomis savivaldybėmis, tarptautinėmis organizacijomis, esant poreikiui rengti bendrus renginius ir seminarus;
- Planuojant biudžetą savivaldybėms rekomenduojama peržiūrėti skiriamų lėšų kibernetiniam saugumui užtikrinti dalį bei skirti papildomų lėšų programinės ir techninės įrangos atnaujinimui;
- Daugiau dėmesio skirti kvalifikuotų IT specialistų pritraukimui bei išlaikymui.

LITERATŪRA

Teisės aktai

1. Lietuvos Respublikos kibernetinio saugumo įstatymas 2014 m. gruodžio 11 d. Nr. XII-1428 (2021-01-01 suvestinė redakcija), < https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/asr >, žiūrėta 2022-11-16.
2. Nacionalinė kibernetinio saugumo strategija 2018 m. rugpjūčio 13 d. Nr. 818, <https://kam.lt/download/66421/2019lt-kibernetinesaugumostrategija-131%20egz.pdf >.

Mokslinės literatūros šaltiniai

3. Al-Ghamdi, M.I. (2021). Effects of knowledge of cyber security on prevention of attacks. Mater. Today: Proc.
4. Attatfa, A, Renaud, K & De Paoli, S. (2020) Cyber diplomacy: a systematic literature review. *Procedia Computer Science*, vol. 176, p. 60-69.
5. Backhaus, S., Gross, M. L., Waismel-Manor, I., Cohen, H., & Canetti, D. (2020). A cyberterrorism effect? Emotional reactions to lethal attacks on critical infrastructure. *Cyberpsychology, Behavior, and Social Networking*, *23*(9), p. 595–603.
6. Bendovschi, A. (2015). Cyber – attacks trends, patterns and security countermeasures. *Procedia Economics and Finance*, No. 28, p. 24-31.
7. Bullock, J.A., Haddow, G.D., Coppola, D.P. (2021). Cybersecurity and critical infrastructure protection. In: Bullock, J.A., Haddow, G.D., Coppola, D.P. (Eds.), Introduction to Homeland Security, sixth ed. Butterworth-Heinemann, p.425–497.
8. Cavelty, M. D. (2018). Cybersecurity research meets science and technology studies. *Politics and Governance*, 6(2), p. 22–30
9. Cao, Y., et al. (2019). A topology-aware access control model for collaborative cyber–physical spaces: Specification and verification. *Comput. Secur*. 87, 101478.
10. Chodakowska, A., Kandula, S. (2022). Cybersecurity in the Local Government Sector in Poland: More Work Needs to be Done. LEX LOCALIS - JOURNAL OF LOCAL SELF-GOVERNMENT Vol. 20, No. 1, p. 161 – 192.
11. Chałubińska-Jentkiewicz, K. (2021). Access to the ICT network as a public task of local government, *Lex Localis - Journal of Local Self-Government*, 19(1), p. 175–195.
12. Chen, J.-K., et al. (2021). Cyber deviance among adolescents in Taiwan: Prevalence and correlates. *Child. Youth Serv. Rev*. 126, 106042
13. Enescu, S. (2020). A comparative study on European cyber security strategies. International conference RCIC'20.

14. ENISA (2017), *Overview of Cybersecurity and Related Terminology, Version 1.* Heraklion: ENISA Publications.
15. Hatcher, W., Meares, W. L. & Heslen, J. (2020) The cybersecurity of municipalities in the United States: an exploratory survey of policies and practices, *Journal of Cyber Policy*, 5(2), p. 302–325.
16. Jacuch, A. (2021). Comparative analysis of cybersecurity strategies. European Union strategy and policies. Polish and selected countries strategies. *Online Journal modelling the new Europe*, No. 37, p. 102-120.
17. Karpiuk, M. (2021) The Local Government's Position in the Polish Cybersecurity System, *Lex Localis – Journal of Local Self-Government*, 19(3), p. 609–620
18. Korauš, A., Gombar, M., Kelemen, P., Backa, S. (2019). Using quantitative methods to identify insecurity due to unusual business operations, *Entrepreneurship and Sustainability Issues* 6(3), p. 1101-1012.
19. Lan, T., Iinkster, N. (2020) International governance of/in cyberspace. In: TIKK E. and KERTTUNEN M. (eds.) *Routledge Handbook of International Cybersecurity* (pp. 79-93). Routledge.
20. Li, Y., Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy reports*, No. 7, p. 8176-8186.
21. Marcinauskaitė, R., Pukanasytė, I. (2019). Cyber security issues: problematic aspects of hacking. *Journal of security and sustainability issues*, vol. 8, No. 3, p. 331-343.
22. Mosteanu, N., Galea, K. (2020). Artificial intelligence and cyber security – face to face with cyber attack – A Maltese case of risk management approach. FGOFORUM, vol. 9, issue 2, p. 1-8.
23. Motsch, W., et al. (2020). Approach for dynamic price-based demand side management in cyber physical production systems. *Procedia Manuf*. 51, p. 1748–1754.
24. Norris, D. F., Mateczun, L., Joshi, A. & Finin, T. (2019) Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity, *Public Administration Review*, 79(6), p. 895–904
25. Limba, T. ir kt. (2017). Cyber security management model for critical infrastructure. *The international journal entrepreneurship and sustainability issues*, vol. 4, No. 4, p. 559-573.
26. Nikolova, I. (2017). Best practice for cybersecurity capacity building in Bulgaria public sector. *Information & Security: international journal*, vol. 38, p. 79-92.
27. Norris, D., Mateczun, L., Forno, R. (2022). *Cybersecurity and local government*. Willey Publishing.
28. Ogbanufe, O. (2021). Enhancing end-user roles in information security: Exploring the setting, situation, and identity. *Comput. Secur*. 108, 102340.
29. Schmitt, M. (2016). *Tallin manual 2.0 on the international law applicable to cyber warfare*. New York: Cambridge University Press, p. 415.

30. Štitilis, D.; Pakutinskas, P.; Kinis, U.; Malinauskaitė, I. (2016). Concepts and principles of cyber security strategies, *Journal of Security and Sustainability Issues* 6(2), p. 197-210.
31. Štitilis, D., Pakutinskas, P. ir kt. (2017). A model for the national cyber security strategy: Lithuanian case. *Journal of security and sustainability issues*, vol.6, No. 3, p. 357-372.
32. Štitilis, D., Rotomskis, I. ir kt. (2020). National cyber security strategies: management, unification and assessment. *Independent Journal of management & production*, vol. 11, No. 9, p. 2341-2354.
33. Tam, T., Rao, A., Hall, J. (2021). The bad and the missing: A narrative review of cyber-security implications for Australian small businesses. Comput. Secur. 102385.
34. The European Parliament and the Council of the European Union. (2016). Directive (EU)2016/1148 of the European Parliament and of the Council concerning Measures for High Common Level of Security of Network and Information Systems across the Union, 2016. *Official Journal of the European Union.* L 194.
35. The European Parliament and the Council of the European Union. (2019). Regulation (EU) 2019/881 n ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). *Official Journal of the European Union.* L 151.
36. Toapanta, S., Cobena, J. (2020). Analysis of Cyberattacks in Public Organizations in Latin America. *Advances in Science, Technology and Engineering Systems Journal* Vol. 5, No. 2, p. 116-125.
37. Tvaronavičienė, M. (2018). Towards internationally tuned approach towards critical infrastructure protection, *Journal of Security and Sustainability Issues* 8(2), p. 143-150.
38. Tvaronavičienė, M., Plėta, T. ir kt. (2020). Cyber security man- agement of critical energy infrastructure in national cybersecurity strategies: cases of USA, UK, France, Estonia and Lithuania. *Insights into Regional Development*, 2 (4), p.802 - 813.
39. Wirtz, B.W. & Weyerer, J.C. (2017). Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats. *International Journal of Public Administration*, 40 (13), p. 1085-1100.

Kiti šaltiniai

40. Chapelle, A., Crama, Y., Huebner, G., & Peters, J.-P. (2018). Practical methods for measuring and managing operational risk in the financial sector: a clinical study. *Banking & Finance*, *32*(6). Prieiga internetu: https://doi.org/10.1016/j.jbankfin.2007.09.017
41. EUROPEAN COMMISSION. (2020) Communication from the Commission to the European Parliament and the Council: Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity Across the Union, repealing Directive (EU) 2016/1148 Brussels 16.12.2020, COM (2020) 823 final.

42. EUROPEAN COMMISSION. (2020) Communication from the Commission to the European Parliament and the Council: Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities Brussels 16.12.2020, COM (2020) 829 final.
43. EUROPEAN COMMISSION. (2020) Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade Brussels 16.12.2020 JOIN (2020) 18 final.
44. EUROPEAN COMMISSION. (2020) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European strategy for data Brussels, 19.02.2020, COM (2020) 66 final.
45. EUROPEAN PARLIAMENT. (2021) European Parliament resolution of 10 June 2021 on the EU's Cybersecurity Strategy for the Digital Decade (2021/2568(RSP)).
46. EUROPEAN PARLIAMENT. (2021) European Parliament resolution of 10 June 2021 on the EU's Cybersecurity Strategy for the Digital Decade (2021/2568(RSP)).
47. Gavėnaitė – Sirvydienė, J., Miečinskienė, A. (2021). Forecasting costs of cyber attacks using estimation the global cost of cyber risk calculation. Prieiga internetu: https://doi.org/10.3846/cibmee.2021.618
48. MINISTRY OF DIGITAL AFFAIRS. (2019) Cybersecurity Strategy of The Republic of Poland for 2019 – 2024.
49. Ministry of Foreign Affairs, "Foreign Minister Reinsalu: membership of the UN Security Council makes Estonia greater on the world map," *Ministry of Foreign Affairs*, 2019. https://vm.ee/en/news/foreign-minister-reinsalumembership-un-security-council-makes-estoniagreater-world-map
50. Perera, S.; Jin, X.; Maurushat, A.; Opoku, D.-G.J. (2022). Factors Affecting Reputational Damage to Organisations Due to Cyberattacks. Informatics, 9, 28. Prieiga internetu: https://doi.org/10.3390/informatics9010028
51. PINGEN A. (2021) Parliament Calls for Tighter EU Cybersecurity Standards for Connected Products and Associated Services, EUCRIM 09.07.2021. Prieiga internetu: https://eucrim.eu/news/parliament-calls-for-tighter-eu-cybersecurity-standards-forconnected-products-and-associated-services/
52. Shandler, R., Gomez, M. (2022): The hidden threat of cyberattacks – undermining public confidence in government, Journal of Information Technology & Politics, Prieiga internetu: https://doi.org/10.1080/19331681.2022.2112796
53. Toch, E., Bettini, C., Shmueli, E., Radaelli, L., Lanzi, A., Riboni, D., & Lepri, B. (2018). The privacy implications of cyber security systems: A technological survey. *ACM Computing Surveys*, *51*(2), Article. Prieiga internetu: https://doi.org/10.1145/3172869

ANOTACIJA

Šalys patiria didesnį kibernetinių grėsmių poveikį ir žalą, nes šalies įstatymai ir politika, susiję su kibernetiniu saugumu, nėra pakankami arba nėra veiksmingai įgyvendinami; technologijų ir infrastruktūros trūkumai ir žinių bei pasirengimo prieš kibernetines atakas trūkumas; vartotojų mokymo bei informuotumo, bei institucijų ir organizacijų koordinavimo ir bendradarbiavimo trūkumas sukelia grėsmę kibernetiniams saugumui. Darbe keliamas probleminis klausimas: kokia užsienio šalių kibernetinių atakų valdymo geroji praktika gali būti pritaikyta Lietuvos viešojo sektoriaus institucijose?

Tyrimo objektas – kibernetinių atakų viešojo valdymo įstaigose valdymas.

Tyrimo tikslas – išanalizavus kibernetinių atakų valdymo teorinius aspektus bei remiantis pusiau struktūruotos apklausos rezultatais, pritaikyti geriausią pasaulinę praktiką kibernetinių atakų valdymui viešojo sektoriaus informacinėse sistemose.

Pirmoje teorinėje darbo dalyje analizuojama kibernetinių atakų apibrėžtis, klasifikacija, aptariamos kibernetinių atakų sukeliamos grėsmės. Šioje darbo dalyje analizuojama kibernetinio saugumo valdymo įgyvendinimo situacija ir priemonės, teisinio reguliavimo nacionaliniu ir tarptautiniu lygmeniu ypatumai, apžvelgiama užsienio šalių geroji praktika, atskleidžianti taikomus modelius ir priemones. Antroje darbo dalyje pateikiama empirinio tyrimo metodologija, tyrimo loginė schema. Trečioje darbo dalyje analizuojami tyrimo rezultatai bei pateikiami sprendimai kibernetinių atakų viešojo sektoriaus institucijose valdymo tobulinimui.

Raktiniai žodžiai: kibernetinė ataka, kibernetinis saugumas, grėsmė, nacionalinė strategija, elektroninės priemonės.

ANNOTATION

Countries experience increased exposure and damage from cyber threats because national laws and policies related to cyber security are insufficient or not effectively implemented; technology and infrastructure deficiencies and lack of knowledge and preparedness against cyber-attacks; the lack of training and awareness of users, as well as the lack of coordination and cooperation of institutions and organizations causes a threat to cyber security. The work raises a problematic question: what good practices of foreign cyber attack management can be applied in Lithuanian public sector institutions?

The object of the study is the management of cyber attacks in public administration institutions.

The purpose of the study is to apply the best global practices for managing cyber attacks in public sector information systems after analyzing the theoretical aspects of cyber attack management and based on the results of a semi-structured survey.

The first theoretical part of the work analyzes the definition and classification of cyber attacks, discusses the threats caused by cyber attacks. This part of the work analyzes the situation and measures of the implementation of cyber security management, the peculiarities of legal regulation at the national and international level, reviews the good practices of foreign countries, revealing the applied models and measures. The second part of the work presents the methodology of the empirical research, the logical scheme of the research. The third part of the work analyzes the research results and presents solutions for improving the management of cyber attacks in public sector institutions.

Keywords: cyber attack, cyber security, threat, national strategy, electronic means.

SANTRAUKA

Šalys patiria didesnį kibernetinių grėsmių poveikį ir žalą, nes šalies įstatymai ir politika, susiję su kibernetiniu saugumu, nėra pakankami arba nėra veiksmingai įgyvendinami; technologijų ir infrastruktūros trūkumai ir žinių bei pasirengimo prieš kibernetines atakas trūkumas; vartotojų mokymo bei informuotumo, bei institucijų ir organizacijų koordinavimo ir bendradarbiavimo trūkumas sukelia grėsmę kibernetiniams saugumui. Darbe keliamas probleminis klausimas: kokia užsienio šalių kibernetinių atakų valdymo geroji praktika gali būti pritaikyta Lietuvos viešojo sektoriaus institucijose?

Tyrimo objektas – kibernetinių atakų viešojo valdymo įstaigose valdymas.

Tyrimo tikslas – išanalizavus kibernetinių atakų valdymo teorinius aspektus bei remiantis pusiau struktūruotos apklausos rezultatais, pritaikyti geriausią pasaulinę praktiką kibernetinių atakų valdymui viešojo sektoriaus informacinėse sistemose.

Pirmoje teorinėje darbo dalyje analizuojama kibernetinių atakų apibrėžtis, klasifikacija, aptariamos kibernetinių atakų sukeliamos grėsmės. Šioje darbo dalyje analizuojama kibernetinio saugumo valdymo įgyvendinimo situacija ir priemonės, teisinio reguliavimo nacionaliniu ir tarptautiniu lygmeniu ypatumai, apžvelgiama užsienio šalių geroji praktika, atskleidžianti taikomus modelius ir priemones. Antroje darbo dalyje pateikiama empirinio tyrimo metodologija, tyrimo loginė schema. Trečioje darbo dalyje analizuojami tyrimo rezultatai bei pateikiami sprendimai kibernetinių atakų viešojo sektoriaus institucijose valdymo tobulinimui.

Dažniausiai pasitaikančios grėsmės savivaldybėje yra susijusios su bandymais užkrėsti arba „Phishing“ tipo elektroniniai laiškai ir mėginimai įsilaužti į naudojamas sistemas. Savivaldybės susiduria ir su dezinformacijos, melagingų elektroninių laiškų grėsmėmis. Savivaldybių taikomi kibernetinio saugumo reikalavimai. Informacinių sistemų tarnybinių stočių apsauga nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėti, nepageidaujamo elektroninio pašto ir pan.) užtikrinama programinėmis priemonėmis: antivirusinėmis programomis, ugniasienėmis (techninė ir programinė). Pagrindinis situacijos gerinimo būdas – organizuoti reguliarius kibernetinio saugumo mokymus savivaldybės darbuotojams, kad jie žinotų apie galimus pavojus. Papildomas – bendradarbiauti su kitomis savivaldybėmis, valstybinėmis institucijomis ir privačiomis įmonėmis, dalintis gerosiomis praktikomis bei rengti bendrus seminarus.

SUMMARY

Countries experience increased exposure and damage from cyber threats because national laws and policies related to cyber security are insufficient or not effectively implemented; technology and infrastructure deficiencies and lack of knowledge and preparedness against cyber-attacks; the lack of training and awareness of users, as well as the lack of coordination and cooperation of institutions and organizations causes a threat to cyber security. The work raises a problematic question: what good practices of foreign cyber attack management can be applied in Lithuanian public sector institutions?

The object of the study is the management of cyber attacks in public administration institutions.

The purpose of the study is to apply the best global practices for managing cyber attacks in public sector information systems after analyzing the theoretical aspects of cyber attack management and based on the results of a semi-structured survey.

The first theoretical part of the work analyzes the definition and classification of cyber attacks, discusses the threats caused by cyber attacks. This part of the work analyzes the situation and measures of the implementation of cyber security management, the peculiarities of legal regulation at the national and international level, reviews the good practices of foreign countries, revealing the applied models and measures. The second part of the work presents the methodology of the empirical research, the logical scheme of the research. The third part of the work analyzes the research results and presents solutions for improving the management of cyber attacks in public sector institutions.

The most common threats in the municipality are related to attempts to infect or "Phishing" type e-mails and attempts to break into the systems used. Municipalities also face the threat of misinformation and false e-mails. Cyber security requirements applied by municipalities. Protection of information systems service stations against harmful software (viruses, software intended for espionage, unsolicited e-mail, etc.) is ensured by software tools: antivirus programs, firewalls (technical and software). The main way to improve the situation is to organize regular cyber security training for municipal employees so that they are aware of possible dangers. Additional - to cooperate with other municipalities, state institutions and private companies, share good practices and hold joint seminars.

PRIEDAI

Ekspertų interviu klausimai

1. Jūsų užimamos pareigos savivaldybėje
2. Jūsų darbo stažas savivaldybėje
3. Apibūdinkite su kokiomis kibernetinio saugumo grėsmėmis jums teko susidurti per pastaruosius dvejus metus savivaldybėje.
4. Kokį poveikį kibernetinės atakos turi/turėjo jūsų savivaldybei. Pateikite kibernetinių atakų pavyzdžių bei apibūdinkite sukeliamą riziką.
5. Kokios kibernetinio saugumo priemonės yra taikomos Jūsų savivaldybėje? Kaip vertinate taikomų priemonių efektyvumą užtikrinant kibernetinį saugumą?
6. Kokias priemones jūs asmeniškai taikote savo darbe siekdamas užtikrinti kibernetinį saugumą?
7. Papasakokite kaip elgiatės ar kokių veiksmų imatės jeigu pastebite kibernetinių atakų riziką?
8. Kaip vertinate kibernetinio saugumo politiką bei teisinį reguliavimą Lietuvoje ir Jūsų savivaldybėje? Kokios teisinės priemonės yra taikomos savivaldybėje? Kokius dokumentus, procedūras ar strategijas esate parengę?
9. Kokie darbuotojų mokymai yra organizuojami savivaldybėje, siekiant užtikrinti kibernetinį saugumą? Kaip dalijamasi patirtimi susijusia su kibernetinio saugumo užtikrinimu?
10. Kokius sprendimus reiktų priimti ir kokias priemones taikyti, siekiant efektyvinti kibernetinių atakų bei grėsmių valdymą savivaldybėje? Lietuvos mastu?
11. Kokius kibernetinio saugumo užtikrinimo bei gerinimo pasiūlymus galite pateikti savivaldybėje?